Canon MFP Security Chip

FIPS140-3 Security Policy

Version 1.27
2024/8/22
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 General

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 FIPS140-3 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 FIPS140-3 Security Policy
Version	1.27
Issuer	Canon Inc.
Date of issue	2024/8/22

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
ENT (P)	Physical entropy source compliant with NIST SP 800-90B.
CO	Crypto Officer
CSP	Critical Security Parameter
PSP	Public Security Parameter
SSP	Sensitive 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.

1.3 Security Level

The Canon MFP Security Chip is a cryptographic module designed and implemented to meet the FIPS140-3 Level 2 security requirements. Table2 shows the security level met by the Canon MFP Security Chip for each of the specified areas. The overall level is level 2.

Table 2 Security Levels

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A

1.4 Certificate Caveat

When installed, initialized and configured as specified in Section 11 of the Security Policy. When entropy is externally loaded[1], no assurance of the minimum strength of generated SSPs (e.g., keys).

[1] “externally loaded” caveat is only applicable when “Input secret information” service is used.

2 Cryptographic Module Specification

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 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 “Multiple-chip embedded cryptographic module” and the cryptographic boundary is the surface of the package. The following table shows the hardware and firmware comprising the Canon MFP Security Chip (As described in Section 2.2, all elements of the module are enclosed in a single package). The firmware includes the boot loader.

Table 3 Cryptographic Module Tested Configuration

Model	Hardware Version	Firmware Version
Canon MFP Security Chip	3.0	3.00, 3.00(V05L00), 3.00(V05L01)

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

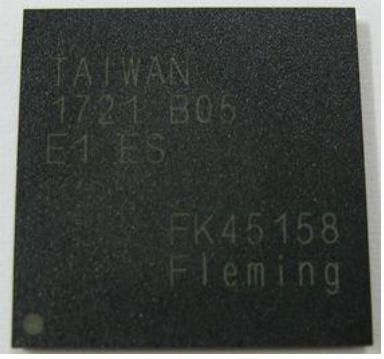

Figure 1 Appearance of the Canon MFP Security Chip

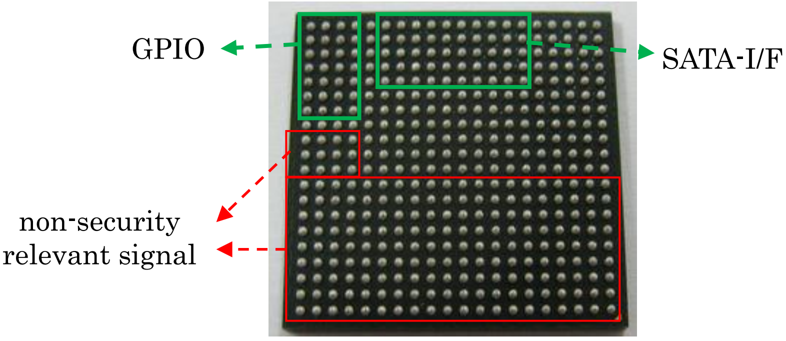

Figure 2 Appearance of Canon MFP Security Chip (Bottom view)

2.2 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.

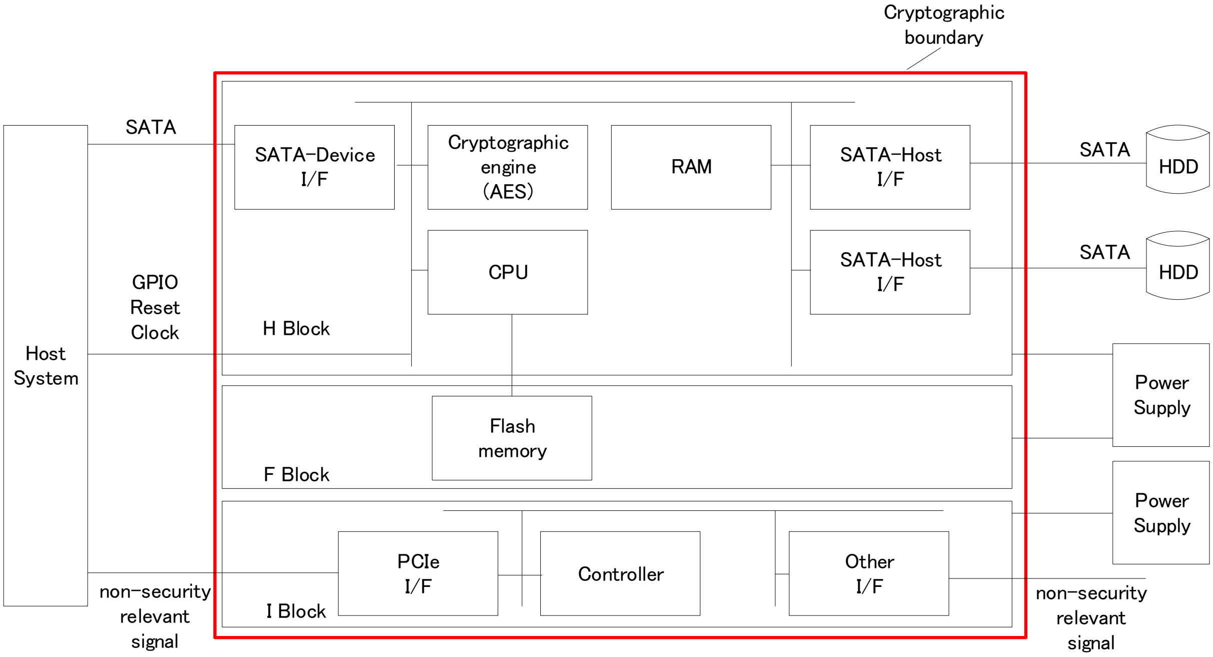

Figure 3 Example of operational configuration of Canon MFP Security Chip

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 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 SSPs 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 FIPS140-3 requirements.

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

Table 4 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	Interface to process SATA I/O for the Canon MFP

SATA-Host I/F	Security Chip.
Cryptographic engine	Handles AES encryption and decryption.

2.3 Mode of Operation

The Canon MFP Security Chip supports Approved mode, which implements security features approved by CMVP, and non-Compliant state, which is considered outside the scope of this certification.

The Canon MFP Security Chip operates in non-Compliant state when installed. It becomes validated one by using the Initialization operation described in Section 11 and is always in Approved mode.

If “Sanitization” service is used in Approved mode, the module will transition to non-Compliant state.

2.4 Cryptographic Algorithm

The Canon MFP Security Chip provides the following approved algorithms in Approved mode.

Table 5 Approved algorithms

CAVP Cert	Algorithm and Standard	Mode/ Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#C217	AES[2] FIPS PUB 197 SP 800-38E	XTS Encryption/ Decryption	Key Strength: 128 bits, 256 bits Length: 128 bits, 256 bits	Used in encryption/decryption of data stored in storage device.
#4547	SHS FIPS PUB 180-4	SHA-256	Size: 256 bits	Used in Hash_DRBG random bit generation, response generation for Device Identification and Authentication, and RSA digital signature verification.
#3059	RSA FIPS PUB 186-4 PKCS#1	Signature Verification	Modulus: 2048 bits	Used for firmware verification.
#2300	Hash_DRBG SP 800-90A Rev.1	N/A	SHA-256	Used in cryptographic key generation, and challenge generation for Device Identification and Authentication.
ENT(P)	Entropy Source SP 800-90B	N/A		Used in generating the seed value for approved DRBG
Vendor Affirmed	CKG SP 800-133rev2	N/A		Used in cryptographic key generation. As per SP 800-133rev2 Section 4.

The Canon MFP Security Chip does not implement any non-Approved algorithms.

[2] #C217 includes AES-ECB as validated algorithm. This is used as a prerequisite for XTS-AES encryption and decryption.

3 Cryptographic Module 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 6 Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
SATA-Device	Control Input	- Non-data portion of the ATA command
	Status Output	- Non-data portion of the response to the ATA command
	Data Input	- Plaintext user data - "Authentication ID" (plaintext) - "CO authentication information" (plaintext) - Challenge for device authentication - Response for host authentication - New firmware image for Update firmware service - "Key seed" (plaintext)
	Data Output	- "Key seed" (plaintext) - Challenge for host authentication - Response for device authentication
SATA-Host	Data Input Data Output	- Ciphertext user data
Power supply	Power supply	None
GPIO	Status Output	- Module status output (indicating a status, such as SSD access)
Reset	Control Input	- Reset signal
Clock	Control Input	- Clock signal

There is no control output in the Canon MFP Security Chip.

4 Roles, Services, and Authentication

4.1 Roles, Service Commands, Input and Output

This section describes the roles with corresponding service with input and output provided by the Canon MFP Security Chip.

Table 7 Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO (USER)	AES encryption DMA*2	Plaintext user data, ATA command (WRITE DMA)	Result*1, Ciphertext user data
CO (USER)	AES encryption MULTIPLE*2	Plaintext user data, ATA command (WRITE MULTIPLE)	Result*1, Ciphertext user data
CO (USER)	AES encryption SECTOR(S) *2	Plaintext user data, ATA command (WRITE SECTOR(S))	Result*1, Ciphertext user data
CO (USER)	AES encryption DMA EXT*2	Plaintext user data, ATA command (WRITE DMA EXT)	Result*1, Ciphertext user data
CO (USER)	AES encryption MULTIPLE EXT*2	Plaintext user data, ATA command (WRITE MULTIPLE EXT)	Result*1, Ciphertext user data
CO (USER)	AES encryption SECTOR(S) EXT*2	Plaintext user data, ATA command (WRITE SECTOR(S) EXT)	Result*1, Ciphertext user data
CO (USER)	AES decryption DMA*2	Ciphertext user data, ATA command (READ DMA)	Result*1, Plaintext user data
CO (USER)	AES decryption MULTIPLE*2	Ciphertext user data, ATA command (READ MULTIPLE)	Result*1, Plaintext user data
CO (USER)	AES decryption SECTOR(S) *2	Ciphertext user data, ATA command (READ SECTOR(S))	Result*1, Plaintext user data
CO (USER)	AES decryption DMA EXT*2	Ciphertext user data, ATA command (READ DMA EXT)	Result*1, Plaintext user data
CO (USER)	AES decryption MULTIPLE EXT*2	Ciphertext user data, ATA command (READ MULTIPLE EXT)	Result*1, Plaintext user data
CO (USER)	AES decryption SECTOR(S) EXT*2	Ciphertext user data, ATA command (READ SECTOR(S) EXT)	Result*1, Plaintext user data
CO	Configure secret information	Authentication ID, CO authentication information, extended ATA command (INSTALL SECRET INFO)	Result*1
CO	Output secret information	extended ATA command*4 (EXPORT CSP)	Result*1, Key seed
CO	Input secret information	Key seed, extended ATA command*4 (IMPORT CSP)	Result*1
CO	Change CO authentication information	CO authentication information, extended ATA command*4 (CONFIG SECRET INFO)	Result*1
CO	Update firmware	New firmware image, extended ATA command*4 (UPDATE BUILD IN FW)	Result*1
None	Process ATA command services*3	ATA command (General feature set/ Power Management feature set/ 48-bit Address feature set/ SMART feature set/ General Purpose Logging feature set/ Security feature set/ Long Logical Sector (LLS) feature set/	Result*1

		Trusted Computing feature set/ Sanitize Device feature set/ Software Setting Preservation (SSP) feature set)	
None	Reconfiguration	Power on	None
None	Zeroize AES key	Power off	None
None	Initialize Settings	extended ATA command*4 (INITIALIZE SETTINGS)	Result*1
None	To Config	extended ATA command*4 (TO CONFIG)	Result*1
None	Setup Mirroring	extended ATA command*4 (SETUP MIRRORING)	Result*1
None	Change Mode	extended ATA command*4 (CHANGE MODE)	Result*1
None	Self-reset	extended ATA command*4 (SELF RESET)	Result*1
None	Show status	extended ATA command*4 (GET STATUS)	Result*1, current status and the error factor if an error occurs
None	Get FW Version Info	extended ATA command*4 (GET VERSION INFO)	Result*1, version of the Firmware module
None	Get HW Version Info	extended ATA command*4 (CHECK CHIP VERSION)	Result*1, version of the Hardware module
None	Zeroize secret information	extended ATA command*4 (ERASE SECRET INFO)	Result*1
None	Sanitization	extended ATA command*4 (CHANGE TO NONFIPS)	Result*1
None	Prepare Sanitization	extended ATA command*4 (PREPARE CHANGE TO NONFIPS)	Result*1
None	Send challenge for Device Identification and Authentication	Challenge, extended ATA command*4 (SEND CHA1)	Result*1
None	Request response for Device Identification and Authentication	extended ATA command*4 (REQUEST RES1)	Result*1, Response
None	Request challenge for Device Identification and Authentication	extended ATA command*4 (REQUEST CHA2)	Result*1, Challenge
None	Device Identification and Authentication	Response, extended ATA command*4 (SEND RES2)	Result*1
None	Request challenge for C1 authentication	extended ATA command*4 (REQUEST CHA C1)	Result*1, Challenge
None	C1 authentication	Response, extended ATA command*4 (SEND RES C1)	Result*1
None	Request challenge for C3 authentication	extended ATA command*4 (REQUEST CHA C3)	Result*1, Challenge
None	C3 authentication	Response, extended ATA command*4 (SEND RES C3)	Result*1
None	Request challenge for C4 authentication	extended ATA command*4 (REQUEST CHA C4)	Result*1, Challenge
None	C4 authentication	Response, extended ATA	Result*1

		command*4 (SEND RES C4)	
None	Request challenge for C5 authentication	extended ATA command*4 (REQUEST CHA C5)	Result*1, Challenge
None	C5 authentication	Response, extended ATA command*4 (SEND RES C5)	Result*1
None	Request challenge for C6 authentication	extended ATA command*4 (REQUEST CHA C6)	Result*1, Challenge
None	C6 authentication	Response, extended ATA command*4 (SEND RES C6)	Result*1
None	Self-test	Power on	None

*1 Result indicates success or failure as a result of executing the service.

*2 AES encryption/decryption services perform different methods of data transfer to the storage device according to the ATA command (i.e., write a single block or multiple blocks, etc.). No matter which command is executed, the module provides same function (data encryption/decryption).

*3 The Process ATA Command services sends non-cryptographic-related ATA commands (as defined in the ANSI INCITS 452 standard document (ATA 8)) received from a host to storage, and sends a response from storage to the host. The Canon MFP Security Chip has a service corresponding to each ATA command, and these services are collectively referred to as the Process ATA Command services.

*4 The extended ATA command is proprietary to the Canon MFP Security Chip.

4.2 Roles

The Canon MFP Security Chip supports two distinct operator roles, CO(USER) and CO. These roles are the "Crypto Officer Role" specified in ISO/IEC 19790 Section 7.4.2. The Canon MFP Security Chip has no "User Role". CO(USER) serves to allow connection to the Host. CO (USER) is allowed use of the AES encryption/decryption services as described in Table 10. CO (USER) is a role that undertakes the CO Role. Further, CO includes C1, C3, C4, C5, and C6. C1 can configure the secret information, C3 can export the secret information, C4 can import the secret information, C5 can change the secret information, and C6 can update the firmware of the Canon MFP Security Chip, respectively. The following table shows the authentication method of 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 9 Roles and Authentication

Role	Authentication Method	Authentication Strength
CO (USER)	CO(USER) is authenticated by “Device Identification and Authentication” service. The method is role-based authentication by shared secret. See Section 4.3 for more information.	32-byte
CO	CO is authenticated by C1, C3, C4, C5, or C6 authentication service. The method is role-based authentication by shared secret. It is possible to set different authentication information for C1, C3, C4, C5, and C6. The authentication method and specification of each authentication information are the same and are referred to as CO authentication. See Section 4.3 for more information.	32-byte

4.3 Operator Authentication

Before providing any of the services associated with CO(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(USER) authentication
  Uses challenge-response authentication based on Authentication ID defined in 9.1. CO(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
  Uses challenge-response authentication based on CO authentication information defined in section 9.1. 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 CO authentication information, and then calculating hash values.

The hash algorithm used in CO (USER) and CO authentication is SHS as described in # 4547 of Table 5, and SHA-256 is used to calculate the hash value.
For the shared secret, both CO authentication and CO(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 can perform CO authentication every 60 milliseconds, and CO(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.

4.4 Services

This section describes the cryptographic services provided by the Canon MFP Security Chip.

The Access rights shown in the table mean the access rights to Keys and/or SSPs and are defined as follows:

G = Generate: The module generates or derives the SSP.
R = Read: The SSP is read from the module (e.g., the SSP is output).
W = Write: The SSP is updated, imported, or written to the module.
E = Execute: The module uses the SSP in performing a cryptographic operation.
Z = Zeroise: The module zeroises the SSP.

Zeroisation of SSP is performed by overwriting the area where corresponding SSP is stored with 0 or 1.
See Table 9 for the method used for authentication to each operator role.

Table 10 Approved Services

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
AES encryption DMA	Encrypts and writes data to the storage device(s).	AES Encryption	AES cryptographic keys	CO (USER)	E	command response
AES encryption MULTIPLE	Encrypts and writes data to the storage device(s).	AES Encryption	AES cryptographic keys	CO (USER)	E	command response

AES encryption SECTOR(S)	Encrypts and writes data to the storage device(s).	AES Encryption	AES cryptographic keys	CO (USER)	E	command response
AES encryption DMA EXT	Encrypts and writes data to the storage device(s).	AES Encryption	AES cryptographic keys	CO (USER)	E	command response
AES encryption MULTIPLE EXT	Encrypts and writes data to the storage device(s).	AES Encryption	AES cryptographic keys	CO (USER)	E	command response
AES encryption SECTOR(S) EXT	Encrypts and writes data to the storage device(s).	AES Encryption	AES cryptographic keys	CO (USER)	E	command response
AES decryption DMA	Reads data from the storage device and decrypts.	AES Decryption	AES cryptographic keys	CO (USER)	E	command response
AES decryption MULTIPLE	Reads data from the storage device and decrypts.	AES Decryption	AES cryptographic keys	CO (USER)	E	command response
AES decryption SECTOR(S)	Reads data from the storage device and decrypts.	AES Decryption	AES cryptographic keys	CO (USER)	E	command response
AES decryption DMA EXT	Reads data from the storage device and decrypts.	AES Decryption	AES cryptographic keys	CO (USER)	E	command response
AES decryption MULTIPLE EXT	Reads data from the storage device and decrypts.	AES Decryption	AES cryptographic keys	CO (USER)	E	command response
AES decryption SECTOR(S) EXT	Reads data from the storage device and decrypts.	AES Decryption	AES cryptographic keys	CO (USER)	E	command response
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 CKG	Authentication ID, CO authentication information AES cryptographic keys Key seed DRBG seed DRBG internal state	CO	W G G/E G/E/Z E/G	command response
Output secret information	Key seed is output in plaintext form from the cryptographic module.	-	Key seed	CO	R	command response
Input secret information	Replaces the key seed, with the secret information received from the host system in plaintext form.	-	Key seed AES cryptographic keys	CO	E/W G	command response
Change CO authentication information	Modifies CO authentication information.	-	CO authentication information	CO	W/Z	command response
Update firmware	Updates firmware of the cryptographic module except for the boot loader. See section 5.	RSA SHA-256	Vendor public key CO authentication information, key seed, authentication ID, DRBG internal state, AES cryptographic	CO	E Z	command response

			keys			
Process ATA command services	Sends non-encryption-related ATA commands received from the host to the storage and sends a response from the storage to the host.	-	N/A	None	N/A	command response
Reconfiguration	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 CKG RSA SHA-256	AES cryptographic keys	None	G	Show status
			Key seed		E	
			DRBG seed		G/E/Z	
			DRBG internal state		G	
			Vendor public key		E	
Zeroize AES key	Clears the cryptographic key stored in volatile memory.	-	AES cryptographic keys	None	Z	The module is powered-off.
Initialize Settings	Initializes the non-security relevant settings of the Canon MFP Security Chip. After initializing, the module automatically resets.	Hash_DRBG CKG RSA SHA-256	AES cryptographic keys	None	G	command response
			Key seed		E	
			DRBG seed		G/E/Z	
			DRBG internal state		G	
			Vendor public key		E	
To Config	Clears the CO(USER) authentication state and transitions to the Config state.	-	N/A	None	N/A	command response
Setup Mirroring	Configures the behavior settings of the Canon MFP Security Chip for mirroring mode.	-	N/A	None	N/A	command response
Change mode	Configures the behavior settings of the Canon MFP Security Chip for mirroring mode.	-	N/A	None	N/A	command response
Self-reset	Performs self-reset and self-tests.	Hash_DRBG CKG RSA SHA-256	AES cryptographic keys	None	G	Show status
			Key seed		E	
			DRBG seed		G/E/Z	
			DRBG internal state		G	
			Vendor public key		E	
Show status	Shows the current status of the module, including status indicators in response to request of some services. If the service resulted in an error, the cause of the error is also shown.	-	N/A	None	N/A	command response
Get FW Version Info	Shows the version of the cryptographic Firmware module.	-	N/A	None	N/A	command response
Get HW Version Info	Shows the version of the cryptographic Hardware module.	-	N/A	None	N/A	command response
Zeroize secret information	Clears (zeroizes) secret information.	-	Key seed, authentication ID,	None	Z	command response

			AES cryptographic keys			
Sanitization	Clears (zeroizes) all CSPs and transitions to non-Compliant state.	-	CO authentication information, key seed, Authentication ID, DRBG internal state, AES cryptographic keys	None	Z	command response
Prepare Sanitization	Prepares to use “Sanitization” service.	-	None	None	N/A	command response
Send challenge for Device Identification and Authentication	Provides a challenge value for Device Identification and Authentication from the host system to the module.	-	Challenge-response	None	W	command response
Request response for Device Identification and Authentication	Provides a response value for Device Identification and Authentication from the module to the host system.	SHA-256	Authentication ID	None	E	command response
			Challenge-response		G/Z/R	
Request challenge for Device Identification and Authentication	Provides a challenge value for Device Identification and Authentication from the module to the host system.	Hash_DRBG	DRBG internal state	None	E/W	command response
			Challenge-response		G/W/R	
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.	SHA-256	Authentication ID	None	E	command response
			Challenge-response		Z/W	
Request challenge for C1 authentication	Provides a challenge value for C1 authentication from the module to the host system.	Hash_DRBG	DRBG internal state	None	E/W	command response
			Challenge-response		G/R	
C1 authentication	Performs C1 authentication with challenge-response authentication. The Canon MFP Security Chip provides services to CO only when authentication succeeds.	SHA-256	CO authentication information	None	E	command response
			Challenge-response		Z/W	
Request challenge for C3 authentication	Provides a challenge value for C3 authentication from the module to the host system.	Hash_DRBG	DRBG internal state	None	E/W	command response
			Challenge-response		G/R	

C3 authentication	Performs C3 authentication with challenge-response authentication. The Canon MFP Security Chip provides services to CO only when authentication succeeds.	SHA-256	CO authentication information Challenge-response	None	E Z/W	command response
Request challenge for C4 authentication	Provides a challenge value for C4 authentication from the module to the host system.	Hash_DRBG	DRBG internal state Challenge-response	None	E/W G/R	command response
C4 authentication	Performs C4 authentication with challenge-response authentication. The Canon MFP Security Chip provides services to CO only when authentication succeeds.	SHA-256	CO authentication information Challenge-response	None	E Z/W	command response
Request challenge for C5 authentication	Provides a challenge value for C5 authentication from the module to the host system.	Hash_DRBG	DRBG internal state Challenge-response	None	E/W G/R	command response
C5 authentication	Performs C5 authentication with challenge-response authentication. The Canon MFP Security Chip provides services to CO only when authentication succeeds.	SHA-256	CO authentication information Challenge-response	None	E Z/W	command response
Request challenge for C6 authentication	Provides a challenge value for C6 authentication from the module to the host system.	Hash_DRBG	DRBG internal state Challenge-response	None	E/W G/R	command response
C6 authentication	Performs C6 authentication with challenge-response authentication. The Canon MFP Security Chip provides services to CO only when authentication succeeds.	SHA-256	CO authentication information Challenge-response	None	E Z/W	command response
Self-test	Performs self-tests.	Hash_DRBG CKG RSA SHA-256	AES cryptographic keys Key seed DRBG seed DRBG internal state Vendor public key	None	G E G/E/Z G E	Show status

5 Software/Firmware Security

At the start-up, the Canon MFP Security Chip perform the boot loader integrity test using 32-bit CRC and an integrity test of the firmware (ELF format) 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 except for the boot loader by completely replacing it using Update firmware service. 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 the firmware data, the Canon MFP Security Chip verifies the received digital signature of RSA 2048-bit by public key that is embedded in the current firmware. In case the verification succeeds, the Canon MFP Security Chip zeroizes CSPs, returns a success status and switches to non-Compliant state. 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. After the new firmware becomes effective, the module becomes another one, and new validation is needed. 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. The CO can verify the updated firmware version by Get FW Version Info service. The firmware version is displayed, consisting of the updated part and the unupdated boot loader.

6 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.

7 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.

Table 11 Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
All components are enclosed in a package and sealed by opaque plastic mold (coating).	Before use	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.

8 Non-invasive Security

The Canon MFP Security Chip does not implement a non-invasive security technology to protect SSPs from non-invasive attacks.

9 Sensitive Security Parameters Management

9.1 Definition of Sensitive Security Parameters (SSPs)

The following tables show CSPs, and PSPs 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.
Since the establishment method does not apply to all CSPs, the description is omitted.

Table 12 SSPs

Key/SSP Name/ Type	Strength	Security Function and Cert. Number*	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & related keys
AES cryptographic keys (CSP)	128 bits, 256 bits	XTS-AES	Generated by using CKG shown in Table 5.	N/A	N/A	Plaintext in RAM	"Zeroize AES key", "Zeroize secret information", "Update firmware" and "Sanitization" "Zeroize AES key" implicitly performs zeroisation. Other services explicitly perform zeroisation.	"Symmetric Key" for encryption/decryption
Key seed (CSP)	256 bits	Hash_DRBG	Generated by the instantiation function of Hash_DRBG in Table 5 by "Configure secret information" in CO Role, that uses DRBG seed described below.	Import/Export: 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 seed output by the "Output secret information" service from this module is input.	N/A	Plaintext in Flash	"Zeroize secret information", "Update firmware" and "Sanitization" All services explicitly perform zeroisation.	Used in AES Cryptographic key generation
Authentication ID (CSP)	Refer to Section 4.3 of [SP].	N/A	N/A	Import: Set by "Configure secret information" service.	N/A	Plaintext in Flash	"Zeroize secret information", "Update firmware" and "Sanitization" All services	Used for mutually authenticating the Canon MFP Security Chip and the host system, for Device Identification and

							explicitly perform zeroisation.	Authentication.
CO authentication information (CSP)	Refer to Section 4.3 of [SP].	N/A	N/A	Import: Set by “Configure secret information” service and “Change CO authentication 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	Plaintext in Flash	“Sanitization”, “Change CO authentication information” and “Update firmware” All services explicitly perform zeroisation.	Information for CO authentication.
DRBG internal state (CSP)	256 bits	N/A	It is generated by the instantiation function of Hash_DRBG in Table 5, that uses DRBG seed described below.	N/A	N/A	Plaintext in RAM	“Sanitization”, “Zeroize AES key” and “Update firmware” "Zeroize AES key" implicitly performs zeroisation. Other services explicitly perform zeroisation.	Used for challenge generation, for “Device Identification and Authentication”, “C1 Authentication”, “C3 authentication”, “C4 authentication”, “C5 authentication” and “C6 authentication” services. And it is updated whenever the generation function of Hash_DRBG is called.
DRBG seed (CSP)	256 bits	N/A	DRBG seed is generated by combining random numbers from Chapter 3.4 ENT (P) that are generated as Entropy Input or Nonce.	N/A	N/A	Plaintext in RAM	“Configure secret information” and “Reconfiguration” All services implicitly perform zeroisation.	Used for key seed generation. Used for DRBG internal state generation.
Challenge-response (PSP)	N/A	Hash_DRBG SHS	Challenge is generated for “Device Identification and Authentication” and “CO authentication”. Response is	Import: a challenge code is input into the module at "Send challenge for Device Identification and Authentication" service, and response codes are input into the module	N/A	Plaintext in RAM. Temporarily stored during “Device Identification and Authenti	“Device Identification and Authentication”, “C1 authentication”, “C3 authentication”, “C4 authenticati	Used for “CO authentication” and “Device Identification and Authentication”.

			generated for “Device Identification and Authentication”.	at "C1 authentication”, “C3 authentication” service, “C4 authentication” service, “C5 authentication” service, “C6 authentication” service, and "Device Identification and Authentication" service. Export: a response code is output from the module at "Request response for Device Identification and Authentication" service, and challenge codes are output from the module at "Request challenge for Device Identification and Authentication" service, "Request challenge for C1 authentication" service, "Request challenge for C3 authentication" service, "Request challenge for C4 authentication" service, "Request challenge for C5 authentication" service and "Request challenge for C6 authentication" service.		cation”, “C1 authentication”, “C3 authentication”, “C4 authentication”, “C5 authentication” and “C6 authentication”	on”, “C5 authentication”, “C6 authentication” and “Request response for Device Identification and Authentication” All services implicitly perform zeroisation	
Vendor public key (PSP)	[Strength] 112 bits [Length] 2048 bits	RSA	Stored when manufacturing the Canon MFP Security Chip.	Import: Set by “Update firmware” service.	N/A	Plaintext in Flash	N/A	Used for verification of firmware.

* See Table 5 for algorithm Certification number.

The RBG entropy source is ENT (P). ENT (P) is used in generating the seed value for approved Hash_DRBG shown in Table 5. The Table shows entropy source specification.

Table 15 Non-Deterministic Random Number Generation Specification

Entropy sources	Minimum number of bits of entropy	Details
ENT (P) ring oscillator embedded in the Canon MFP Security Chip	5 bits per 8 bits	Minimum entropy provided by the ENT (P) is 5 bits per 8 bits. Total 896 bits random data is provided by ENT (P) to Hash_DRBG for key generation, and it includes 560 bits (=896 bits x 5 bits/8 bits) entropy.

If the entropy source deteriorates to the point that it can no longer guarantee the generation of a sufficient amount of entropy, the Canon MFP Security Chip transitions to an error state as the result of the Conditional Self-test shown in 11.2. To recover from the error condition, it is necessary to contact the vendor to repair the Canon MFP security chip.

10 Self-Tests

The Canon MFP Security Chip has pre-operational self-test and conditional self-test functions. Table 16 shows tests to be performed in self-test.

Table 16 Self-test

Test item	Test method	Test type	Parameter	Condition
Firmware Integrity Test	Firmware integrity test uses RSA 2048-bit digital signature to verify the firmware except for the boot loader	Pre-operational (software/firmware integrity test)	public key, 2048-bit RSA digital signature	performed automatically when the power is turned on
Boot Loader Integrity Test	Boot Loader integrity test using CRC Check(32bit)	Pre-operational (software/firmware integrity test)	CRC	same as above
AES Encryption	Known answer test (XTS)	Conditional (Cryptographic algorithm test)	256-bit key	same as above
AES Decryption	Known answer test (XTS)	Conditional (Cryptographic algorithm test)	256-bit key	same as above
Hash_DRBG	Known answer test (instantiate/generate)	Conditional (Cryptographic algorithm test	None	same as above
SHA-256	Known answer test	Conditional (Cryptographic algorithm test)	None	same as above
RSA signature	Known answer test using 2048-bit RSA digital signature	Conditional (Cryptographic algorithm test)	2048-bit RSA digital signature	same as above
Hash_DRBG	Continuous random bit generator test	Conditional (Cryptographic algorithm test)	None	performed before using Hash_DRBG
Entropy Source Test	Perform the Repetition Count Test and Adaptive Proportion Test as "Start-up health tests" and "Continuous health tests" as specified in SP 800-90B.	Conditional (Cryptographic algorithm test)	None	performed automatically when the power is turned on
		Conditional (Cryptographic algorithm test)	None	performed before seed generation
CSP Integrity Test	Secret information integrity test using CRC Check (32 bits)	Conditional (Critical functions test)	CRC	performed when secret information is read
Firmware Load Test	Firmware verification with 2048-bit RSA digital signature when loading firmware	Conditional (software/firmware load test)	public key, 2048-bit RSA digital signature	performed when updating the firmware

10.1 Pre-operational Self-test

When the power is turned on, the Canon MFP Security Chip performs pre-operational self-test automatically. It performs the firmware integrity test shown in Table 16 as the pre-operational self-test. Cryptographic algorithm tests are also conducted since the firmware integrity test uses RSA signature verification and SHA-256.

In case the result of the firmware integrity test and cryptographic algorithm tests 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 pre-operational self-test can be performed by resetting the Canon MFP Security Chip.

10.2 Conditional Self-test

The Canon MFP Security Chip provides cryptographic algorithm tests, Hash_DRBG continuous random bit generator test, entropy source test, CSP integrity test, and test for firmware loading as the conditional self-test shown in Table 16.
The cryptographic algorithm tests are conducted at the same time as the pre-operational self-test, as described in 11.1.
Hash_DRBG continuous random bit generator test is conducted every time before using the Hash_DRBG pseudo-random number generator.
Entropy source tests are conducted as conditional cryptographic algorithm tests when performing start-up (i.e., as start-up health tests) and seed generation (i.e., as continuous health tests).
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 16 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 16 is performed when updating the firmware.

In case the result of one of the cryptographic algorithm tests 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 except the cryptographic algorithm tests and firmware load test, it is possible to recover from an error state by transitioning to non-Compliant state using “Sanitization” service. The status of the error state can be obtained by using Show status 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. The result can be obtained by using Show status service.
No bypass test is implemented because the Canon MFP Security Chip does not have a bypass function.

11 Life-cycle Assurance

11.1 Initial Set-Up

The Canon MFP Security Chip operates in non-Compliant state when installed. In this state, the SSPs are not in the Canon MFP Security Chip and no security functions can be performed. To use the Canon MFP Security Chip in Approved mode, the CO shall perform the following.

The CO first runs "Initialization operation" by the [PREPARE INSTALL] extended ATA command in non-Compliant state, and the Canon MFP Security Chip transitions to Approved mode after conducting pre-operational tests and cryptographic algorithm tests described in Section 10. 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 32 Byte value which is written in the specified position of the setting command is set as the CO authentication information. It should not be easily 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 by the [GET STATUS] extended ATA command 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 Approved mode or non-Compliant state.

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. Although it cannot be switched, key sizes can be re-set after erasing CSPs by the [ERASE SECRET INFO] command. In this case, user data will not be migrated.

11.2 Sanitization

The Canon MFP Security Chip zeroizes all CSPs and switches to non-Compliant state by using the “Sanitization” service.

11.3 Guidance Documents

Provide the following private document as Administrator guidance and non-Administrator guidance.

- Canon MFP Security Chip Firmware specification

12 Mitigation of Other Attacks

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

END