FIPS 140-3 Non-Proprietary Security Policy for:

KIOXIA FIPS TC58NC1132GTC Crypto Sub-Chip

KIOXIA CORPORATION

Rev 2.4.0

Section 1 - General

This document explains precise specification of the security rules about KIOXIA FIPS TC58NC1132GTC Crypto Sub-Chip. The Cryptographic Module (CM) meets the requirements of FIPS 140-3 Security Level 2 Overall. The Table below shows the security level detail.

Section	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
Overall Level	**2**

Table 1 - Security Levels

This document is non-proprietary and may be reproduced in its original entirety.

Section 1.1 - Acronyms

AES	Advanced Encryption Standard
CM	Cryptographic Module
SSP	Sensitive Security Parameter
DRBG	Deterministic Random Bit Generator
HMAC	The Keyed-Hash Message Authentication code
KAT	Known Answer Test
POST	Pre-Operational Self-Test
CAST	Cryptographic Algorithm Self-Test
PSID	Printed SID
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm
SID	Security ID
TCG	Trusted Computing Group
LBA	Logical Block Address

Section 2 – Cryptographic Module Specification

KIOXIA FIPS TC58NC1132GTC Crypto Sub-Chip (listed in Section2.1 Product Version) is used for solid state drive data security. The CM is a single chip hardware module implemented as a sub-chip compliant with IG 2.3.B in the TC58NC1132GTC 0003 SoC (see Figure 1 in Section 7). Overall Security Rating of the CM is Level2 (See Table 1 in Section 1 for individual security area levels). The CM is embedded in TCG Enterprise compliant solid state drive controllers which provides user data encryption/decryption through build-in HW engines. The CM is responsible for providing key management, access control of stored user data, and various cryptographic algorithm for the solid state drive.

The CM has multiple cryptographic services using approved algorithms, but they do not support the degraded operation. The physical boundary of the CM is the TC58NC1132GTC 0003 SoC and the logical boundary of the CM is TC58NC1132GTC CRPT module.

The CM has one approved mode of operation and CM is always in approved mode of operation after initial operations are performed (See Section 11). In approved mode, the CM provides services defined in Table 7 in Section 4.2.

Section 2.1 – Product Version

The CM are validated with the following versions:

Physical single-chip	The sub-chip cryptographic subsystem soft circuitry core	The associated firmware
TC58NC1132GTC 0003	TC58NC1132GTC CRPT module 0001	SC02AS

Table 2 - Cryptographic Module Tested Configuration

Section 2.2 – Security Functions

The CM executes following approved algorithms:

CAVP Cert	Algorithm and Standard	Mode/ Method	Description/Key Size(s)/ Key Strength(s)	Use/Function
#C1925	AES256 (FIPS 197 / SP800-38A)	CBC	Key Size: 256 bits/ Key Strength: 256 bits	Data Encryption/ Decryption
#C1925	SHA256 (FIPS 180-4)	N/A	N/A	Hashing messages

#C1925	HMAC-SHA256 (FIPS 198-1)	N/A	Key Size: 256 bits/ Key Strength: 256 bits	Message Authentication Code
#C2009	RSASSA-PKCS#1-v1_5 (FIPS 186-4)	N/A	Key Size: 2048 bit/ Key Strength: 112 bits	Signature verification
#C2002	Hash_DRBG (SP800-90A Rev.1)	N/A	Hash based: SHA256	Deterministic Random Bit Generation
#C2001	KBKDF (SP800-108 Revised)	Counter	MACs: HMAC-SHA256/ Key Size: 256 bits/ Key Strength: 256 bits	Key derivation
#C1925	KTS (IG D.G)	N/A	Combination of AES256 CBC Mode and HMAC-SHA256 / Key Size: 256 bits/ Key Strength: 256 bits	Key Transport Scheme
Vendor Affirmation	CKG (SP800-133 Rev.2)	N/A	Methods described in section 4 of the SP800-133 Rev.2	Cryptographic Key Generation
ENT(P)	Entropy Source (SP800-90B)	N/A	N/A	Hardware RNG used to seed the approved Hash_DRBG.

Table 3 - Approved Algorithm

The CM does not implement any Non-Approved Algorithms Allowed in the Approved Mode of Operation.

Section 2.3 – Module Configuration

Overview block diagram of the CM is shown below.

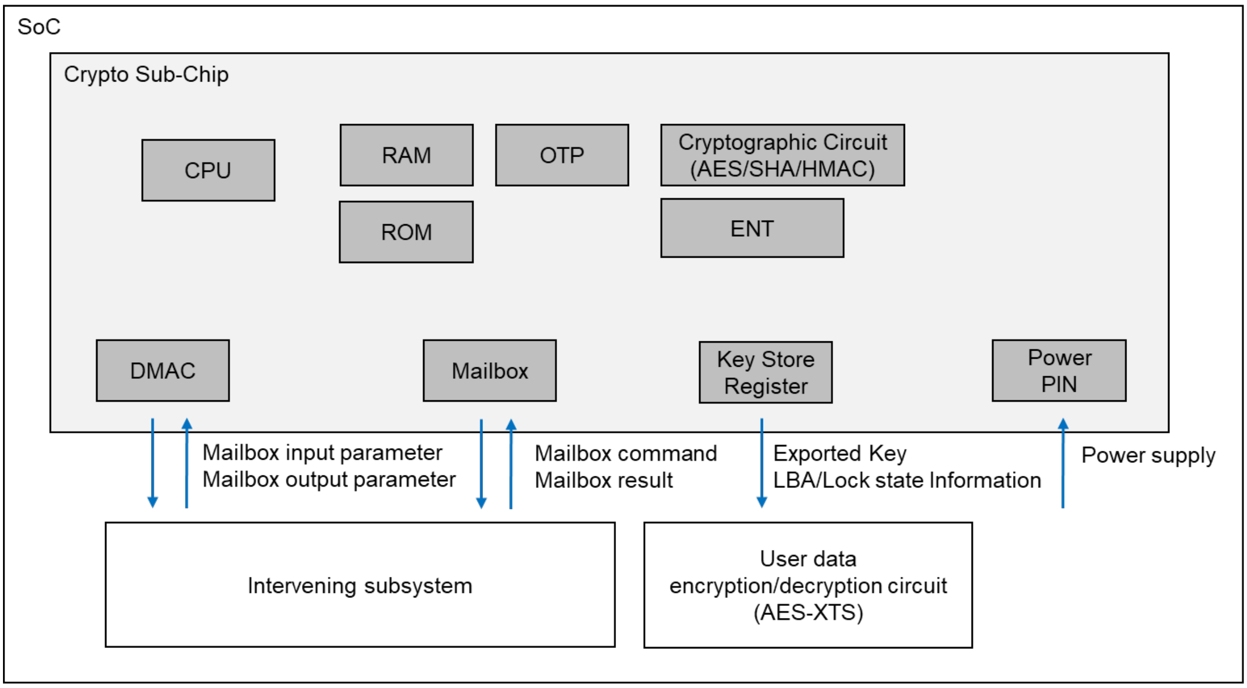

Figure 1 – Configuration of the cryptographic module and peripheral components

Components of the CM is shown with gray background include processor and memories (volatile and non-volatile memory) and HW circuitry for cryptographic processing. Physical ports bordering outside the CM's boundary and the data passing over them are also indicated (see Section 3 for details on physical ports and interfaces).

Section 3 – Cryptographic Module Interface

Physical port	Logical Interface	Data that passes over port/interface
Mailbox DMAC	Data Input	Mailbox input parameter.
Mailbox DMAC Key Store Register	Data Output	Mailbox output parameter. Encryption key for use of other functional subsystems. Range information.
Mailbox	Control Input	Mailbox command information.
Mailbox	Status Output	Mailbox command result.
Power PIN	Power Input	Power

Note 1: Control output is omitted in the table above because the CM does not implement this type of interface.

Note 2: Range information includes LBA and Lock state information.

Table 4 - Ports and Interface

Section 4 – Roles Services and Authentication

The relation between Roles and Services in this CM is shown below.

Role	Service	Input	Output
FIPS Crypto Officer (EraseMaster)	Cryptographic Erase Set PIN (for EraseMaster)	Mailbox command	Mailbox command result Exported encryption key Range information
FIPS Crypto Officer (SID)	Download Port Lock/Unlock Firmware Download[1] Set PIN (for SID)	Mailbox command	Mailbox command result
FIPS Crypto Officer (BandMaster0)	Band Lock/Unlock (for GlobalRange) Set Band Position and Size (for GlobalRange) Set PIN (for BandMaster0)	Mailbox command	Mailbox command result Exported encryption key Range information
FIPS Crypto Officer (BandMaster1)	Band Lock/Unlock (for Band1) Set Band Position and Size (for Band1) Set PIN (for BandMaster1)	Mailbox command	Mailbox command result Exported encryption key Range information
…	…	…	…
FIPS Crypto Officer (BandMaster64)	Band Lock/Unlock (for Band64) Set Band Position and Size (for Band64) Set PIN (for BandMaster64)	Mailbox command	Mailbox command result Exported encryption key Range information
None	Firmware Verification Random Number Generation Show Status Zeroisation	Mailbox command	Mailbox command result
	Reset	Power	N/A

Table 5 - Roles, Service Commands, Input and output

Section 4.1 – Roles and Authentication

This section describes roles, authentication method, and strength of authentication.

Role Name	Role Type	Type of Authentication	Authentication	Authentication Strength	Multi Attempt strength
EraseMaster	Crypto Officer	Role	PIN	1 / 2^{64} < 1 / 1,000,000	30 / 2^{64} < 1 / 100,000
SID	Crypto Officer	Role	PIN	1 / 2^{64} < 1 / 1,000,000	30 / 2^{64} < 1 / 100,000
BandMaster0	Crypto Officer	Role	PIN	1 / 2^{64} < 1 / 1,000,000	30 / 2^{64} < 1 / 100,000
BandMaster1	Crypto Officer	Role	PIN	1 / 2^{64} < 1 / 1,000,000	30 / 2^{64} < 1 / 100,000
…	…	…	…	…	…
BandMaster64	Crypto Officer	Role	PIN	1 / 2^{64} < 1 / 1,000,000	30 / 2^{64} < 1 / 100,000

Table 6 - Identification and Authentication Policy

[1] “Firmware Download” service is controlled by SID role and signature of downloaded external firmware is verified (RSASSA-PKCS#1-v1_5).

The CM performs role authentication by comparing whether the PIN entered by the user matches the information stored inside the CM. PINs are hashed with SHA-256 to store them on the CM. The PIN entered by the user is hashed and compared to the stored PIN hash.

PINs can be changed by executing the Set PIN Service (see Section4.2) with appropriate roles authenticated. The CM refuses to set a PIN less than 8 bytes, and responds with an error if such a setting is attempted. Therefore, the probability that a random attempt will succeed is $1 / 2^{64} < 1 / 1,000,000$ (the CM accepts any value (0x00-0xFF) as each byte of PIN). The CM waits 2sec when authentication attempt fails, so the maximum number of authentication attempts is 30 times in 1 min. Consequently, the probability that random attempts in 1min will succeed is $30 / 2^{64} < 1 / 100,000$.

Section 4.2 – Services

This section describes services which the CM provides.

Service	Description	Approved Security Function	Keys and/or SSPs	Role(s)	Access rights to Keys and/or SSPs[2]	Indicator
Band Lock/Unlock	Lock or unlock setting for read/ write of user data in a band.	KBKDF	KDK MEKs	BandMaster0 … BandMaster64	E G, R, Z	Mailbox command result
		HMAC-SHA256	System MAC Key		E	
Cryptographic Erase	Erase user data (in cryptographic means) by changing the key that derives the data encryption key.	CKG (Hash_DRBG)	DRBG Internal Value KDK	EraseMaster	E G, Z	Mailbox command result
		KBKDF	KDK MEKs		E G, R, Z	
		HMAC-SHA256	System MAC Key		E	
		AES256-CBC	System Enc Key		E	
		KTS	KDK		W, R	
Download Port Lock/Unlock	Lock / unlock firmware download.	N/A	N/A	SID	N/A	Mailbox command result
Firmware Verification	Digital signature verification for firmware outside the CM.	RSASSA-PKCS#1-v1_5	Public Key embedded on the CM's code	None	E	Mailbox command result
Firmware Download	Download a firmware image[3].	SHA256	PubKey1	SID	W, E	Mailbox command result
		RSASSA-PKCS#1-v1_5	PubKey1		E	

[2] The letters (G, R, W, E, Z) mean Generate, Read, Write, Execute and Zeroise respectively.

[3] Only the CMVP validated version is to be used

Random Number Generation	Provide a random number generated by the CM.	Hash_DRBG	DRBG Internal Value	None	E	Mailbox command result
Set Band Position and Size	Set the location and size of the band.	CKG (Hash_DRBG)	DRBG Internal Value KDK	BandMaster0 … BandMaster64	E G, Z	Mailbox command result
		KBKDF	KDK MEKs		E G, R, Z	
		HMAC-SHA256	System MAC Key		E	
		AES256-CBC	System Enc Key		E	
		KTS	KDK		W, R	
Set PIN	Set PIN (authentication data).	SHA256	PINs	EraseMaster SID BandMaster0 … BandMaster64[4]	W, E	Mailbox command result
		HMAC-SHA256	System MAC Key		E	
		AES256-CBC	System ENC Key		E	
		KTS	PINs		W, R	
Show Status	Report status of the CM and versioning information.	N/A	N/A	None	N/A	Mailbox command result
Zeroisation	Erase SSPs.	N/A	RKey	None[5]	Z	Mailbox command result
			KDK		Z	
			PINs		Z	
			System MAC Key		Z	
			System Enc Key		Z	
			DRBG Internal Value		Z	
Reset	Power-OFF: Delete SSPs in RAM.	N/A	System MAC Key	None	Z	N/A
			System Enc Key		Z	
			KDK		Z	
			PINs		Z	
			DRBG Internal Value		Z	
			PubKey1		Z	
	Power-ON: Runs various self-tests to be performed at power-on (POSTs, CASTs, Firmware Load test) and generate / import some SSPs.	RSASSA-PKCS#1-v1_5	PubKey1		W, E	
		KBKDF	Rkey System MAC Key System Enc Key		E G G	
		Entropy Source	DRBG Seed		G	
		Hash_DRBG	DRBG Seed DRBG Internal Value		E, Z G	
		HMAC-SHA256	System MAC Key		E	
		AES256-CBC	System Enc Key		E	
		KTS	KDK PINs		W W	

[4] Each role can set a PIN for themselves only.

[5] Need to input PSID, which is public drive-unique value used for the zeroisation service.

	Derive MEKs if the corresponding band has been unlocked by the appropriate roles.	KBKDF	KDK MEKs		E G, R, Z	

Note 1: "CKG(Hash_DRBG)" means direct use of Hash_DRBG output as a key.

Note 2: "PINs" in the above table means "SID/BandMaster(s)/EraseMaster PINs".

Table 7 - Approved services

Section 5 – Software/Firmware Security

Firmware Security of components in this CM is shown below.

ROM Code:
・ Form of the executable code: ELF format
・ Integrity verification method: 32bit CRC
・ Method for integrity test on demand: Power cycling

Firmware image (User Code):
・ Form of the executable code: ELF format
・ Integrity verification method: Approved signature verification (see table 3)
・ Method for integrity test on demand: Power cycling

Section 6 – Operational Environment

Operational Environment requirements are not applicable because the CM does not employ operating systems and operates in a non-modifiable environment that is the CM cannot be modified and no code can be added or deleted.

Section 7 – Physical Security

The CM is a sub-chip enclosed in a single chip that is an opaque package. Gathering information of the module's internal construction or components is impossible without forcing the package to open. In this case, it is confirmed package damage as a tamper-evidence. Operators of the CM can ensure that the physical security is maintained to confirm the package has no obvious attack damage. If the operator discovers tamper evidence, the CM should be removed.

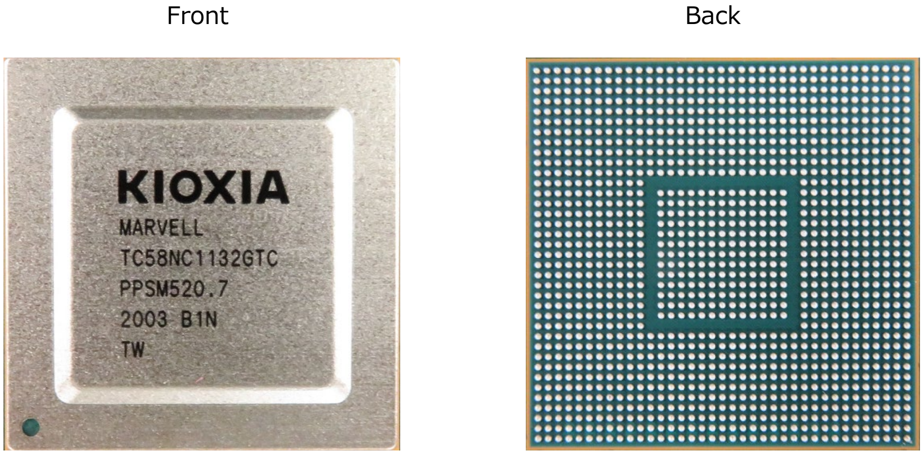

Figure 2 - TC58NC1132GTC 0003 SoC

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Detail
Passivated opaque package	Every month or every two months	Confirmation that there is no visual damage

Table 8 - Physical Security Inspection Guidelines

Section 8 – Non-invasive security

The CM does not apply Non-invasive security.

Section 9 – Sensitive security parameter management

The CM uses keys and SSPs in the following table.

Key/SSP Name/Type	Strength (bit)	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use & related keys
Critical Security Parameters (CSPs)								
RKey	256	KBKDF (#C2001)	Hash_DRBG (Method SP800-133 Rev.2 Section 4)	N/A	Manufacturing	Plaintext in OTP	Explicit Zeroisation service	Derivation of System Enc Key and System MAC Key
System Enc Key	256	AES-CBC (#C1925)	KDF in Counter Mode	N/A	Power-On	Plaintext in RAM	Explicit Zeroisation	Data Encryption / Decryption for KTS

							service Implicit Power-Off	
System MAC Key	256	HMAC (#C1925)	KDF in Counter Mode	N/A	Power-On	Plaintext in RAM	Explicit Zeroisation service Implicit Power-Off	Message Authentication Code generation and verification for KTS
KDK	256	KBKDF (#C2001)	Hash_DRBG (Method SP800-133 Rev.2 Section 4)	Imported and Exported by KTS (see Table 3)	Cryptographic Erase service, Set Band Position and Size service	Plaintext in RAM Encrypted in System Area outside the module using the Approved KTS	Explicit Zeroisation service, Cryptographic Erase service, Set Band Position and Size service Implicit Power-Off	Derivation of MEKs
MEKs	256	N/A	KDF in Counter Mode	Exported to other functional subsystems on the same single-chip	Band Lock/Unlock service, Cryptographic Erase service, Set Band Position and Size service	Plaintext in RAM	Implicit Immediately after exported	Data encryption / decryption by other functional subsystems
SID/BandMaster(s)/Erase Master PINs	Referred to in Section 4.1 (Table 6)	SHA256 (#C1925)	Electronic input	Imported and Exported by KTS (see Table 3)	Set PIN service	Hashed in RAM Hashed + Encrypted in System Area outside the module using the	Explicit Zeroisation service Implicit Power-Off	User authentication

						Approved KTS		
DRBG Internal Value	V: 440 bits C: 440 bits	Hash_DRBG (#C2002)	SP800-90A Instantiation of Hash_DRBG	N/A	Power-On	Plaintext in RAM	Explicit Zeroisation service Implicit Power-Off	Random number generation
DRBG Seed	Entropy Input String and Nonce: 512 bits	Hash_DRBG (#C2002)	Entropy collected from Entropy Source at instantiation (Minimum entropy of 8 bits: 6.31)	N/A	Power-On	Plaintext in RAM	Implicit Immediately after use[6]	Random number generation
Public Security Parameters (PSPs)								
PubKey1	112	RSA (#C2009)	Electronic input	Imported during FW load.	Power-on FW Download service	Plaintext in RAM Hashed in OTP	Implicit Power-Off (Data in RAM)	Signature verification.

Table 9 - SSPs

Entropy source	Minimum number of bits of entropy	Details
Entropy Source[7]	Minimum entropy of 8 bits is 6.31.	Hardware RNG used to seed the approved Hash_DRBG.

Table 10 - Non-Deterministic Random Number Generation Specification

[6] Zeroised after input to Hash_DRBG algorithm.

[7] The Entropy Source is a hardware module inside the CM boundary. The Entropy Source supplies the Hash_DRBG with 512 bits entropy input. From Table 10 this input contains about 404 bits of entropy, which is sufficient entropy to obtain 256 bits of security strength.

For the Entropy Source listed in the table above, self-tests are performed each time before data is obtained (see Section 10 for details of these self-tests). When these tests detect that the Entropy Source cannot generate the sufficient amount of entropy, the CM is transient to error state. The CM can be recovered from the error state by rebooting the module, and the obtaining of Entropy data is attempted again. If the CM continuously enters in error state in spite of several trials of reboot, the CM may be sent back to factory to recover from error state.

Section 10 – Self Tests

The CM runs self-tests in the following table.

Function	Self-Test Type	Execution Condition	Abstract	Failure Behavior
AES256-CBC	Conditional	Power-On	Encrypt/Decrypt KAT	Enters Boot Error State (Indicated Error Code: 0x24)
SHA256	Conditional	Power-On	Digest KAT	Enters Boot Error State. (Indicated Error Code: 0x25)
HMAC-SHA256	Conditional	Power-On	Digest KAT	Enters Boot Error State. (Indicated Error Code: 0x26)
Hash_DRBG	Conditional	Power-On	DRBG KAT	Enters Boot Error State. (Indicated Error Code: 0x18/0x19)
RSASSA-PKCS#1-v1_5	Conditional	Power-On	Signature verification KAT	Enters Boot Error State. (Indicated Error Code: 0x27)
KDF in Counter Mode	Conditional	Power-On	KDF KAT	Enters Boot Error State (Indicated Error Code: 0x28)
Entropy Source (Health tests of noise source at startup.)	Conditional	Power-On	Verify not deviating from the intended behavior of the noise source by Repetition Count Test and Adaptive Proportion Test specified in SP800-90B.	Enters Boot Error State (Indicated Error Code: 0x2C/0x2D)
Hash_DRBG	Conditional	Random number generation	Verify newly generated random number not equal to previous one	Enters Error State. (Indicated Error Code: 0x1D)
Entropy Source	Conditional	Entropy output request	Verify newly generated random number not equal to previous one	Enters Error State. (Indicated Error Code: 0x1E)

Entropy Source (Continuous noise source health tests during operation.)	Conditional	Entropy output request	Verify not deviating from the intended behavior of the noise source by Repetition Count Test and Adaptive Proportion Test specified in SP800-90B.	Enters Error State. (Indicated Error Code: 0x2C/0x2D)
Firmware load test	Conditional[8]	Power-on	Verify signature of loaded firmware image by RSASSA-PKCS#1-v1_5	Enters Power Up Load Test Error State (Indicated Error Code: 0x13)
		FW download	Verify signature of downloaded firmware image by RSASSA-PKCS#1-v1_5	Enters Conditional Load Test Error State. After reporting Error code, transition from error state to normal state and continue to operate with FW before download. (Indicated Error Code: 0x13)
Firmware integrity test	Pre-operational	Power-On	Verify ROM code integrity with 32bit CRC.	Enters Boot Error State (Implicit error reporting by stopping the startup sequence)

Table 11 - Self Tests

As shown in the table above, self-tests are performed automatically at the CM startup and before execution certain security functions. Operator can also initiate self-test on-demand for periodic testing by using the Reset service which is automatically invoked when the module is powered-off and powered-on (rebooted).

If the self-tests fail, the CM reports error status and enters to the error state. In this case, the CM must be powered-off to clear error condition. When power-on is executed again, self-tests are also executed like an on-demand operator reset. If the CM continuously enters in error state in spite of several trials of reboot, the CM may be sent back to factory to recover from error state.

Section 11 – Life-cycle Assurance

In the SSD’s manufacturing process, installation is executed as below:

[8] Firmware load test is also run at the time of Power-up, and the integrity of the Firmware loaded into the CM can be confirmed.

1. The Firmware described in Section 2.1 is downloaded into the CM.
2. Initial SSPs are generated.
3. Initial authentication information is set to the CM.
4. System area including SSPs generated in Step2 and Step3 are encrypted and calculated message authentication code.

Initial operations to setup this CM are following:

1. Load Firmware into the CM.
2. Load System area including SSPs into the CM.
3. Execute Range state setting method.
4. Execute Download port setting method.

The CM switches to approved mode after the initial operation success. When the initial operation succeeds, the CM indicates success on the Status Output interface. Users can confirm that the CM is in approved mode by executing Show Status service and checking that the startup is successfully completed. As described in Section 2, the CM is used by being embedded in the solid state drive. Therefore, there are no maintenance requirements for the CM alone. Guidance for this module is provided to solid state drive developers who embed the CM. The usage and maintenance of solid state drives with the CM built-in are outside of the scope of this document.

Section 12 – Mitigation of Other Attacks

The CM does not mitigate other attacks beyond the scope of FIPS 140-3 requirements.