FIPS 140-3 Non-Proprietary Security Policy for:

KIOXIA FIPS TC58NC1030GTB Crypto Sub-Chip

KIOXIA CORPORATION

Rev 3.0.5

Section 1 - General

This document explains precise specification of the security rules about KIOXIA FIPS TC58NC1030GTB 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.

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

Table 1 - Security Levels

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	Power on 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

Section 2 – Cryptographic Module Specification

KIOXIA FIPS TC58NC1030GTB 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 TC58NC1030GTB 0002 SoC (see Figure 1 in Section 7). Overall Security Rating of the CM is Level 2 (See Table 1 in Section 1 for individual security area levels). The CM is embedded in TCG OPAL compliant solid state drive controllers which provides user data encryption/decryption through build-in HW engines.
The CM provides various cryptographic services using approved algorithms. The CM has multiple functions, but they do not support the degraded operation. The physical boundary of the CM is the TC58NC1030GTB 0002 SoC and the logical boundary of the CM is TC58NC1030GTB 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 is validated with the following versions:

Physical single-chip	The sub-chip cryptographic subsystem soft circuitry core	The associated firmware
TC58NC1030GTB 0002	TC58NC1030GTB CRPT module 0001	SC01CN

Table 2 - Cryptographic Module Tested Configuration

Section 2.2 – Security Functions

The CM executes the following approved algorithms:

CAVP Cert	Algorithm and Standard	Mode/ Method	Description/Key Size(s)/ Key Strength(s)	Use/Function
#A2402	AES256 (FIPS 197 / SP800-38A)	CBC	Key Size: 256 bits/ Key Strength: 256 bits	Data and Key Encryption/ Decryption

#A2402	AES256 (FIPS 197 / SP800-38A, SP800-38E)	XTS, ECB[1]	Key Size: 256 bits/ Key Strength: 256 bits	Data Encryption/ Decryption
#A2402	SHA2-256 (FIPS 180-4)	N/A	N/A	Hashing messages
#A2402	HMAC-SHA2-256 (FIPS 198-1)	N/A	Key Size: 256 bits/ Key Strength: 256 bits	Message Authentication Code
#A2402	RSASSA-PKCS#1-v1_5 (FIPS 186-4)	N/A	Key Size: 2048, 3072 bits/ Key Strength: 112, 128 bits	Signature verification
#A2450	ECDSA (FIPS 186-4)	N/A	Curve: P-256/ Key Strength: 128 bits	Signature generation/ verification
#A2432	Hash_DRBG (SP800-90A Rev.1)	N/A	Hash based: SHA2-256	Deterministic Random Bit Generation
#A2433	KBKDF (SP800-108 Revised)	Counter	MACs: HMAC-SHA2-256/ Key Size: 256 bits/ Key Strength: 256 bits	Key derivation
#A2402	KTS (IG D.G)	N/A	Combination of AES256 CBC Mode and HMAC-SHA2-256 / 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
#E143	Entropy Source (SP800-90B)	N/A	N/A	Hardware RNG used to seed the approved Hash_DRBG.

Note 1: The "CAVP Cert" of KTS comes from the fact that KTS is composed of AES256-CBC and HMAC-SHA2-256 (#A2402).

Note 2: There are algorithms, modes, and keys that have been CAVP tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by the module.

Table 3 - Approved Algorithms

The CM does not have any Non-approved algorithms allowed in the approved mode of operation.

[1] ECB mode is used as a prerequisite of XTS mode. ECB is not directly used in services of the Cryptographic Module. The CM performs a check that the XTS Key1 and XTS Key2 are different according to IG C.I. AES-XTS is only used for encryption/decryption of data stored in solid state drives equipped with this CM.

Section 2.3 – Module Configuration

Overview block diagram of the CM is shown below.

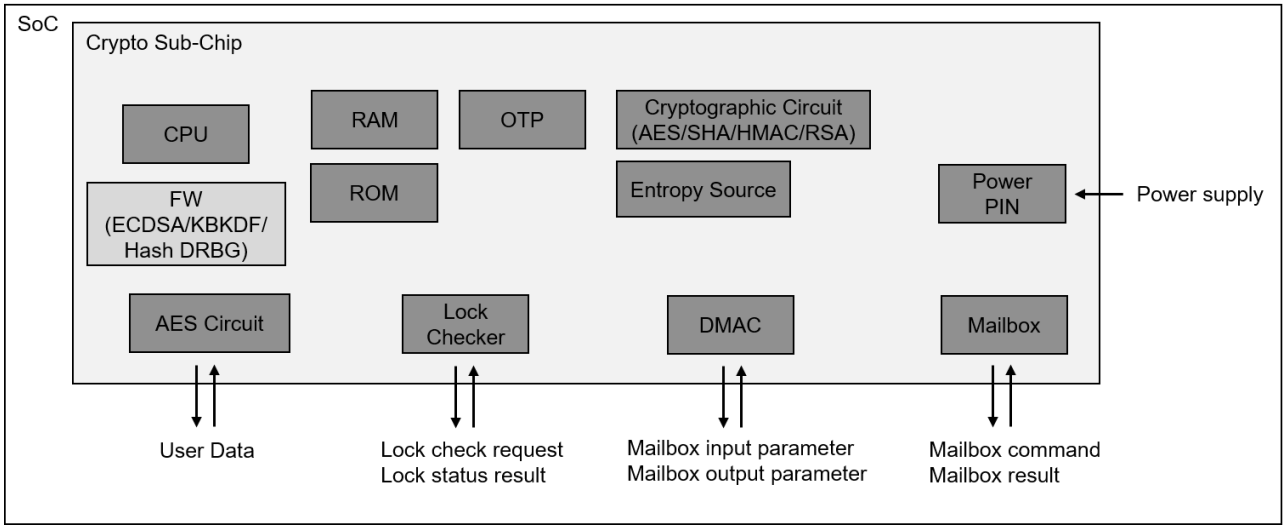

Figure 1 – Configuration of module and peripheral components

Components of the CM is shown with gray background blocks include processor, memories (volatile and non-volatile memory) and HW circuitry for cryptographic processing. Cryptographic algorithms implemented as FW are shown in light-gray background block. 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 Interfaces

Physical port	Logical Interface	Data that passes over port/interface
Mailbox AES circuit DMAC Lock Checker	Data Input	Mailbox input parameter. User data. Read/Write destination address information.
Mailbox AES circuit DMAC	Data Output	Mailbox output parameter. User data.
Mailbox Lock Checker	Control Input	Mailbox command information. Lock status confirmation request signal.
Mailbox Lock Checker	Status Output	Mailbox command result. Lock status confirmation result signal.
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.

Table 4 - Ports and Interfaces

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 (AdminSP.SID)	Download Port Lock/Unlock	Mailbox command	Mailbox command result
	Firmware Download[2]		
	Set PIN (for AdminSP.SID and AdminSP.Admin1)		
	Authority Enable/Disable		
	Revert		
	Data Locking protection Enable		
	Sanitize		
	Format Namespace		
	Namespace Create/Delete		
FIPS Crypto Officer (AdminSP.Admin1)	Set PIN (for AdminSP.Admin1)	Mailbox command	Mailbox command result
	Revert		
	Sanitize		
	Format Namespace		
	Namespace Create/Delete		
FIPS Crypto Officer (LockingSP.Admin1-4)	Band Lock/Unlock	Mailbox command	Mailbox command result
	Cryptographic Erase		
	Cryptographic Erase and Initialize Band State		
	Set Band position and Size, Set Band position and Size for Band of Single User Mode		
	Set PIN(for LockingSP.Admin1-4 and LockingSP.User1-192)		
	Authority Enable/Disable		
	Revert		
	Data Locking protection Enable		
	Sanitize		
	Format Namespace		
	Namespace Create/Delete		
	Band Set Enable		
	Band Set Disable		
	Data Read/Write	Encrypted/Decrypted data	Decrypted/Encrypted data
FIPS Crypto Officer (LockingSP.User1)	Band Lock/Unlock for Band of Single User Mode (for GlobalRange)	Mailbox command	Mailbox command result
	Cryptographic Erase for Band of Single User Mode (for GlobalRange)		
	Cryptographic Erase and Initialize		

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

	Band State (for GlobalRange)		
	Set Band position and Size for Band of Single user Mode (for GlobalRange		
	Set PIN (for LockingSP.User1), Set PIN for Band of Single User Mode (for LockingSP.Use1)		
	Format Namespace		
	Namespace Create/Delete		
	Data Read/Write	Encrypted/Decrypted data	Decrypted/Encrypted data
FIPS Crypto Officer (LockingSP.User2)	Band Lock/Unlock for Band of Single User Mode (for Band1)	Mailbox command	Mailbox command result
	Cryptographic Erase for Band of Single User Mode (for Band1)		
	Cryptographic Erase and Initialize Band State (for Band1)		
	Set Band position and Size for Band of Single user Mode (for Band1)		
	Set PIN (for LockingSP.User2), Set PIN for Band of Single User Mode (for LockingSP.User2)		
	Format Namespace		
	Data Read/Write	Encrypted/Decrypted data	Decrypted/Encrypted data
…	…	…	…
FIPS Crypto Officer (LockingSP.User192)	Band Lock/Unlock for Band of Single User Mode (for Band191)	Mailbox command	Mailbox command result Exported encryption key Range information
	Cryptographic Erase for Band of Single User Mode (for Band191)		
	Cryptographic Erase and Initialize Band State (for Band191)		
	Set Band position and Size for Band of Single user Mode (for Band191)		
	Set PIN (for LockingSP.User192), Set PIN for Band of Single User Mode (for LockingSP.User192)		
	Format Namespace		
	Data Read/Write	Encrypted/Decrypted data	Decrypted/Encrypted data
None	Firmware Verification	Mailbox command	Mailbox command result
	Random Number Generation		
	Show Status		
	Zeroisation		
	Signature Generation		
	Signature Verification		
	Calculate Hash Digest		
	Check Lock State	Read/Write Command	Lock state of each Band
	Reset	Power	N/A

Note: There are LockingSP.Users from user 1 to user 192, but user 3 to user 191 are omitted in the table above.

Table 5 - Roles, Service Commands, Input and output

The CM supports the configuration of roles and services. The authenticated operator is expected to configure locked bands for data storage, the associated role and the lock-based authentication data (PIN) per Table 5 (refer to section 11 for detail settings to maintain secure operation). Bands that are not configured are considered unprotected or plaintext. This configuration enables Data Read/Write service using the lock-based authentication model (IG 4.1.A). To Read/Write data from/to each band, an operator must unlock the bands with appropriate authenticated roles. Once the bands are unlocked, Read and Write access to the bands must be controlled by a trusted operator outside of the module who has authenticated the associated role until powered off. The module prevents Data read/write service for locked bands. If Read and Write access needs to be inhibited prior to power off, the operator who authenticates the role must set the bands to the locked state again.

Section 4.1 – Roles and Authentication

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

Role	Authentication Method	Authentication Strength
AdminSP.SID	Role based PIN authentication	Single random attempt: 1 / 2^{64} < 1 / 1,000,000 Multi attempt per minute: 60,000 / 2^{64} < 1 / 100,000
AdminSP.Admin1	Role based PIN authentication	Single random attempt: 1 / 2^{64} < 1 / 1,000,000 Multi attempt per minute: 60,000 / 2^{64} < 1 / 100,000
LockingSP.Admin1-4	Role based PIN authentication	Single random attempt: 1 / 2^{64} < 1 / 1,000,000 Multi attempt per minute: 60,000 / 2^{64} < 1 / 100,000
LockingSP.User1	Role based PIN authentication	Single random attempt: 1 / 2^{64} < 1 / 1,000,000 Multi attempt per minute: 60,000 / 2^{64} < 1 / 100,000
LockingSP.User2	Role based PIN authentication	Single random attempt: 1 / 2^{64} < 1 / 1,000,000 Multi attempt per minute: 60,000 / 2^{64} < 1 / 100,000
…	…	…
LockingSP.User192	Role based PIN authentication	Single random attempt: 1 / 2^{64} < 1 / 1,000,000 Multi attempt per minute: 60,000 / 2^{64} < 1 / 100,000

Note 1: All roles to be authenticated are FIPS Crypto Officer

Note 2: There are LockingSP.Users from user 1 to user 192, but user 3 to user 191 are omitted in the table above.

Table 6 - Identification and Authentication Policy

The CM provides a role-based PIN authentication function. The CM stores PINs that has been previously hashed with SHA2-256, and verifies the PIN entered by the operator matches the stored information at the time of authentication.
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 1ms when authentication attempt fails, so the maximum number of authentication attempts is 60,000 times in 1 min. Consequently, the probability that random attempts in 1min will succeed is $60{,}000 / 2^{64} < 1 / 100{,}000$.
Initial PINs of AdminSP.Admin1, LockingSP.Admin2-4 and LockingSP.User1-192 are set to null (i.e., data length is 0). These role's authentication data are need to be replaced upon the first-time authentication. Otherwise, the operator who assumes these roles cannot execute services except Set PIN and services that does not need authorized roles.

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[3]	Indicator
Band Lock/Unlock	Lock or unlock read / write of user data in a band.	KBKDF HMAC-SHA2-256	KDK MEKs System MAC Key	LockingSP.Admin 1-4	E G E	Mailbox command result
Band Lock/Unlock for Band of Single User Mode	Lock or unlock read / write of user data in band "X" of single user mode.			LockingSP.User"X +1"		
Check Lock State	Check a lock state of band that read / write user data.	N/A	N/A	None	N/A	Band Lock state
Data Read/Write	Encryption / decryption of user data to/from unlocked band of SSD[4].	AES256-XTS	MEKs	LockingSP.Admin 1-4 LockingSP.User1-192	E	Readable/Writable signal from lock check module
Cryptographic Erase	Erase user data (in cryptographic means) by changing the key that derives the data encryption key.	CKG(Hash_DRBG) KBKDF HMAC-SHA2-256 AES256-CBC KTS	DRBG Internal Value KDK KDK MEKs System MAC Key System Enc Key KDK	LockingSP.Admin 1-4	E G, Z E G, Z E E W, R	Mailbox command result

[3] The letters (G, R, W, E, Z) mean Generate, Read, Write, Execute and Zeroise respectively.
[4] The band has to be unlocked by the corresponding role beforehand.

Cryptographic Erase for Band of Single User Mode	Erase user data in band "X" of single user mode (in cryptographic means) by changing the key that derives the data encryption key.			LockingSP.user"X+1"		
Cryptographic Erase and Initialize Band State	Erase user data in band "X" of single user mode (in cryptographic means) by changing the key that derives the data encryption key, and initialize the band state.	CKG(Hash_DRBG) KBKDF HMAC-SHA2-256 AES256-CBC KTS	DRBG Internal Value KDK KDK MEKs System MAC Key System Enc Key KDK	LockingSP.Admin 1-4 LockingSP.user"X+1"	E G, Z E G, Z E E W, R	Mailbox command result
Download Port Lock/Unlock	Lock / unlock firmware download.	N/A	N/A	AdminSP.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[5].	SHA2-256 RSASSA-PKCS#1-v1_5	PubKey1 PubKey1	AdminSP.SID	W, E E	Mailbox command result
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) KBKDF HMAC-SHA2-256 AES256-CBC KTS	DRBG Internal Value KDK KDK MEKs System MAC Key System Enc Key KDK	LockingSP.Admin 1-4	E G, Z E G, Z E E W, R	Mailbox command result
Set Band Position and Size for Band of Single User Mode	Set the location and size of the band "X" of single user mode			LockingSP.Admin 1-4 LockingSP.User"X+1"		
Set PIN	Set PIN (authentication data).	SHA2-256 HMAC-SHA2-256 AES256-CBC KTS	PINs System MAC Key System ENC Key PINs	AdminSP.SID, AdminSP.Admin1 , LockingSP.Admin 1-4, LockingSP.User1-192	W, E E E W, R	Mailbox command result
Set PIN for Band of Single User Mode	Set PIN (authentication data) of authority for band "X" of single use mode			LockingSP.User1-192		
Authority	Enable/Disable the	HMAC-SHA2-256	System MAC Key	AdminSP.SID	E	Mailbox

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

Enable/Disable	authority.	AES256-CBC	System Enc Key	LockingSP.Admin 1-4	E	command result
Revert	Initialize the band State and disable band lock setting.	SHA2-256 CKG(Hash_DRBG) KBKDF HMAC-SHA2-256 AES256-CBC KTS	PINs DRBG Internal Value KDK KDK MEKs System MAC Key System Enc Key PINs KDK	AdminSP.SID, AdminSP.Admin1 LockingSP.Admin 1-4,	W, E E G, Z E G, Z E E W, R W, R	Mailbox command result
Data Locking Protection Enable	Enable Data protection with band lock setting.	SHA2-256 HMAC-SHA2-256 AES256-CBC KTS	PINs System MAC Key System Enc Key PINs	AdminSP.SID LockingSP.Admin 1-4	W, E E E W, R	Mailbox command result
Sanitize	Erase all user data (in cryptographic means) by changing the key that derives the data encryption key.	CKG(Hash_DRBG) KBKDF HMAC-SHA2-256 AES256-CBC KTS	DRBG Internal Value KDK KDK MEKs System MAC Key System Enc Key KDK	AdminSP.SID, AdminSP.Admin1 , LockingSP.Admin 1-4	E G, Z E G, Z E E W, R	Mailbox command result
Format Namespace	Erase user data (in cryptographic means) on Namespace by changing the key that derives the data encryption key.	CKG(Hash_DRBG) KBKDF HMAC-SHA2-256 AES256-CBC KTS	DRBG Internal Value KDK KDK MEKs System MAC Key System Enc Key KDK	AdminSP.SID, AdminSP.Admin1 , LockingSP.Admin 1-4, LockingSP.User1-192	E G, Z E G, Z E E W, R	Mailbox command result
Namespace Create/Delete	Create and delete Namespace.	CKG(Hash_DRBG) KBKDF HMAC-SHA2-256 AES256-CBC KTS	DRBG Internal Value KDK KDK MEKs System MAC Key System Enc Key KDK	AdminSP.SID, AdminSP.Admin1 , LockingSP.Admin 1-4, LockingSP.User1	E G, Z E G, Z E E W, R	Mailbox command result
Band Set Enable	Set the location, size and lock state of the band.	CKG(Hash_DRBG) KBKDF HMAC-SHA2-256 AES256-CBC KTS	DRBG Internal Value KDK KDK MEKs System MAC Key System Enc Key KDK	LockinSP.Admin1 -4	E G, Z E G, Z E E W, R	Mailbox command result
Band Set Disable	Initialize the location, size and lock state of the band.	CKG(Hash_DRBG) KBKDF HMAC-SHA2-256 AES256-CBC KTS	DRBG Internal Value KDK KDK MEKs System MAC Key System Enc Key KDK	LockingSP.Admin 1-4	E G, Z E G, Z E E W, R	Mailbox command result

Signature Generation	Generate a signature of the data by using a private key entered from outside of the CM.	ECDSA	Key Pair Private Key	None	W, E, Z	Mailbox command result
Signature Verification	Verify input signature by using a public key entered from outside of the CM.	ECDSA	Key Pair Public Key	None	W, E, Z	Mailbox command result
Calculate Hash Digest	Hash the data entered from outside of the CM.	SHA2-256	N/A	None	N/A	Mailbox command result
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 KDK MEKs PINs System MAC Key System Enc Key DRBG Internal Value	None[6]	Z Z Z Z Z Z Z	Mailbox command result
Reset	Power-OFF: Delete SSPs in RAM.	N/A	System MAC Key System Enc Key KDK MEKs PINs DRBG Internal Value PubKey1	None	Z Z Z Z Z Z Z	N/A
	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 KBKDF Entropy Source Hash_DRBG HMAC-SHA2-256 AES256-CBC KTS	PubKey1 RKey System MAC Key System Enc Key DRBG Seed DRBG Seed DRBG Internal Value System MAC Key System Enc Key KDK PINs		W, E E G G G E, Z G E E W W	

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

Note 2: A cryptographic module is required to provide services “Show module’s versioning information”, “Show status”, “Perform self-tests”, “Perform approved security functions” and “Perform zeroisation”. In this CM, “Show module’s information” and “Show status” are included in the Show Status service and “Perform self-tests” is included in the Reset service. “Perform zeroisation” is executed by the Zeroisation service. All other services fall under “Perform approved security functions”.

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

Table 7 - Approved services

The CM does not provide Non-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 (RSASSA-PKCS#1-v1_5, see table 3)
・ Method for integrity test on demand: Power cycling

The CM supports the partial loading that replaces the current Firmware image, excluding the ROM Code, with a new Firmware image loaded from outside the module. In this case the CM becomes another validated one.

Section 6 – Operational Environment

Operational Environment requirements are not applicable because the CM does not employ operating systems and operates in a limited operational environment under the FIPS 140-3 definitions.

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.

Front

Back

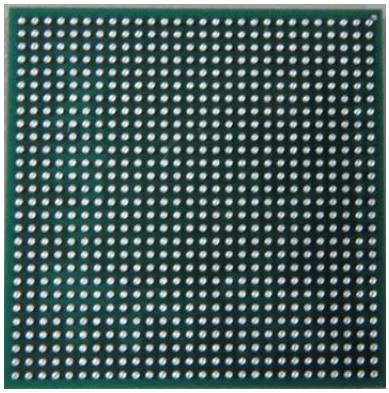

Figure 2 - TC58NC1030GTB 0002 SoC

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 (#A2433)	Hash_DRBG (Method SP800-133 Rev.2 Section 4)	N/A	Installation	Plaintext in OTP	Explicit Zeroisation service	Derivation of System Enc Key and System MAC Key
System Enc Key	256	AES-CBC (#A2402)	KDF in Counter Mode	N/A	Power-On	Plaintext in RAM	Explicit Zeroisation service Implicit Power-Off	Data and Key Encryption / Decryption for KTS
System MAC Key	256	HMAC (#A2402)	KDF in Counter Mode	N/A	Power-On	Plaintext in RAM	Explicit Zeroisation service	Message Authentication Code generation

							Implicit Power-Off	and verification for KTS
KDK	256	KBKDF (#A2433)	Hash_DRBG (Method SP800-133 Rev.2 Section 4)	Imported and Exported by KTS (see Table 3)	Key update services[7]	Plaintext in RAM Encrypted in System Area outside the module using the Approved KTS	Explicit Zeroisation service, Key update services Implicit Power-Off	Derivation of MEKs
MEKs	256	AES-XTS (#A2402)	KDF in Counter Mode	N/A	Band Lock/Unlock service, Key update services	Plaintext in AES register	Explicit Zeroisation service, Key update services Implicit Power-Off	Data encryption / decryption
PINs	Referred to in Section 4.1 (Table 6)	SHA2-256 (#A2402)	Electric 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 Approved KTS	Explicit Zeroisation service Implicit Power-Off	User authentication
Key Pair Private Key	128	ECDSA (#A2450)	Electric input	Imported during Signature Generation Service	Signature Generation service	Plaintext in RAM	Implicit Immediately after use[8]	Signature generation for arbitrary data
DRBG Internal Value	V: 440 bits C: 440 bits	Hash_DRBG (#A2432)	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: 1024 bits	Hash_DRBG (#A2432)	Entropy collected from Entropy Source at instantiation (Minimum	N/A	Power-On	Plaintext in RAM	Implicit Immediately after use[8]	Random number generation

[7] The following service are applicable, Cryptographic Erase, Cryptographic Erase for Band of Single User Mode, Cryptographic Erase and Initialize Band State, Set Band Position and Size, Set Band Position and Size for Band of Single User Mode, Revert, Sanitize, Format Namespace, Namespace Create/Delete and Band Set Enable.

[8] Zeroised after input to related algorithm.

			entropy of 8 bits:3.00)					
Public Security Parameters (PSPs)								
PubKey1	112	RSA (#A2402)	Electric input	Imported during FW load.	Power-on, FW Download service	Plaintext in RAM Hashed in OTP	Implicit Power-Off (Data in RAM)	Signature verification
Key Pair Public Key	128	ECDSA (#A2450)	Electric input	Imported during Signature Verification Service	Signature Verification service	Plaintext in RAM	Implicit Immediately after use[8]	Signature verification for arbitrary data

Table 9 - SSPs

Entropy source	Minimum number of bits of entropy	Details
Entropy Source[9]	Minimum entropy of 8 bits is 3.00.	Hardware RNG used to seed the approved Hash_DRBG.

Table 10 - Non-Deterministic Random Number Generation Specification

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.

[9] The Entropy Source is a hardware module inside the CM boundary. The Entropy Source supplies the Hash_DRBG with 1024 bits entropy input. From Table 10 this input contains about 384 bits of entropy, which is sufficient entropy to obtain 256 bits of security strength.

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 KAT Decrypt KAT	Enters Boot Error State. (Indicated Error Code: 0x24)
AES256-XTS	Conditional	Power-On	Encrypt KAT Decrypt KAT	Enters Boot Error State. (Indicated Error Code: 0x23)
SHA2-256	Conditional	Power-On	Digest KAT	Enters Boot Error State. (Indicated Error Code: 0x25)
HMAC-SHA2-256	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)
ECDSA	Conditional	Power-On	Signature generation KAT	Enters Boot Error State (Indicated Error Code: 0x10)
ECDSA	Conditional	Before first use	Signature verification KAT	Enters Error State (Indicated Error Code: 0x10)
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)
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 (Conditional Test). (Indicated Error Code: 0x2C/0x2D)

Firmware load test	Conditional[10]	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:
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.

[10] 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.

2. Load system area including SSPs into the CM.
3. Execute range state setting method.
4. Execute download port setting method.
5. Execute service execution state setting method.
6. Execute namespace 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.

For secure operation, the following settings must be maintained:

- Data Locking Protection is Enabled
- Each Band is set to be locked when power-on. Bands that are not configured are considered unprotected or plaintext.

(Refer to SSD setting procedure[11])

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.

[11] For maintaining secure condition, the SSD needs several setting at least.
Owners of the SSD that embeds the CM must use it securely according to the followings:

1. TCG LockingSP is enabled by Activate method.
2. Both ReadLockEnabled and WriteLockEnabled are set to “True” for each band (included Global Range) and it must not be modified.
3. For each band, “Power Cycle" of LockOnReset setting is not change.
4. If the LockingSP has been made disabled, the Activate method is re-executed before PowerCycle is performed.