FIPS 140-2 Non-Proprietary Security Policy for:

KIOXIA TCG Enterprise SSC Crypto Sub-Chip

KIOXIA CORPORATION

Rev 2.0.0

Overview

The KIOXIA TCG Enterprise SSC Crypto Sub-Chip (listed in Section1.1 Product Version) is used for solid state drive data security. The Cryptographic Module (CM) is a single chip module implemented as a sub-chip compliant with IG 1.20 in the TC58NC1033GTC 0003 SoC. The CM provides various cryptographic services using FIPS approved algorithms. The CM is multiple functions embedded, and the physical boundary of the CM is the TC58NC1033GTC 0003 SoC. The logical boundary of the CM is CRPT module.
The CM is intended to meet the requirements of FIPS 140-2 Security Level 2 Overall. The Table below shows the security level detail.

Section	Level
1. Cryptographic Module Specification	2
2. Cryptographic Module Ports and Interfaces	2
3. Roles, Services, and Authentication	2
4. Finite State Model	2
5. Physical Security	2
6. Operational Environment	N/A
7. Cryptographic Key Management	2
8. EMI/EMC	2
9. Self-Tests	2
10. Design Assurance	2
11. Mitigation of Other Attacks	N/A
Overall Level	**2**

Table 1 - Security Level Detail

Interface	Ports
Data Input	Mailbox AES circuit DMAC
Control Input	Mailbox Lock Checker
Data Output	Mailbox AES circuit DMAC
Status Output	Mailbox Lock Checker
Power Input	Power PIN

Table 2 - Physical/Logical Port Mapping

Acronyms

AES Advanced Encryption Standard

CM	Cryptographic Module
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
HMAC	The Keyed-Hash Message Authentication code
KAT	Known Answer Test
NDRNG	Non-Deterministic Random Number Generator
POST	Power on Self-Test
PSID	Printed SID
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm
SID	Security ID

Section 1 – Module Specification

The CM has one FIPS 140 approved mode of operation and CM is always in approved mode of operation after initial operations are performed. The CM provides services defined in Section 2.1 and other non-security related services.

Section 1.1 – Product Version

The CM are validated with the following versions:

The Sub-Chip Cryptographic Subsystem Name: CRPT module
The Sub-Chip Cryptographic Subsystem Version: 0000
Hardware Version: TC58NC1033GTC 0003
Firmware Version: SC01

Section 2 – Roles Services 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	$1 / 2^{48} < 1 / 1{,}000{,}000$	$30 / 2^{48} < 1 / 100{,}000$
SID	Crypto Officer	Role	PIN	$1 / 2^{48} < 1 / 1{,}000{,}000$	$30 / 2^{48} < 1 / 100{,}000$
BandMaster0	User	Role	PIN	$1 / 2^{48} < 1 / 1{,}000{,}000$	$30 / 2^{48} < 1 / 100{,}000$
BandMaster1	User	Role	PIN	$1 / 2^{48} < 1 / 1{,}000{,}000$	$30 / 2^{48} < 1 / 100{,}000$
…	…	…	…	…	…
BandMaster64	User	Role	PIN	$1 / 2^{48} < 1 / 1{,}000{,}000$	$30 / 2^{48} < 1 / 100{,}000$

Table 3 - Identification and Authentication Policy

Per the security policy rules, the minimum PIN length is 6 bytes. Therefore the probability that a random attempt will succeed is $1 / 2^{48} < 1 / 1{,}000{,}000$ (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. Therefore the probability that random attempts in 1min will succeed is $30 / 2^{48} < 1 / 100{,}000$. Even if TryLimit[1] is infinite, the probability that random attempts is same.

[1] TryLimit is the upper limit of failure of authentication of each role.

Section 2.1 – Services

This section describes services which the CM provides.

Service	Description	Role(s)	Keys & CSPs[2]	RWX (Read, Write,e Xecute)	Algorithm	Method
Band Lock/Unlock	Lock or unlock read / write of user data in a band.	BandMaster0 … BandMaster64	KEK MEKs	R, X R	AES256-CBC	setRangeInformation method
Check Lock State	Check a lock state of band that read / write user data.	None	N/A	N/A	N/A	HW auto
Data Read/Write	Encryption / decryption of user data to/from unlocked band of SSD.	None[3]	MEKs	X	AES256-XTS (#5067, #5068)	HW auto
Cryptographic Erase	Erase user data (in cryptographic means) by changing the data encryption key.	EraseMaster	KEK MEKs System MAC Key System Enc Key	R, X W R, X R, X	AES256-CBC Hash_DRBG HMAC-SHA256 AES256-CBC	eraseBand method setRangeInformation method
Download Port Lock/Unlock	Lock / unlock firmware download.	SID	N/A	N/A	N/A	setLogicalPort method
Firmware Verification	Digital signature verification for firmware outside the CM.	None	PubKey2	R, X	RSASSA-PKCS# 1-v1_5 (#2753)	verification method
Firmware Download	Download a firmware image.	SID	PubKey1	R, X	RSASSA-PKCS# 1-v1_5 (#2752)	reloadCrypto method
Random Number Generation	Provide a random number generated by the CM.	None	DRBG Internal State	R, W	Hash_DRBG	getRandom method
Set Band Position and Size	Set the location and size of the band.	BandMaster0 … BandMaster64	KEK MEKs System MAC Key System Enc Key	R, X R, W R, X R, X	AES256-CBC Hash_DRBG HMAC-SHA256 AES256-CBC	setRangeInformation method
Set PIN	Set PIN (authentication data).	EraseMaster SID BandMaster0 … BandMaster64[4]	KEK System MAC Key System Enc Key	R, X R, X R, X	AES256-CBC HMAC-SHA256 SHA256 AES256-CBC	setPIN method
Show Status	Report status of the CM.	None	N/A	N/A	N/A	Method status

[2] Symmetric keys are generated from the DRBG according to SP800-133.

[3] The band has to be unlocked by corresponding BandMaster beforehand.

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

Zeroization	Erase CSPs.	None[5]	RKey KEK MEKs System MAC Key System Enc Key DRBG Internal State	W W W W W W	N/A	zeroization method
Reset	Run POSTs and delete CSPs in RAM.	None	N/A	N/A	N/A	Power on reset

Table 4 - FIPS Approved services

Algorithm	Description	CAVP Certification Number
AES256-CBC	Encryption, Decryption	#5062
AES256-XTS[6]	Decryption	#5068
AES256-XTS[6]	Encryption	#5067
SHA256	Hashing	#4128
HMAC-SHA256	Message Authentication Code	#3388
RSASSA-PKCS#1-v1_5	Function: Signature Verification Key Size: 2048 bits	#2752
RSASSA-PKCS#1-v1_5	Function: Signature Verification Key Size: 2048 bits	#2753
Hash_DRBG	Hash based: SHA256	#1890
KBKDF	Counter Mode MACs: HMAC-SHA256	#173
CKG	Cryptographic Key Generation referred by SP800-133	Vendor Affirmation
KTS	Key Transport Scheme reffered by IG D.9; AES Cert. #5062 and HMAC Cert. #3388	#5062, #3388

Table 5 - FIPS Approved Algorithms

Algorithm	Description
NDRNG	Hardware RNG used to seed the approved Hash_DRBG. Minimum entropy of 8 bits is 7.56.

Table 6 - Non-FIPS Approved Algorithms

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

[6] 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 A.9.

Section 3 – Physical Security

The CM is a sub-chip enclosed in a single chip that is an opaque package.

Front Back

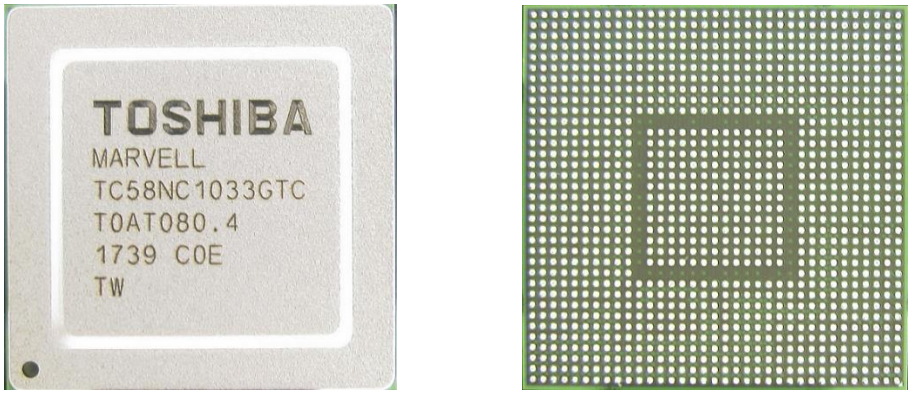

Figure 1 - TC58NC1033GTC 0003 SoC

Section 4 – Operational Environment

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

Section 5 – Key Management

The CM uses keys and CSPs in the following table.

Key/CSP	Length (bit)	Type/ Algorithm	Zeroize Method	Establishment	Output	Persistence/ Storage
RKey	256	KBKDF	Zeroization service	Hash_DRBG	No	Plain / OTP
System Enc Key	256	AES-CBC	Zeroization service	KDF in Counter Mode	No	Plain / RAM
System MAC Key	256	HMAC	Zeroization service	KDF in Counter Mode	No	Plain / RAM
KEK	256	AES-CBC	Zeroization service	Hash_DRBG	Output (encrypted)	Plain / RAM

MEKs	512	AES-XTS	Zeroization service	Hash_DRBG	Output (encrypted)	Plain / RAM and AES register
PubKey1	2048	RSA	N/A	Manufacturing	No	Plain / ROM
PubKey2	2048	RSA	N/A	Manufacturing	No	Plain / RAM
SID/BandMaster(s) /EraseMaster PINs	256	PIN	N/A	Electronic input	Output (SHA digest)	SHA digest / RAM
DRBG Internal State	880	DRBG	Zeroization service	Entropy collected from NDRNG at instantiation (Minimum entropy of 8 bits: 7.56)	No	Plain / RAM

Table 7 - Key/CSP

Note that there is no security-relevant audit feature and audit data.

Section 6 – Self Tests

The CM runs self-tests in the following table.

Function	Self-Test Type	Abstract	Failure Behavior
AES256-CBC	Power-On	Encrypt and Decrypt KAT	Enters Boot Error State.
AES256-XTS	Power-On	Encrypt KAT	Enters Boot Error State.
AES256-XTS	Power-On	Decrypt KAT	Enters Boot Error State.
SHA256	Power-On	Digest KAT	Enters Boot Error State.
HMAC-SHA256	Power-On	Digest KAT	Enters Boot Error State.
Hash_DRBG	Power-On	DRBG KAT	Enters Boot Error State.
RSASSA-PKCS#1-v1_5	Power-On	Signature verification KAT	Enters Boot Error State.
RSASSA-PKCS#1-v1_5	Power-On	Signature verification KAT	Enters Boot Error State.
KDF in Counter Mode	Power-On	KDF KAT	Enters Boot Error State
Hash_DRBG	Conditional	Verify newly generated random number not equal to previous one	Enters Error State.
NDRNG	Conditional	Verify newly generated random number not equal to previous one	Enters Error State.
Firmware integrity test	Power-On	Verify signature of	Incoming firmware image is

		downloaded firmware image by RSASSA-PKCS#1-v1_5	not loaded.
Firmware load test	Conditional	Verify signature of downloaded firmware image by RSASSA-PKCS#1-v1_5	Incoming firmware image is not loaded and is not saved.

Table 8 - Self Tests

When 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 7 – Design Assurance

Initial operations to setup this CM are following:

1. Execute setRangeInformationInitialize method.
2. Execute setLogicalPortInfoInitialize method.

The CM switches to a FIPS Approved mode after the initial operation success. When the initial operation succeeds, the CM indicates success on the Status Output interface.

Section 8 – Mitigation of Other Attacks

The CM does not mitigate other attacks beyond the scope of FIPS 140-2 requirements.

Appendix A – EMI/EMC

FIPS 140-2 requires the Federal Communications Commission (FCC) ID, but this CM does not have FCC ID. This CM is a single chip module implemented in a device described in Subpart B, Class A of FCC 47 Code of Federal Regulations Part 15. However, all systems using this CM and sold in the United States must meet these applicable FCC requirements.