FIPS 140-2 Non-Proprietary Security Policy for:

KIOXIA TCG OPAL SSC Crypto Sub-Chip TC58NC1132GTC

KIOXIA CORPORATION

Rev 1.1.0

Overview

KIOXIA TCG OPAL SSC Crypto Sub-Chip TC58NC1132GTC (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 TC58NC1132GTC 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 TC58NC1132GTC 0003 SoC. The logical boundary of the CM is TC58NC1132GTC 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 Lock Checker 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

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

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
SoC	System on a Chip

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:

- Physical single-chip:
  TC58NC1132GTC, Revision 0003
- The sub-chip cryptographic subsystem soft circuitry core:
  TC58NC1132GTC CRPT module, Revision 0001
- The associated firmware: SC01AN

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
AdminSP.SID	Crypto Officer	Role	PIN	$1 / 2^{48} < 1 / 1{,}000{,}000$	$30 / 2^{48} < 1 / 100{,}000$
AdminSP.Admin1	Crypto Officer	Role	PIN	$1 / 2^{48} < 1 / 1{,}000{,}000$	$30 / 2^{48} < 1 / 100{,}000$
LockingSP.Admin1-4	Crypto Officer	Role	PIN	$1 / 2^{48} < 1 / 1{,}000{,}000$	$30 / 2^{48} < 1 / 100{,}000$
LockingSP.User1	User	Role	PIN	$1 / 2^{48} < 1 / 1{,}000{,}000$	$30 / 2^{48} < 1 / 100{,}000$
LockingSP.User2	User	Role	PIN	$1 / 2^{48} < 1 / 1{,}000{,}000$	$30 / 2^{48} < 1 / 100{,}000$
…	…	…	…	…	…
LockingSP.User192	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	RWX (Read,Write,eXecute)	Algorithm	Method
Band Lock/Unlock	Lock or unlock read / write of user data in a band.	LockingSP.Admins	KDK MEKs System MAC Key	R, X R R, X	KBKDF N/A HMAC-SHA256	setSingleRange method
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"				setSingleRange 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[2]	MEKs	X	AES256-XTS	HW auto
Cryptographic Erase	Erase user data (in cryptographic means) by changing the key that derives the data encryption key.	LockingSP.Admin1-4	KDK MEKs System MAC Key System Enc Key	W R, X R, W R, X R, X	Hash_DRBG KBKDF HMAC-SHA256 AES256-CBC	genKey method
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"				genKey method
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.	LockingSP.Admin1-4 LockingSP.user"X+1"	KDK MEKs System MAC Key System Enc Key	W R, X R, W R, X R, X	Hash_DRBG KBKDF HMAC-SHA256 AES256-CBC	tcgErase method

[2] The band has to be unlocked by corresponding role beforehand.

Download Port Lock/Unlock	Lock / unlock firmware download.	AdminSP.SID	N/A	N/A	N/A	setDownloadPort method
Firmware Verification	Digital signature verification for firmware outside the CM.	None	PubKey2	R, X	RSASSA-PKCS#1-v1_5	checkPKCSExternal method
Firmware Download	Download a firmware image[3].	AdminSP.SID	PubKey1	R, X	RSASSA-PKCS#1-v1_5	reloadCrypto method
Random Number Generation	Provide a random number generated by the CM.	None	DRBG Internal Value	R	Hash_DRBG	getRandomData method
Set Band Position and Size	Set the location and size of the band.	LockingSP.Admin1-4	KDK MEKs System MAC Key System Enc Key	W R, X R, W R, X R, X	Hash_DRBG KBKDF HMAC-SHA256 AES256-CBC	setSingleRange method
Set Band Position and Size for Band of Single User Mode	Set the location and size of the band ” of single user mode	LockingSP.Admin1-4 LockingSP.User”X+1”				setSingleRange method
Set PIN	Set PIN (authentication data).	AdminSP.SID, AdminSP.Admin1, LockingSP.Admin1-4, LockingSP.User1-192	N/A System MAC Key System ENC Key	N/A R, X R, X	SHA256 HMAC-SHA256 AES256-CBC	setPIN method
Set PIN for Band of Single User Mode	Set PIN (authentication data) of authority for band ” of single use mode	LockingSP.User1-192				setPIN method
Authority Enable/Disable	Enable/Disable the authority.	AdminSP.SID LockingSP.Admins	System MAC Key System ENC Key	R, X R, X	HMAC-SHA256 AES256-CBC	setAuthority method
Revert	Initialize the band State and disable band lock setting.	AdminSP.SID, AdminSP.Admin1	N/A KDK MEKs System MAC Key System Enc Key	N/A W R, X R, W R, X R, X	SHA256 Hash_DRBG KBKDF HMAC-SHA256 AES256-CBC	revert method
Data Locking Protection Enable	Enable Data protection with band lock setting.	AdminSP.SID LockingSP.Admins	N/A System MAC Key System ENC Key	N/A R, X R, X	SHA256 HMAC-SHA256 AES256-CBC	activate method reactivate method
Sanitize	Erase all user data (in cryptographic means) by changing the key that derives the data encryption key.	AdminSP.SID, AdminSP.Admin1, LockingSP.Admin1-4	KDK MEKs System MAC Key System ENC Key	W R, X R, W R, X R, X	Hash_DRBG KBKDF HMAC-SHA256 AES256-CBC	sanitize method

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

Format Namespace	Erase user data (in cryptographic means) on Namespace by changing the key that derives the data encryption key.	AdminSP.SID, AdminSP.Admin1, LockingSP.Admin1-4, LockingSP.User1-192	KDK MEKs System MAC Key System ENC Key	W R, X R, W R, X R, X	Hash_DRBG KBKDF HMAC-SHA256 AES256-CBC	FormatNS method
Namesapace Create/Delete	Create and delete Namespace.	AdminSP.SID, AdminSP.Admin1, LockingSP.Admin1-4, LockingSP.User1	KDK MEKs System MAC Key System ENC Key	W R, X R, W R, X R, X	Hash_DRBG KBKDF HMAC-SHA256 AES256-CBC	notifyNSInformation method
Band Set Enable	Set the location, size and lock state of the band.	LockinSP.Admins	KDK MEKs System MAC Key System Enc Key	W R, X R, W R, X R, X	Hash_DRBG KBKDF HMAC-SHA256 AES256-CBC	AssignNSGlobal method AssignNSNonGlobal method
Band Set Disable	Initialize the location, size and lock state of the band.	LockingSP.Admins	KDK MEKs System MAC Key System Enc Key	R, X R, W R, X R, X	KBKDF HMAC-SHA256 AES256-CBC	DeassignNSGlobal method DeassignNSNonGlobal method
Show Status	Report status of the CM.	None	N/A	N/A	N/A	Method status
Zeroization	Erase CSPs.	None[4]	RKey KDK MEKs System MAC Key System Enc Key DRBG Internal Value DRBG Seed	W W W W W W W W	N/A	zeroization method
Reset	Runs POSTs, generate DRBG CSPsanddelete CSPs in RAM.	None	DRBG Internal Value DRBG Seed	W W,X	Hash_DRBG NDRNG	Power on reset

Table 4 - FIPS Approved services

Algorithm	Description	CAVP Certification Number
AES256-CBC	Encryption, Decryption	#C1925
AES256-XTS[5]	Encryption, Decryption	#C1925
SHA256	Hashing	#C1925
HMAC-SHA256	Message Authentication Code	#C1925

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

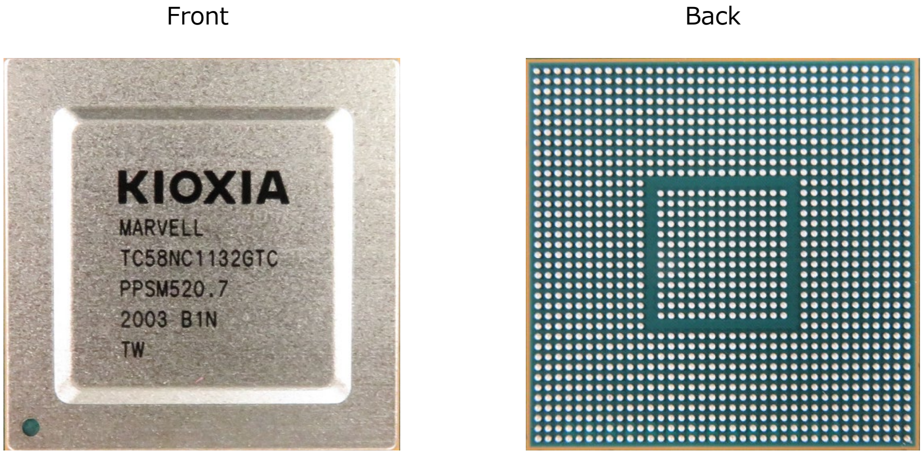
[5] ECB mode is used as a prerequisite of XTS mode which is used only for hardware storage application. ECB is not directly used in services of the cryptographic module. The CM performs a check that the XTS Key1 and XTS Key2 are different at the time of key generation according to IG A.9.

RSASSA-PKCS#1-v1_5	Function: Signature Verification Key Size: 2048 bits	#C2009
Hash_DRBG	Hash based: SHA256	#C2002
KBKDF	Counter Mode MACs: HMAC-SHA256	#C2001
CKG	Cryptographic Key Generation referred by SP800-133 Revision 2 sections 6.1 and 6.2.2	Vendor Affirmation
KTS	Key Transport Scheme referred by IG D.9; AES and HMAC Cert. #C1925	#C1925
NDRNG[6]	Hardware RNG used to seed the approved Hash_DRBG. Minimum entropy of 8 bits is 6.74.	ENT

Table 5 - FIPS Approved Algorithms

Section 3 – Physical Security

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


Front

Back

Figure 1 - TC58NC1132GTC 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.

[6] The NDRNG is a hardware module used as an entropy source inside the CM boundary. The NDRNG supplies the Hash_DRBG with 512 bits entropy input. From Table 5, this input contains about 431 bits of entropy, which is sufficient entropy to obtain 256 bits of security strength.

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
KDK	256	KBKDF	Zeroization service Key update services[7]	Hash_DRBG	Output (encrypted)	Plain / RAM
MEKs	512	AES-XTS	Zeroization service	KDF in Counter Mode	No	Plain / AES register
PubKey1	256	RSA	N/A	Manufacturing	No	SHA digest / OTP
PubKey2	2048	RSA	N/A	Manufacturing	No	Plain / ROM
PINs	256	PIN	N/A	Electronic input	Output (SHA digest/ encrypted)	SHA digest / RAM
DRBG Internal Value	V: 440 bits C: 440 bits	DRBG	Zeroization service	SP800-90A Instantiation of Hash_DRBG	No	Plain / RAM
DRBG Seed	Entropy Input String	DRBG	Zeroization service	Entropy collected from NDRNG at	No	Plain / RAM

[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, Namesapace Create/Delete and Band Set Enable.

	and Nonce: 512 bits			instantiation (Minimum entropy of 8 bits: 6.74)		

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.
KDF in Counter Mode	Power-On	KDF KAT	Enters Boot Error State
NDRNG (Health tests of noise source at startup.)	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
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.
NDRNG (Continuous noise source health tests during operation.)	Conditional	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.

Firmware load test	Conditional[8]	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. Load Firmware into the CM.
2. Load System area including CSPs into the CM.
3. Execute setAllRangeForBoot method.
4. Execute setDownloadPort method.
5. Execute setCCPUServiceACL method.
6. Execute notifyNamespaceInformation 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

[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.