KIOXIA

FIPS 140-2 Non-Proprietary Security Policy for:

KIOXIA TCG OPAL SSC Self-Encrypting Solid State Drive CD5 Series

KIOXIA CORPORATION

Rev 2.0.0

Overview

The KIOXIA TCG OPAL SSC Self-Encrypting Solid State Drive (listed in Section1.1 Product Version) is used for solid state drive data security. This Cryptographic Module (CM) provides various cryptographic services using FIPS approved algorithms. Services include hardware-based data encryption, cryptographic erase, and FW download.

This CM is multiple-chip embedded, and the physical boundary of the CM is the entire SSD. The logical boundary is PCIe (NVMe) interface (same as the physical boundary). The physical interface for power-supply and for communication is one PCIe (NVMe) connector. The logical interface is the PCIe (NVMe), TCG SWG, and OPAL SSC.

The CM has the non-volatile storage area for not only user data but also the keys, CSPs, and FW. The latter storage area is called the “system area”, which is not logically accessible by the host application.

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	PCIe connector
Control Input	PCIe connector
Data Output	PCIe connector
Status Output	PCIe connector
Power Input	PCIe connector

Table 2 - Physical/Logical Port Mapping

Acronyms

AES	Advanced Encryption Standard
CM	Cryptographic Module
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
FW	Firmware
HMAC	Keyed-Hashing for Message Authentication code
KAT	Known Answer Test
KEK	Key Encryption Key
LBA	Logical Block Address
MEK	Media Encryption Key
MSID	Manufactured SID
NDRNG	Non-Deterministic Random Number Generator
NVMe	Non-Volatile Memory Express
PCB	Printed Circuit Board
PCIe	Peripheral Component Interconnect Express
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. The CM provides services defined in Section 2.1 and other non-security related services.

Section 1.1 – Product Version

The following models are validated with the following FW version and HW version.

HW version, Drive capacity: A2 with KCD5FLUG960G, 960 GB [1]
A2 with KCD5FLUG1T92, 1920 GB [1]
A2 with KCD5FLUG3T84, 3840 GB [1]
A2 with KCD5FLUG7T68, 7680 GB [1]
A3 with KCD5FLUG960G, 960 GB [2]
A3 with KCD5FLUG1T92, 1920 GB [2]
A3 with KCD5FLUG3T84, 3840 GB [2]
A3 with KCD5FLUG7T68, 7680 GB [2]

FW version: KCD50107 [1], KCD50108 [2]

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.User1-9	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.

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	Command /Method
Band Lock/Unlock	Lock or unlock read / write of user data in a band.	LockingSP.Admin1-4	KEK MEKs Table MAC Key	R, X R R, X	AES256-CBC HMAC-SHA256	TCG Set 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"[3]				TCG Set Method
Data Read/Write	Encryption / decryption of user data to/from unlocked band.	None[4]	MEKs	X	AES256-XTS (#5067, #5068)	Read Command, Write Command
Cryptographic Erase	Erase user data (in cryptographic means) by changing the data encryption key.	LockingSP.Admin1-4	KEK MEKs DRBG Internal Value	R, X W R, X	AES256-CBC Hash_DRBG	TCG 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 data encryption key.	LockingSP.User"X+1"[3]				TCG Genkey Method
Cryptographic Erase and Initialize Band State	Erase user data in band"X" of single user mode (in cryptographic means) by changing the data encryption key, and initialize the band state.	LockingSP.Admin1-4, LockingSP.User"X+1"[3]	KEK MEKs PINs Table MAC Key DRBG Internal Value	R, X W W R, X R, X	AES256-CBC Hash_DRBG HMAC-SHA256	TCG Erase Method
Sanitize	Erase all user data (in cryptographic means).	AdminSP.SID, AdminSP.Admin1, LockingSP.Admin1-4	RKey KEK MEKs PINs Table MAC Key DRBG Internal Value	R, X R, X, W W W R, X R, X	AES256-CBC Hash_DRBG HMAC-SHA256	TCG Revert Method, TCG RevertSP Method, Sanitize Command
Format NVM	Erase all user data (in cryptographic means).	LockingSP.Admin1-4, LockingSP.User1-9	KEK MEKs DRBG Internal Value	R, X W R, X	AES256-CBC Hash_DRBG	Format NVM Command

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

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

[3] "X" is band number.

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

Firmware Download	Enable / Disable firmware download and load a complete firmware image, and save it. If the code passes "Firmware load test", the device is reset and will run with the new code. Only firmware versions validated in CMVP are allowed to be downloaded.	AdminSP.SID	Table MAC Key PubKey	R, X R, X	HMAC-SHA256 RSASSA-PKCS #1-v1_5	TCG Set Method Firmware Image Download Command Firmware Commit Command
Random Number Generation	Provide a random number generated by the CM.	None	DRBG Internal Value	R, X	Hash_DRBG	TCG Random Method
Reset	Run POSTs and delete CSPs in RAM.	None	N/A	N/A	N/A	Power on reset
Set Band Position and Size	Set the location and size of the band.	LockingSP.Admin1-4	KEK MEKs Table MAC Key DRBG Internal Value	R, X R, W R, X R, X	AES256-CBC Hash_DRBG HMAC-SHA256	TCG Set Method
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.Admin1-4, LockingSP.User"X+1"[3]				TCG Set Method
Set PIN	Set PIN (authentication data).	AdminSP.SID, AdminSP.Admin1, LockingSP.Admin1-4, LockingSP.User1-9[5]	PINs Table MAC Key	W R, X	SHA256 HMAC-SHA256	TCG Set Method
Set PIN for Band of Single User Mode	Set PIN (authentication data) of authority for band"X" of single use mode.	LockingSP.User"X+1"[3]				TCG Set Method
Show Status	Report status of the CM.	None	N/A	N/A	N/A	Security Send Command, Security receive Command, Read Command, Write Command, Sanitize Command, FormatNVM Command, Firmware Image Download Command Firmware Commit Command, Zeroization Command
Zeroization	Erase user data in all bands by zeroizing the data encryption key, and zeroize other CPSs.	None[6]	RKey KEK MEKs Table MAC Key DRBG Internal Value	W W W W W	N/A	Zeroization Command

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

Entry Single User Mode	Entry for single user mode.[7]	AdminSP.SID	Table MAC Key	R, X	HMAC-SHA256	TCG Activate Method
		LockingSP.Admin1-4				TCG Reactivate Method
Exit Single User Mode	Exit from single use mode.	LockingSP.Admin1-4	PINs Table MAC Key	W R, X	HMAC-SHA256	TCG Reactivate Method
Revert	Initialize the band state.	AdminSP.SID, AdminSP.Admin1[8]	RKey KEK MEKs PINs Table MAC Key DRBG Internal Value	R, X W W W R, X R, X	AES256-CBC Hash_DRBG HMAC-SHA256	TCG Revert Method
		LockingSP.Admin1-4				TCG RevertSP Method
Authority Enable/Disable	Enable/Disable the authority.	AdminSP.SID LockingSP.Admin1-4	Table MAC Key	R, X	HMAC-SHA256	TCG Set Method

Table 4 - FIPS Approved services

Algorithm	Description	CAVP Certification Number
AES256-CBC	Encryption, Decryption	#5062
AES256-XTS[9]	Decryption	#5068
AES256-XTS[9]	Encryption	#5067
SHA256	Hashing	#4128
HMAC-SHA256	Message Authentication Code	#3388
RSASSA-PKCS#1-v1_5	Function: Signature Verification Key Size: 2048 bits	#2753
Hash_DRBG	Hash based: SHA256	#1890
CKG	Cryptographic Key Generation referred by SP800-133	Vendor Affirmation

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 - Allowed Algorithm

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

[7] Single User Mode is defined in the TCG Opal SSC Feature Set, and is set for each individual band. The band setting Single User Mode is managed only by the associated LockingSP.User role.

[8] TCG Revert method also may be invoked using the PSID.

[9] 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. AES256 XTS can only be used in storage application in FIPS mode.

Section 3 – Physical Security

The CM has the following physical security:

- Production-grade components with standard passivation
- Exterior of the drive is opaque
- Two tamper-evident security seals are applied to the CM in factory
  - Two opaque and tamper-evident security seals (VOID LABEL L and VOID LABEL M or VOID LABEL P and VOID LABEL Q) are applied to side of the CM. These seals prevent cover removal and an attacker to access the PCB.
- The tamper-evident security seals cannot be penetrated or removed and reapplied without tamper-evidence

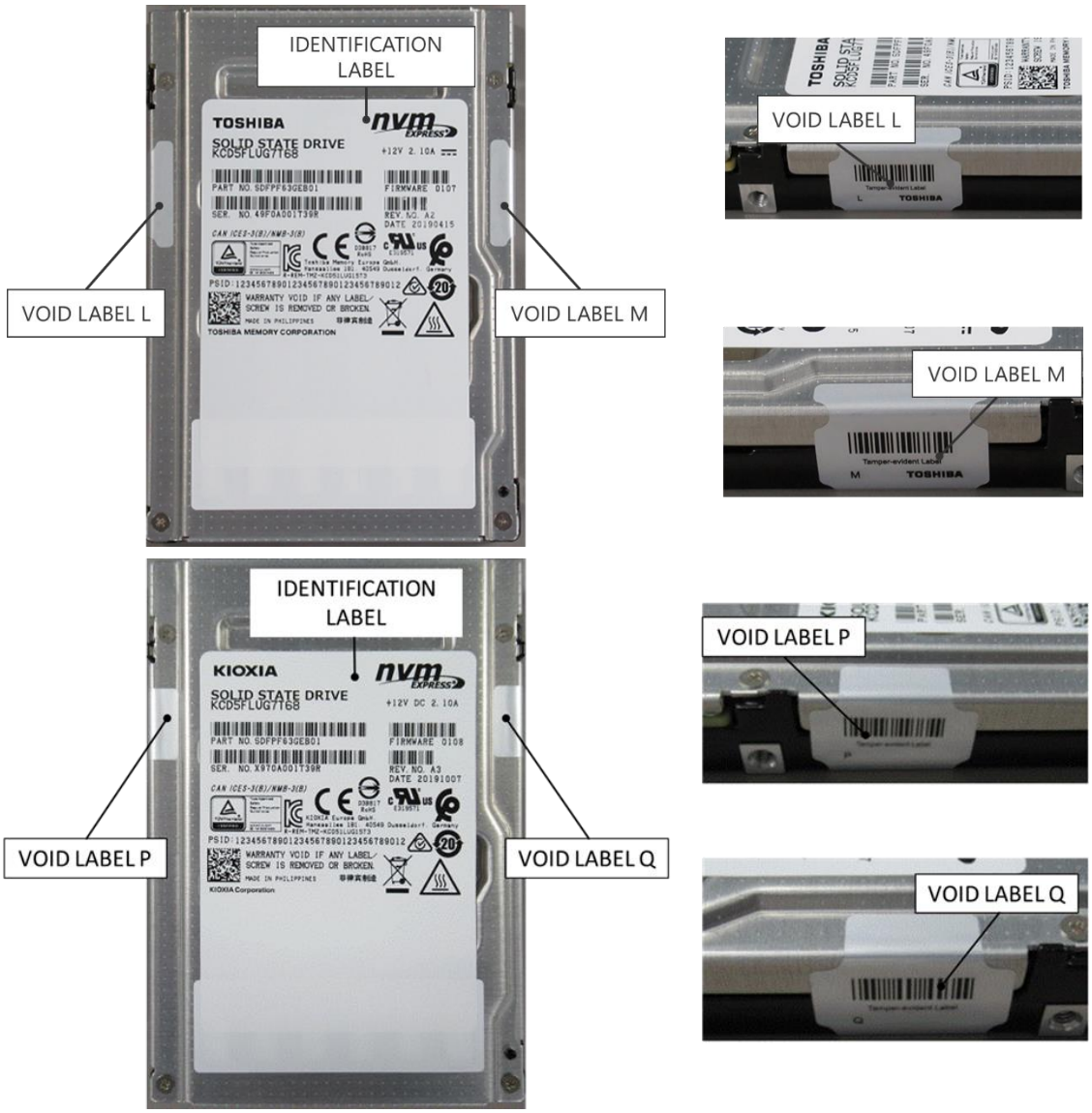

Figure 1 - Tamper-evident security seals

The operator is required to inspect the CM periodically (every month or every two months) for one or more of the following tamper evidence. If the operator discovers tamper evidence, the CM should be removed.

- Message “VOID” on security seal or the CM
- Text on security seals do not match original
- Cutting line on security seal
- Security seal cutouts do not match original

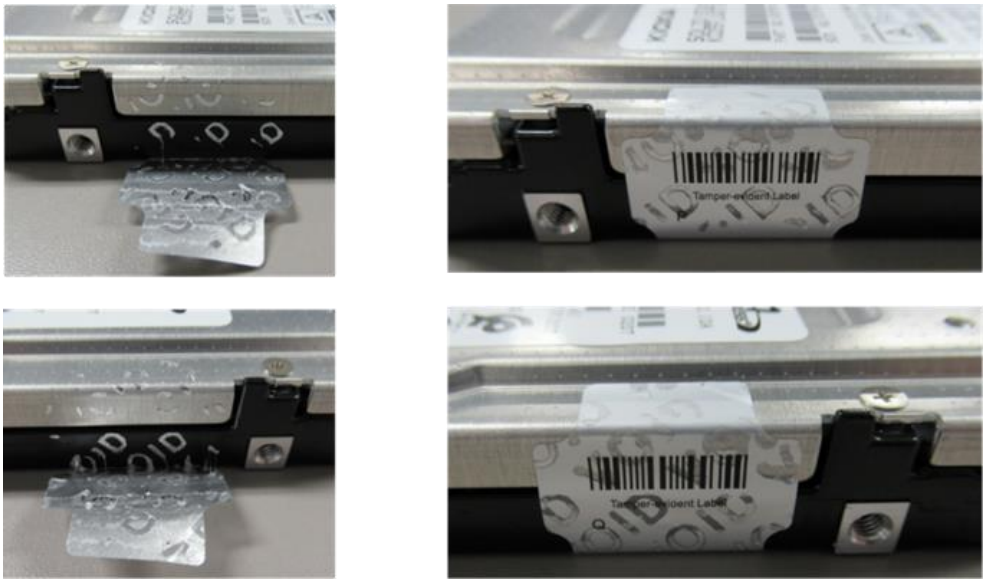

Figure 2 -Mark of alphabetic character(s) which constitute a word “VOID”

Figure 3 - Cutting line on security seals

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	AES-CBC	Zeroization service	Hash_DRBG	No	Plain / OTP
KEK	256	AES-CBC	Zeroization service	Hash_DRBG	No	Encrypted by RKey / System Area
Table MAC Key	256	HMAC	Zeroization service	Hash_DRBG	No	Encrypted by KEK / System Area
MEKs	512	AES-XTS	Zeroization service	Hash_DRBG	No	Encrypted by KEK / System Area
PubKey	2048	RSA	N/A	Manufacturing	No	Plain / RAM
PINs	256	PIN	Revert service	Electronic input	No	SHA digest / System Area
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 and Nonce: 512 bits	DRBG	Zeroization service	Entropy collected from NDRNG at instantiation (Minimum entropy of 8 bits: 7.56)	No	Plain / RAM

Table 7 - Keys and CSPs

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
Firmware Integrity Test	Power-On	HMAC 256bit	Enters Boot Error State.
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.
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 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 – Secure Installation

Initial operations to setup this CM are following:

1. Get MSID from PCIe (NVMe) interface.
2. Activate
3. Set range configurations with AdminSP.SID authority by using MSID as PIN.
4. Change AdminSP.SID PIN and AdminSP.Admin1 PIN.
5. Set PortLocked in Download port to “TRUE”.

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

The CM was tested by NVLAP accredited laboratory to be Subpart B, Class B of FCC 47 Code of Federal Regulations Part 15 compliant.