

FIPS 140-2 Non-Proprietary Security Policy for:

KIOXIA TCG Enterprise SSC Self-Encrypting Solid State Drive (PX04S model) Type B1



KIOXIA CORPORATION

Rev 3.0.0

OVERVIEW	3
ACRONYMS	4
SECTION 1 – MODULE SPECIFICATION.....	5
SECTION 1.1 – PRODUCT VERSION	5
SECTION 2 – ROLES SERVICES AND AUTHENTICATION	5
SECTION 2.1 – SERVICES.....	6
SECTION 3 – PHYSICAL SECURITY.....	7
SECTION 4 – OPERATIONAL ENVIRONMENT.....	9
SECTION 5 – KEY MANAGEMENT	9
SECTION 6 – SELF TESTS	10
SECTION 7 – DESIGN ASSURANCE	11
SECTION 8 – MITIGATION OF OTHER ATTACKS	11
APPENDIX A – EMI/EMC	11

Overview

The KIOXIA TCG Enterprise SSC Self-Encrypting Solid State Drive (listed in Section 1.1 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 SAS interface (same as the physical boundary). The physical interface for power-supply and for communication is one SAS connector. The CM is connected with host system by SAS cable. The logical interface is the SAS, TCG SWG, and Enterprise 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 / addressable by the host application.

The CM is intended to meet the requirements of FIPS140-2 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	SAS connector
Control Input	SAS connector
Data Output	SAS connector
Status Output	SAS connector
Power Input	SAS connector

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
EDC	Error Detection Code
FW	Firmware
HMAC	Keyed-Hashing for Message Authentication code
KAT	Known Answer Test
LBA	Logical Block Address
MSID	Manufactured SID
NDRNG	Non-Deterministic Random Number Generator
PCB	Printed Circuit Board
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: A1 with PX04SVQ080B [1]
 A1 with PX04SVQ160B [1]
 A2 with PX04SVQ080B [2]
 A2 with PX04SVQ160B [2]

FW version: MS01 [1], MS02 [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
EraseMaster	Crypto Officer	Role	PIN	$1/2^{48} < 1/1,000,000$	$15,000 / 2^{48} < 1 / 100,000$
SID	Crypto Officer	Role	PIN	$1/2^{48} < 1/1,000,000$	$15,000 / 2^{48} < 1 / 100,000$
BandMaster0	User	Role	PIN	$1/2^{48} < 1/1,000,000$	$15,000 / 2^{48} < 1 / 100,000$
BandMaster1	User	Role	PIN	$1/2^{48} < 1/1,000,000$	$15,000 / 2^{48} < 1 / 100,000$
...
BandMaster8	User	Role	PIN	$1/2^{48} < 1/1,000,000$	$15,000 / 2^{48} < 1 / 100,000$

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 4msec when authentication attempt fails, so the maximum number of authentication attempts is 15,000 times in 1 min. Therefore the probability that random attempts in 1min will succeed is $15,000 / 2^{48} < 1 / 100,000$. Even if TryLimit¹ 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, eXecute)	Algorithm	Method
Band Lock/Unlock	Block or allow read (decrypt) / write (encrypt) of user data in a band. Locking also requires read / write locking to be enabled.	BandMaster0 ... BandMaster8	Table MAC Key	X	HMAC-SHA256	SCSI SECURITY PROTOCOL IN Command (TCG Set Method)
Cryptographic Erase	Erase user data (in cryptographic means) by changing the data encryption key.	EraseMaster	MEK(s) RKey Table MAC Key	W X X	Hash_DRBG AES256-CBC HMAC-SHA256	SCSI SECURITY PROTOCOL IN Command (TCG Erase Method)
Data read/write (decrypt/encrypt)	Encryption / decryption of unlocked user data to/from band.	None ³	MEKs	X	AES256-XTS (#3486, #3487)	SCSI READ/WRITE Commands
Firmware Download	Enable / Disable firmware download and load a complete firmware image ⁴ , and save it. If the code passes "Firmware load test", the device is reset and will run with the new code.	SID	Table MAC Key PubKey	X X	HMAC-SHA256 RSASSA-PKCS #1-v1_5	SCSI SECURITY PROTOCOL IN Command (TCG Set Method), SCSI WRITE BUFFER Command
Random Number generation	Provide a random number generated by the CM.	None	DRBG Internal Value	R	Hash_DRBG	SCSI SECURITY PROTOCOL IN Command (TCG Random Method)
Reset(run POSTs)	Runs 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 LBA range.	BandMaster0 ... BandMaster8	Table MAC Key	X	HMAC-SHA256	SCSI SECURITY PROTOCOL IN Command (TCG Set Method)
Set PIN	Setting PIN (authentication data).	EraseMaster, SID, BandMaster0 ... BandMaster8 ⁵	RKey Table MAC Key	X X	AES256-CBC HMAC-SHA256 SHA256	SCSI SECURITY PROTOCOL IN Command (TCG Set Method)
Show Status	Report status of the CM.	None	N/A	N/A	N/A	SCSI REQUEST SENSE Command

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

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

⁴ Only the CMVP validated version is to be used.

⁵ Each role can set a PIN for themselves only.

Zeroization	Erase user data in all bands by changing the data encryption key, initialize range settings, and reset PINs for TCG.	None ⁶	RKey Table MAC KEY MEKs PIN	X,W X,W W W	AES256-CBC HMAC-SHA256 Hash_DRBG	SCSI SECURITY PROTOCOL IN Command (TCG RevertSP Method)
-------------	--	-------------------	--------------------------------------	----------------------	--	---

Table 4 - FIPS Approved services

Algorithm	Description	CAVP Certification Number
AES256-CBC	Encryption, Decryption	#3485
AES256-XTS ⁷	Decryption	#3487
AES256-XTS ⁷	Encryption	#3486
SHA256	Hashing	#2879
HMAC-SHA256	Message Authentication Code	#2231
RSASSA-PKCS#1-v1_5	Function: Signature Verification Key Size: 2048 bits	#1795
Hash_DRBG	Hash based: SHA256	#867

Table 5 - FIPS Approved Algorithms

Algorithm	Description
NDRNG ⁸	Hardware RNG used to seed the approved Hash_DRBG. Minimum entropy of 8 bits is 7.19.

Table 6 - Non-FIPS Approved Algorithm

Section 3 – Physical Security

The CM has the following physical security:

- Production-grade components with standard passivation
- Exterior of the drive is opaque
- Five tamper-evident security seals are applied to the CM in factory
 - Three opaque and tamper-evident security seals (VOID LABEL H, VOID LABEL J and VOID LABEL K) are applied to side of the CM and edge of OUTER SHEET⁹. These seals prevent cover removal and an attacker to access the PCB
 - Two opaque and tamper-evident security seals (VOID LABEL F and VOID LABEL G) are

⁶ Need to input PSID, which is public drive-unique value used for the TCG RevertSP method. The PSID is printed on identification label of the module.

⁷ 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.

⁸ The NDRNG is a hardware module inside the CM boundary. The NDRNG supplies the Hash_DRBG with sufficient entropy to obtain 256 bits of security strength.

⁹ OUTER SHEET is an opaque seal covering some holes of the top cover. It cannot leave "VOID" message, but leaves the evidence of the cut.

applied to side of the CM. These seals prevent cover removal

- The tamper-evident security seals cannot be penetrated or removed and reapplied without tamper-evidence

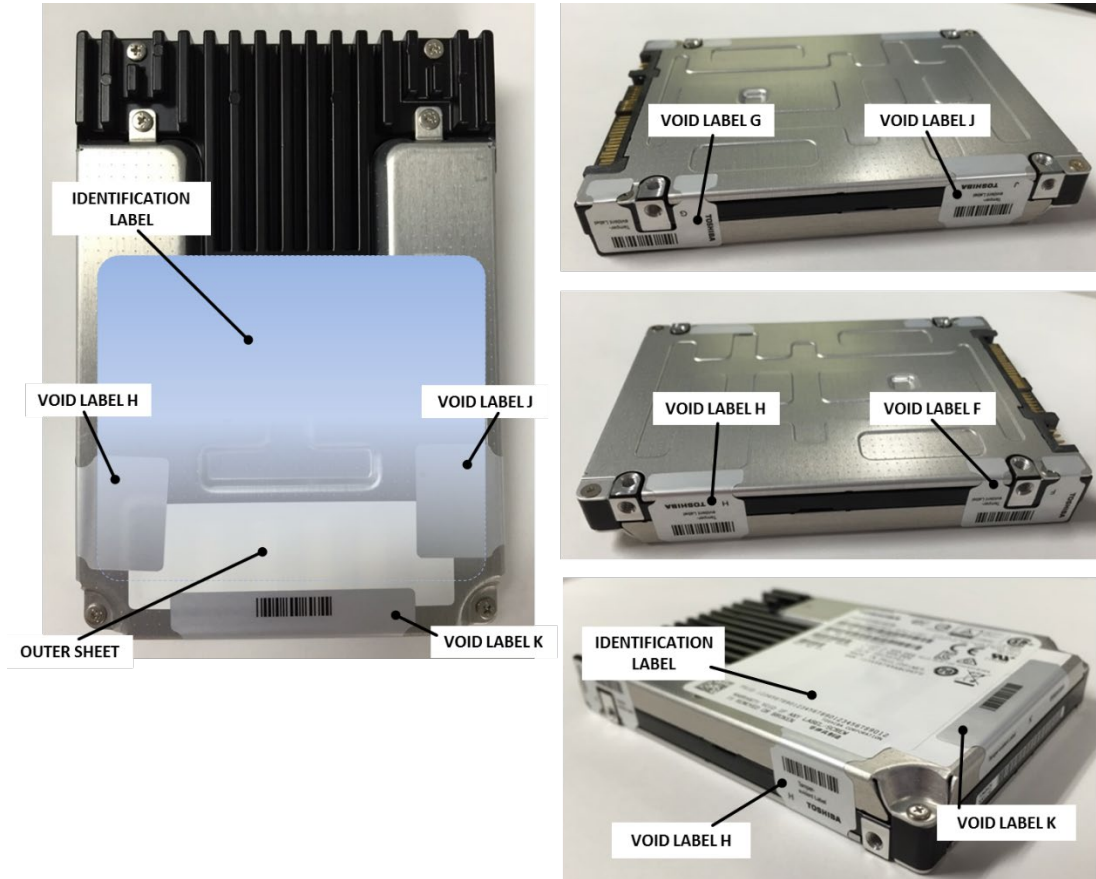


Figure 1 - Tamper-evident security seals

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 the following tamper evidence, the CM should be removed:

- Message "VOID" on security seal or the CM
- Text on security seals that do not match original
- Cutting line on security seal or OUTER SHEET
- Security seal cutouts that do not match original



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



Figure 3 - Cutting line (Security seals and OUTER SHEET)

Section 4 – Operational Environment

Operational Environment requirements are not applicable because the CM operates in a non-modifiable operational 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	Type/ Algorithm	Zeroize Method	Establishment	Output	Persistence/Storage
BandMaster/Erase Master/SID PINs	256	PIN	Zeroization service	Electronic input	No	SHA digest/System Area
MEKs	512	AES-XTS	Zeroization service	DRBG	No	Encrypted by RKey / System Area
MSID	256	Public	N/A(Public)	Manufacturing	Output: Host can retrieve	Plain / System Area

PubKey	2048	RSA	N/A(Public)	Manufacturing	No	Plain / System Area
RKey	256	AES-CBC	Zeroization service	DRBG	No	Obfuscated(Plain in FIPS means) / System Area
DRBG Internal Value	V: 440 bits C: 440 bits	DRBG	Power-Off	SP800-90A Instantiation of Hash_DRBG	No	Plain/RAM
DRBG Seed	Entropy Input String and Nonce: 512 bits	DRBG	Power-Off	Entropy collected from NDRNG at instantiation (Minimum entropy of 8 bits: 7.19)	No	Plain/RAM
Table MAC Key	256	HMAC	Zeroization service	DRBG	No	Encrypted by RKey / System Area

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 Check	Power-On	EDC 32-bit	Enters Boot Error State
SHA256	Power-On	Digest KAT	Enters Boot Error State
HMAC-SHA256	Power-On	Digest KAT	Enters Boot Error State
AES256-CBC	Power-On	Encrypt and Decrypt KAT	Enters Boot Error State
AES256-XTS	Power-On	Decrypt KAT	Enters Boot Error State
AES256-XTS	Power-On	Encrypt 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 – Design Assurance

Initial operations to setup this module are following:

1. Get MSID from SAS interface.
2. Set range configurations with BandMaster(s) authority by using MSID as PIN.
3. Change BandMaster(s)/EraseMaster/SID PINs.
4. Set LockOnReset in Download port to “Power Cycle”.
5. In BandMaster1, set ReadLockEnabled and WriteLockEnabled to 1 and set LockOnReset to “Power Cycle”.
6. Power Cycling.

To get more details, refer to the guidance document provided with the CM.

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. Because this CM is 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.