KIOXIA

KIOXIA Corporation

KIOXIA FIPS TC58NC1137GTC Crypto Sub-Chip Class A1

FIPS 140-3 Non-Proprietary Security Policy

Rev 1.4.0

KIOXIA

Table of Contents

KIOXIA

List of Tables

List of Figures

KIOXIA

1 General

1.1 Overview

This document explains precise specification of the security rules about KIOXIA FIPS TC58NC1137GTC Crypto Sub-Chip Class A1. The Cryptographic Module (CM) meets the requirements of FIPS 140-3 Security Level 2 Overall.

1.2 Security Levels

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
	Overall Level	2

Table 1: Security Levels

1.3 Additional Information

Acronyms

AES Advanced Encryption Standard
APT Adaptive Proportion Test
CAST Cryptographic Algorithm Self-Test
CM Cryptographic Module
DRBG Deterministic Random Bit Generator
HMAC The Keyed-Hash Message Authentication code
KAT Known Answer Test
LBA Logical Block Address
LMS Leighton-Micali Signature
POST Power on Self-Test
PSID Printed SID
RCT Repetition Count Test
SED Self-Encrypting Drive
SHA Secure Hash Algorithm
SID Security ID
SSP Sensitive Security Parameter
TCG Trusted Computing Group

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

KIOXIA FIPS TC58NC1137GTC Crypto Sub-Chip Class A1 (listed in Section2.2 Tested and Vendor Affirmed Module Version and Identification) 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 TC58NC1137GTC 0003 SoC (see Figure 2 in Section 7.1). The CM is embedded in TCG OPAL compliant solid state drive controllers which provides user data encryption/decryption through build-in HW engines.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics: SubChip

Cryptographic Boundary:

The cryptographic boundary is defined as the set of TC58NC1137GTC CPRT module as soft circuity core and SC02DN as associated firmware, and the physical perimeter is defined as the surface of TC58NC1137GTC 0003 SoC.
Components of the CM is shown with gray background include processor and memories (volatile and non-volatile memory) and HW circuitry for cryptographic processing. Physical ports bordering outside the CM's boundary and the data passing over them are also indicated (see Section 3.1 for details on physical ports and interfaces).

Overview block diagram of the CM is shown below.

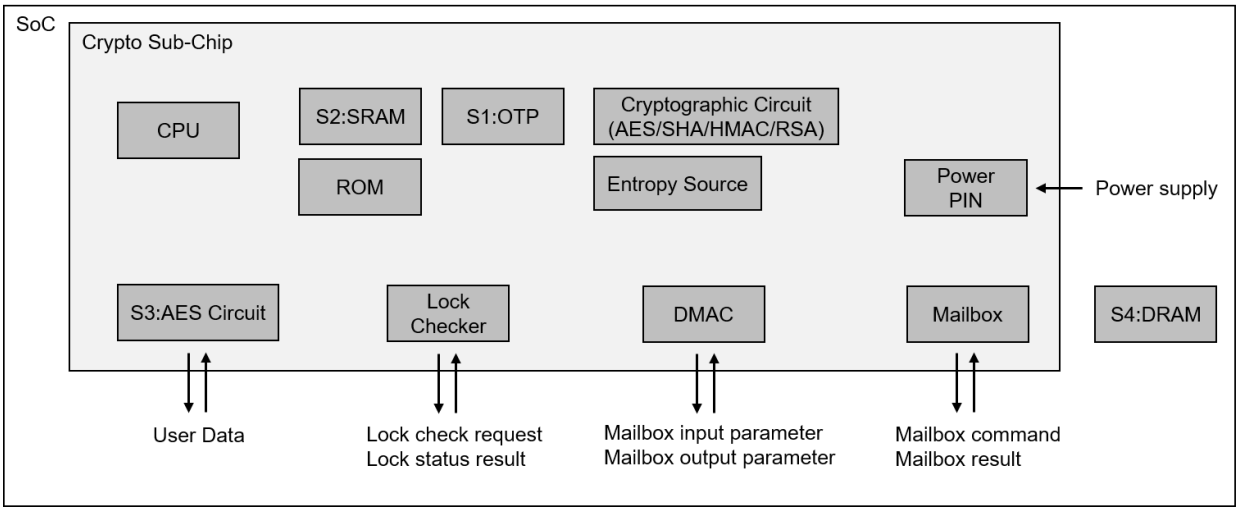

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
KIOXIA FIPS TC58NC1137GTC Crypto Sub-Chip Class A1	0003	SC02DN	Cortex-M3	Single-Chip: TC58NC1137GTC-0003; Soft Circuitry core: CPRT module 0002

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	Approved mode	Approved	The service indicators in Table 12 are equivalent to the indicator for approved mode.

Table 3: Modes List and Description

The CM has one approved mode of operation and CM is always in approved mode of operation after initial operations are performed (See Section 11.1).

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A7087	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A7087	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-XTS Testing Revision 2.0	A7087	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
ECDSA SigGen (FIPS186-5)	A7223	Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A7223	Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
Hash DRBG	A7173	Prediction Resistance - No Mode - SHA2-256	SP 800-90A Rev. 1
HMAC-SHA2-256	A7087	Key Length - Key Length: 256	FIPS 198-1
KDF SP800-108	A7174	KDF Mode - Counter Supported Lengths - Supported Lengths: 512	SP 800-108 Rev. 1
LMS SigVer	A7297	LMS Modes - LMS_SHA256_M32_H15	SP 800-208
RSA SigVer (FIPS186-5)	A7087	Modulo - 2048, 3072 Signature Type - pkcs1v1.5	FIPS 186-5
SHA2-256	A7087	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-384	A7087	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

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.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric	N/A	SP800-133 r2, Section 4, example 1

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
KDK Generation	CKG	Generate KDK with random number		Hash DRBG: (A7173) CKG: ()
MEKs Generation	KBKDF	Derive MEKs to be used in external AES circuit based on KDK		KDF SP800-108: (A7174)
HMAC Generation/Verification	MAC	HMAC generation and verification for arbitrary data		HMAC-SHA2-256: (A7087)
KTS	KTS-Unwrap KTS-Wrap	Transport data to/from external memory area	IG D.G:approved method from IG D.G Caveat:Key establishment methodology provides 256 bits of security strength	AES-CBC: (A7087) HMAC-SHA2-256: (A7087)
User Data Encryption/Decryption	BC-UnAuth	Encryption / Decryption of user data		AES-XTS Testing Revision 2.0: (A7087) AES-ECB: (A7087)
FW digital signature verification 1	DigSig-SigVer	Signature verification for firmware image using LMS		LMS SigVer: (A7297) SHA2-256: (A7087)
FW digital signature verification 2	DigSig-SigVer	Signature verification for firmware image using RSA		RSA SigVer (FIPS186-5): (A7087) SHA2-384: (A7087)
Signature Generation	DigSig-SigGen	Signature generation for arbitrary data		ECDSA SigGen (FIPS186-5): (A7223)
Signature Verification	DigSig-SigVer	Signature verification for arbitrary data		ECDSA SigVer (FIPS186-5): (A7223)
Hash calculation	SHA	Calculate hash for the arbitrary data		SHA2-256: (A7087)

Name	Type	Description	Properties	Algorithms
				SHA2-384: (A7087)
Random Number Generation	DRBG	Generate Random Number		Hash DRBG: (A7173)
Entropy Generation	ENT-ESV	Entropy Source (E275)		

Table 6: Security Function Implementations

The CM does not implement any Non-Approved Security Function Implementations in the Approved Mode of Operation.

2.7 Algorithm Specific Information

N/A for this module.

2.8 RBG and Entropy

Cert Number	Vendor Name
E275	KIOXIA Corporation

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Entropy Source	Physical	TC58NC1137GTC-0003	1 bit	0.667	N/A

Table 8: Entropy Sources

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 8 this input contains about 683 bits of entropy, which is sufficient entropy to obtain 256 bits of security strength.

2.9 Key Generation

Please refer to Section 9.4.

2.10 Key Establishment

N/A for this module.

2.11 Industry Protocols

N/A for this module.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Mailbox	Data Input	Mailbox input parameter
Mailbox	Data Output	Mailbox output parameter
Mailbox	Control Input	Mailbox command information
Mailbox	Status Output	Mailbox command result
AES circuit	Data Input	User data
AES circuit	Data Output	User data
DMAC	Data Input	Mailbox input parameter
DMAC	Data Output	Mailbox output parameter
Lock Checker	Data Input	Read/Write destination address information
Lock Checker	Control Input	Lock status confirmation request signal
Lock Checker	Status Output	Lock status confirmation result signal
Power PIN	Power	Power

Table 9: Ports and Interfaces

Control output is omitted in the table above because the CM does not implement this type of interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
PIN	Verifying the PIN entered by the user matches the information stored inside the CM (Memorized secrets) .	SHA2-256 (A7087)	Probability of 1/2^64	Probability of 60,000/2^64

Table 10: Authentication Methods

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. Therefore, the probability that random attempts in 1min will succeed is 60,000 / 2^64 < 1 / 100,000.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
AdminSP.SID	Role	CO	PIN

Name	Type	Operator Type	Authentication Methods
AdminSP.Admin1	Role	CO	PIN
LockingSP.Admin1-4	Role	CO	PIN
LockingSP.UserX (X=1, ...192)	Role	CO	PIN

Table 11: Roles

The CM only supports Crypto Officer Role.

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 11 (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.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Band Lock/Unlock	Lock or unlock read / write of user data in a band.	Mailbox command and result	Mailbox command / input parameter	Mailbox Command Result	MEKs Generation HMAC Generation/Verification	LockingSP.Admin1-4 - KDK: E - MEKs: G,Z - System MAC Key: E
Band Lock/Unlock for Band of Single User Mode	Lock or unlock read / write of user data in band "X" of single user mode	Mailbox command and result	Mailbox command / input parameter	Mailbox Command Result	MEKs Generation HMAC Generation/Verification	LockingSP.UserX (X=1, ...192) - KDK: E - MEKs: G,Z - System MAC Key: E
Check Lock State	Check a lock state of band that read / write user data.	N/A	Lock status confirmation request signal	Lock status confirmation result signal	None	Unauthenticated
Data Read/Write	Encryption / Decryption of user	Readable / Writable	LBA, User Data of ciphertex	LBA, User Data of plaintext	User Data Encryption/Decryption	LockingSP.Admin1-4 - MEKs: E LockingSP.Us

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	data to / from unlocked band of SSD.	signal from Lock Checker	t / plaintext (read / write)	/ ciphertext (read / write)		erX (X=1, ...192) - MEKs: E
Cryptographic Erase	Erase user data (in cryptographic means) by changing the key that derives the data encryption key.	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	KDK Generation MEKs Generation KTS	LockingSP.Admin1-4 - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E
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.	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	KDK Generation MEKs Generation KTS	LockingSP.UserX (X=1, ...192) - KDK: G,R,W,E,Z - System MAC Key: E - System Enc Key: E - MEKs: G,Z
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	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	KDK Generation MEKs Generation HMAC Generation/Verification KTS	LockingSP.Admin1-4 - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E LockingSP.UserX (X=1, ...192) - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	the band state					Key: E - System Enc Key: E
Download Port Lock/Unlock	Lock / unlock firmware download	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	None	AdminSP.SID
Firmware Verification 1	Digital signature verification for the entire firmware of SSD equipped with this CM using LMS	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	FW digital signature verification 1	Unauthenticated
Firmware Verification 2	Digital signature verification for the entire firmware of SSD equipped with this CM using RSA	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	FW digital signature verification 2	Unauthenticated
Firmware Download	Download a firmware image	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	FW digital signature verification 2	AdminSP.SID - PubKey1: W,E,Z
Random Number Generation	Provide a random number generated by the CM.	Mailbox command result	Mailbox command	Mailbox Command Result	Random Number Generation	Unauthenticated - DRBG Internal Value: E
Set Band Position and Size	Set the location and size of the band	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	KDK Generation MEKs Generation HMAC Generation/Verification KTS	LockingSP.Admin1-4 - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- System Enc Key: E
Set Band Position and Size for Band of Single User Mode	Set the location and size of the band "X" of single user mode	Mailbox command and result	Mailbox command / input parameter	Mailbox Command Result	KDK Generation MEKs Generation HMAC Generation/Verification KTS	LockingSP.Admin1-4 - MEKs: G,Z - KDK: G,R,W,E,Z - System MAC Key: E - System Enc Key: E LockingSP.UserX (X=1, ...192) - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E
Set PIN for Band of Single User Mode	Set PIN (authentication data) of authority for band X of single user mode	Mailbox command and result	Mailbox command / input parameter	Mailbox Command Result	KTS Hash calculation	LockingSP.UserX (X=1, ...192) - PINs: R,W,E - System MAC Key: E - System Enc Key: E
Set PIN	Set PIN (authentication data)	Mailbox command and result	Mailbox command / input parameter	Mailbox Command Result	KTS Hash calculation	AdminSP.SID - PINs: R,W,E - System MAC Key: E - System Enc Key: E AdminSP.Admin1 - PINs: R,W,E - System MAC Key: E - System Enc Key: E LockingSP.Admin1-4 - PINs: R,W,E - System MAC Key: E - System Enc

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: E LockingSP.UserX (X=1, ...192) - PINs: R,W,E - System MAC Key: E - System Enc Key: E
Authority Enable/Disable	Enable/Disable the authority.	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	KTS	AdminSP.SID - System MAC Key: E - System Enc Key: E LockingSP.Admin1-4 - System MAC Key: E - System Enc Key: E
Revert	Initialize the band State and disable band lock setting.	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	KDK Generation MEKs Generation HMAC Generation/Verification KTS Hash calculation	AdminSP.SID - PINs: R,W,E - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E AdminSP.Admin1 - PINs: R,W,E - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E LockingSP.Admin1-4 - PINs: R,W,E - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Data Locking Protection Enable	Enable Data protection with band lock setting.	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	KTS Hash calculation	AdminSP.SID - PINs: R,W,E - System MAC Key: E - System Enc Key: E LockingSP.Admin1-4 - PINs: R,W,E - System MAC Key: E - System Enc Key: E
Sanitize	Erase all user data (in cryptographic means) by changing the key that derives the data encryption key.	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	KDK Generation MEKs Generation KTS	AdminSP.SID - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E AdminSP.Admin1 - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E LockingSP.Admin1-4 - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E
Format Namespace	Erase user data (in cryptographic means) on Namespace by changing the key that	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	KDK Generation MEKs Generation KTS	AdminSP.SID - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E AdminSP.Admin1

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	derives the data encryption key.					- KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E LockingSP.Admin1-4 - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E LockingSP.UserX (X=1, ...192) - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E
Namespace Create/Delete	Create and delete Namespace.	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	KDK Generation MEKs Generation KTS	AdminSP.SID - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E AdminSP.Admin1 - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E LockingSP.Admin1-4 - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: E - System Enc Key: E LockingSP.UserX (X=1, ...192) - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E
Band Set Enable	Set the location, size and lock state of the band.	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	KDK Generation MEKs Generation HMAC Generation/Verification KTS	LockingSP.Admin1-4 - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E
Band Set Disable	Initialize the location, size and lock state of the band.	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	KDK Generation MEKs Generation HMAC Generation/Verification KTS	LockingSP.Admin1-4 - KDK: G,R,W,E,Z - MEKs: G,Z - System MAC Key: E - System Enc Key: E
Signature Generation	Generate a signature of the data by using a private key entered from outside of the CM.	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	Signature Generation	Unauthenticated - Key Pair Private Key: W,E,Z
Signature Verification	Verify input signature by using a public key entered from outside of the CM.	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	Signature Verification	Unauthenticated - Key Pair Public Key: W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Calculate Hash Digest	Hash the data entered from outside of the CM	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	Hash calculation	Unauthenticated
Show Status (Show Version)	Report status of the CM and versioning information.	Mailbox command result	Mailbox command	Mailbox Command Result	None	Unauthenticated
Zeroization	Zeroize SSPs.	Mailbox command result	Mailbox command / input parameter	Mailbox Command Result	None	Unauthenticated - RKey: Z - KDK: Z - MEKs: Z - PINs: Z - System MAC Key: Z - System Enc Key: Z - DRBG Internal Value: Z
Reset (Power-OFF)	Delete SSPs in SRAM.	N/A	N/A	N/A	None	Unauthenticated - KDK: Z - MEKs: Z - PINs: Z - System MAC Key: Z - System Enc Key: Z - DRBG Internal Value: Z
Reset (Power-ON) (Self Test)	Runs various self-tests to be performed at power-on (POSTs, CASTs, Firmware	N/A	N/A	N/A	MEKs Generation KTS FW digital signature verification 2 Hash calculation Entropy Generation	Unauthenticated - RKey: E - KDK: W - PINs: W - System MAC Key: G,E - System Enc Key: G,E - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Load test) and generate / import some SSPs.					Internal Value: G - DRBG Seed: G,E,Z - PubKey1: W,E,Z

Table 12: Approved Services

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

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The CM performs signature verification on Firmware loaded from external memory using RSASSA-PKCS#1-v1_5 (SHA2-384, 3072-bit key). The Firmware is verified at separated memory from the current firmware, and it is loading if the firmware verification is successful.

5 Software/Firmware Security

5.1 Integrity Techniques

Firmware Security of components in this CM is shown below.

MaskROM Code:

- Form of the executable code: Binary
- Integrity verification method: 32bit CRC

Firmware image (User Code):

- Form of the executable code: Binary
- Integrity verification method: Approved signature verification (RSASSA-PKCS#1-v1_5)

5.2 Initiate on Demand

MaskROM Code, Firmware image (User Code)

- Initiate on demand integrity verification: Power cycling

5.3 Open-Source Parameters

N/A for this module.

5.4 Additional Information

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

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. Any firmware/software loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a success of firmware load test and a separate FIPS 140-3 validation

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Passivated opaque package	N/A	N/A

Table 13: Mechanisms and Actions Required

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 forcibly opening the package. Consequently, tampering with the module's components is impossible without leaving evidence of tampering.
The CM is used by being in the SSD, and the SSD's enclosure surrounds it.

Front Back

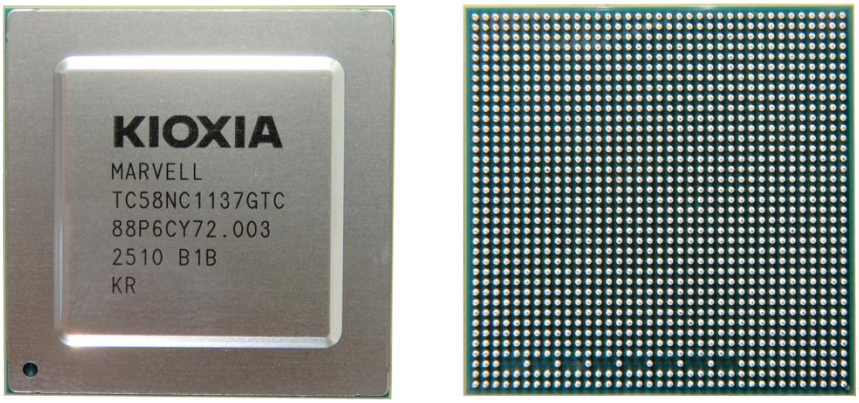

Figure 2: TC58NC1137GTC 0003 SoC

8 Non-Invasive Security

The CM does not apply Non-invasive security.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
S1	OTP: One Time Programmable area	Static
S2	SRAM: Storage area to store FW components and SSPs as volatile information	Dynamic
S3	AES Circuit HW Register: Write Only Storage area to store MEKs of unlock band	Dynamic
S4	DRAM: Outside the cryptographic module	Dynamic

Table 14: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
IE1	S2	S4	Encrypted	Automated	Electronic	KTS
IE2	S4	S2	Encrypted	Automated	Electronic	KTS
IE3	S4	S2	Plaintext	Manual	Electronic	

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Overwriting S1 with All 1	S1 is overwritten, All 1 key is not allowed.	Zeroization
Z2-1	Overwriting S2 with All 0	S2 is overwritten, All 0 key is not allowed.	Zeroization, Services that allow setting the range length to zero*
Z2-2	Overwriting S3 with All 0	S3 is overwritten, All 0 key is not allowed.	Zeroization, Services that allow setting the range length to zero; Services that allow locking the corresponding band**
Z3-1	Overwriting S2 with random value	S2 is overwritten with newly generated random value.	Services that update key***
Z3-2	Overwriting S3 with random value	S3 is overwritten with newly generated random value.	Services that update key
Z4	Overwriting immediately after use	The CM overwrites SSP with All 0 immediately	N/A
Z5	Clear the data in volatile memory	S2 and S3, S4 are cleared when Power-off	Reset(Power-OFF) service

Table 16: SSP Zeroization Methods

* Services that allow setting the range length to zero: Set Band position and Size, Set Band Position and Size for Band of Single User Mode, Namespace Create/Delete, Band Set Enable and Band Set Disable.
** Services that allow locking the corresponding band: Band Lock/Unlock, Cryptographic Erase and initialize Band State, Revert, and Band Set Enable.
*** Services that update key: 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, Revert, Sanitize and Format Namespace.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
RKey	Derivation of System Enc Key and System MAC Key	256 - 256	Symmetric - CSP	Hash DRBG (A7173)		KDF SP800-108 (A7174)
System Enc Key	Data Encryption / Decryption for KTS	256 - 256	Symmetric key encryption and decryption key - CSP	KDF SP800-108 (A7174)		KTS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
System MAC Key	Message Authentication Code generation and verification for KTS	256 - 256	MAC algorithm key for symmetric authentication - CSP	KDF SP800-108 (A7174)		HMAC Generation/Verification KTS
KDK	Derivation of MEKs	256 - 256	Symmetric - CSP	KDK Generation	KTS	MEKs Generation
MEKs	Data encryption/decryption	512 - 256	Symmetric - CSP	MEKs Generation		User Data Encryption/Decryption
PINs	User authentication PIN	256 - 128	PIN - CSP			KTS Hash calculation
Key Pair Private Key	Imported Private Key for ECDSA	384 - 192	Private - CSP			Signature Generation
DRBG Internal Value	DRBG state(V: 440 bits, C: 440 bits)	880 - 256	DRBG Internal State - CSP			Random Number Generation
DRBG Seed	DRBG seed	1024 - 256	Seed - CSP	Entropy Generation		Hash DRBG (A7173)
PubKey1	Signature verification key for RSA	3072 - 128	Public - PSP			FW digital signature verification 2
Key Pair Public Key	Imported Public key for ECDSA	384 - 192	Public - PSP			Signature Verification

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
RKey		S1:Plaintext	Until zeroization	Z1	System Enc Key:Derives System MAC Key:Derives
System Enc Key		S2:Plaintext	Until Power-Off	Z2-1 Z5	RKey:Derived From KDK:Wraps PINs:Wraps
System MAC Key		S2:Plaintext	Until Power-Off	Z2-1 Z5	RKey:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					KDK:Wraps PINs:Wraps
KDK	IE1 IE2	S2:Plaintext	While the band exist, Until Power-Off	Z2-1 Z2-2 Z3-1 Z5	System Enc Key:wrapped by System MAC Key:wrapped by MEKs:Derives
MEKs		S3:Plaintext	While the band is unlocked, Until Power-Off	Z2-2 Z3-2 Z5	KDK:Derived From
PINs	IE1 IE2 IE3	S2:Obfuscated	Until Power-Off	Z2-1 Z4 Z5	System Enc Key:wrapped by System MAC Key:wrapped by
Key Pair Private Key	IE3	S2:Plaintext	While in use	Z4	
DRBG Internal Value		S2:Plaintext	Until Power-Off	Z2-1 Z5	
DRBG Seed		S2:Plaintext	While in use	Z4	
PubKey1	IE3	S2:Plaintext S1:Obfuscated	While in use	Z4	
Key Pair Public Key	IE3	S2:Plaintext	While in use	Z4	

Table 18: SSP Table 2

PINs are stored in S2, and PubKey1 is stored in S1 as hashed value. “Obfuscated” in “Storage” column of these SSPs means hashed value.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware integrity test	integrity	32 bit CRC	SW/FW Integrity	Implicit error reporting by stopping the startup sequence	Verify MaskROM code integrity with 32bit CRC

Table 19: Pre-Operational Self-Tests

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.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A7087) - Encrypt	Key Size: 256 bits	KAT	CAST	0x01 or 0x24	Encrypt	Power-on
AES-CBC (A7087) - Decrypt	Key Size: 256 bits	KAT	CAST	0x01 or 0x24	Decrypt	Power-on
AES-XTS Testing Revision 2.0 (A7087) - Encrypt	Key Size: 256 bits	KAT	CAST	0x01 or 0x23	Encrypt	Power-on
AES-XTS Testing Revision 2.0 (A7087) - Decrypt	Key Size: 256 bits	KAT	CAST	0x01 or 0x23	Decrypt	Power-on
SHA2-256 (A7087)	Digest Size : 256 bits	KAT	CAST	0x01 or 0x25	Digest	Power-on
Hash DRBG (A7173)	Hash based: SHA2-256	KAT	CAST	0x01 or 0x18/0x19	DRBG	Power-on
SHA2-384 (A7087)	Digest Size: 384 bits	KAT	CAST	0x01 or 0x25	Digest	Power-on
HMAC-SHA2-256 (A7087)	Key Size: 256 bits	KAT	CAST	0x01 or 0x26	Digest	Power on
RSA SigVer (FIPS186-5) (A7087)	Key Size: 2048 and 3072 bits	KAT	CAST	0x01 or 0x27	Signature Verification	Power-on
ECDSA SigVer (FIPS186-5) (A7223)	Curve: P-384	KAT	CAST	0x01 or 0x36	Signature Verification	Before first use
ECDSA SigGen (FIPS186-5) (A7223)	Curve: P-384	KAT	CAST	0x01 or 0x36	Signature Generation	Before first use
KDF SP800-108 (A7174)	HMAC-SHA2-256	KAT	CAST	0x01 or 0x28	KDF	Power-on
Entropy Source (Health tests of noise source at startup)	Cut off RCT: 61, APT: 752	RCT, APT	CAST	0x01 or 0x2C/2D	Entropy Generation	Power-on
Entropy Source (Continuous noise source	Cut off RCT: 61, APT: 752	RCT, APT	CAST	0x01 or 0x2C/2D	Entropy Generation	Entropy output request

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
health tests during operation)						
LMS SigVer (A7297)	Key Size: 448 bits	KAT	CAST	0x01 or 0x37	Signature Verification	Power-on
Firmware load test at Power on	hash type: SHA2-384; key length: 3072 bit.	sigVer	SW/FW Load	0x01 or 0x13/0x38	Verify signature of loaded firmware image	Power-on
Firmware load test at FW download	hash type: SHA2-384; key length: 3072 bit	sigVer	SW/FW Load	0x01 or 0x13/0x38	Verify signature of downloaded firmware image	FW download

Table 20: Conditional Self-Tests

If the Conditional Self-Tests are successful, the CM will return 0x01 as an indicator; if they fail, it will return Error Code in Table20.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware integrity test	32 bit CRC	SW/FW Integrity	On Demand	Power cycling

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A7087) - Encrypt	KAT	CAST	On Demand	Power cycling
AES-CBC (A7087) - Decrypt	KAT	CAST	On Demand	Power cycling
AES-XTS Testing Revision 2.0 (A7087) - Encrypt	KAT	CAST	On Demand	Power cycling
AES-XTS Testing Revision 2.0 (A7087) - Decrypt	KAT	CAST	On Demand	Power cycling
SHA2-256 (A7087)	KAT	CAST	On Demand	Power cycling
Hash DRBG (A7173)	KAT	CAST	On Demand	Power cycling

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-384 (A7087)	KAT	CAST	On Demand	Power cycling
HMAC-SHA2-256 (A7087)	KAT	CAST	On Demand	Power cycling
RSA SigVer (FIPS186-5) (A7087)	KAT	CAST	On Demand	Power cycling
ECDSA SigVer (FIPS186-5) (A7223)	KAT	CAST	On Demand	First provided service after power cycling
ECDSA SigGen (FIPS186-5) (A7223)	KAT	CAST	On Demand	First provided service after power cycling
KDF SP800-108 (A7174)	KAT	CAST	On Demand	Power cycling
Entropy Source (Health tests of noise source at startup)	RCT, APT	CAST	On Demand	Power cycling
Entropy Source (Continuous noise source health tests during operation)	RCT, APT	CAST	On Demand	Provided service with generating entropy
LMS SigVer (A7297)	KAT	CAST	On Demand	Power cycling
Firmware load test at Power on	sigVer	SW/FW Load	On Demand	Power cycling
Firmware load test at FW download	sigVer	SW/FW Load	On Demand	Provided service

Table 22: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Boot Error State	The CM has failed Pre-operational self-test, cryptographic algorithm test excluded ECDSA, and health tests of noise source at startup	Pre-operational self-test, cryptographic algorithm test excluded ECDSA, and health tests of noise source at startup Failure	Power-off	Indicated Error Code: 0x23 0x24, 0x25, 0x26, 0x18, 0x19, 0x27, 0x28, 0x2C, 0x2D, 0x37 and/or no response

Name	Description	Conditions	Recovery Method	Indicator
Error State (Conditional Test)	The CM has failed ECDSA algorithm test and continuous noise source health tests	ECDSA algorithm test and continuous noise source health tests Failure	Power-off	Indicated Error Code: 0x2C, 0x 2D, 0x36
Power Up Load Test Error State	The CM has failed FW Load at power up	FW Load at power up Failure	Power-off	Indicated Error Code: 0x13 , 0x38
Conditional Load Test Error State	The CM has failed FW update	FW update Failure	N/A	Indicated Error Code: 0x13, 0x38

Table 23: Error States

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 (i.e. Recovery Method). 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. When the CM is in an error state except for Conditional Load Test Error State, cryptographic functions cannot be executed by the CM. If the CM enters Conditional Load Test Error State, it reports Error code and transitions from error state to normal state, and continues to operate with FW before download.

10.5 Operator Initiation of Self-Tests

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).

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

In the SSD's manufacturing process, installation is executed as below:

1. The Firmware described in Section 2.2 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:

- Load Firmware into the CM.
- Load system area including SSPs into the CM.
- Execute range state setting method (Set the location and size of all range).
- Execute download port setting method (Lock / unlock firmware download).
- Execute namespace setting method (Create Namespace).
- Execute service execution state setting method (Enable CM settings (location and size of all range, lock/unlock firmware download, namespace status)).

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. Operators can confirm that the CM is in approved mode by executing Show Status (Show Version) 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.

11.2 Administrator Guidance

After the procedure written in section 11.1, the CM can be used as an approved mode. Users can confirm that the CM is in approved mode by executing Show Status (Show Version) service and checking that the startup is successfully completed. 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.

11.3 Non-Administrator Guidance

The module implements only the Crypto Officer. There is no guidance for non-administrators.

11.4 Design and Rules

N/A for this module.

11.5 Maintenance Requirements

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.

11.6 End of Life

The user needs to erase CPSs by executing Revert service for secure sanitization.

12 Mitigation of Other Attacks

The CM does not mitigate other attacks beyond the scope of FIPS 140-3 requirements.