Micron Technology

Micron 7400 SSD Controller Sub Chip Security Subsystem

Non-Proprietary FIPS 140-3 Security Policy

Document Version: 1.3

Date: April 11th, 2024

Table of Contents

List of Tables

List of Figures

1 General

This document defines the non-proprietary Security Policy for the Micron Technology, Inc. Micron 7400 SSD Controller Security Subsystem module, hereafter denoted as the Module. The Module is a Single Chip Hardware sub-chip cryptographic subsystem, as defined in FIPS 140-3 Implementation Guidance 2.3.B.

The FIPS 140-3 security levels for the Module are as follows:

Table 1 – Security Levels

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 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

2 Cryptographic Module Specification

The Module is a Single Chip Hardware Sub-Chip cryptographic module operating on a single chip embodiment.

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated cryptographic controllers. The Module is embedded in the ASIC 7400 Controller package (see Figure 1 below).

Figure 1 – Micron 7400 ASIC

2.1 Operational Environment

The cryptographic module is tested on the following operational environment.

Table 2 – Cryptographic Module Tested Configuration

Model	Hardware [Part Number and version]	Firmware version	Distinguishing Features
Micron 7400 SSD Controller Security Subsystem	SCCS v1.0	Runtime SCSS v2.3 Bootloader v1.0 Function ROM v2.0 Boot ROM v1.0	Tested Configuration: 7400 SSD Controller v20190703

Module operational environment information is provided from the Module from the get status service and is returned from the controller as TCG Level 0 discovery content.

2.2 Cryptographic Boundary

The physical form of the Module is depicted above in Figure 1. The cryptographic boundary of the Module is defined by the Security Subsystem and includes all cryptographic algorithm implementations. The physical embodiment is the Micron 7400 Controller ASIC and includes its package. The cryptographic boundary is depicted by the red outline line in Figure 2 below. The Module is a Single Chip Hardware Sub-Chip cryptographic module operating on a single chip embodiment. Table 2 above specifies the firmware components of the module.

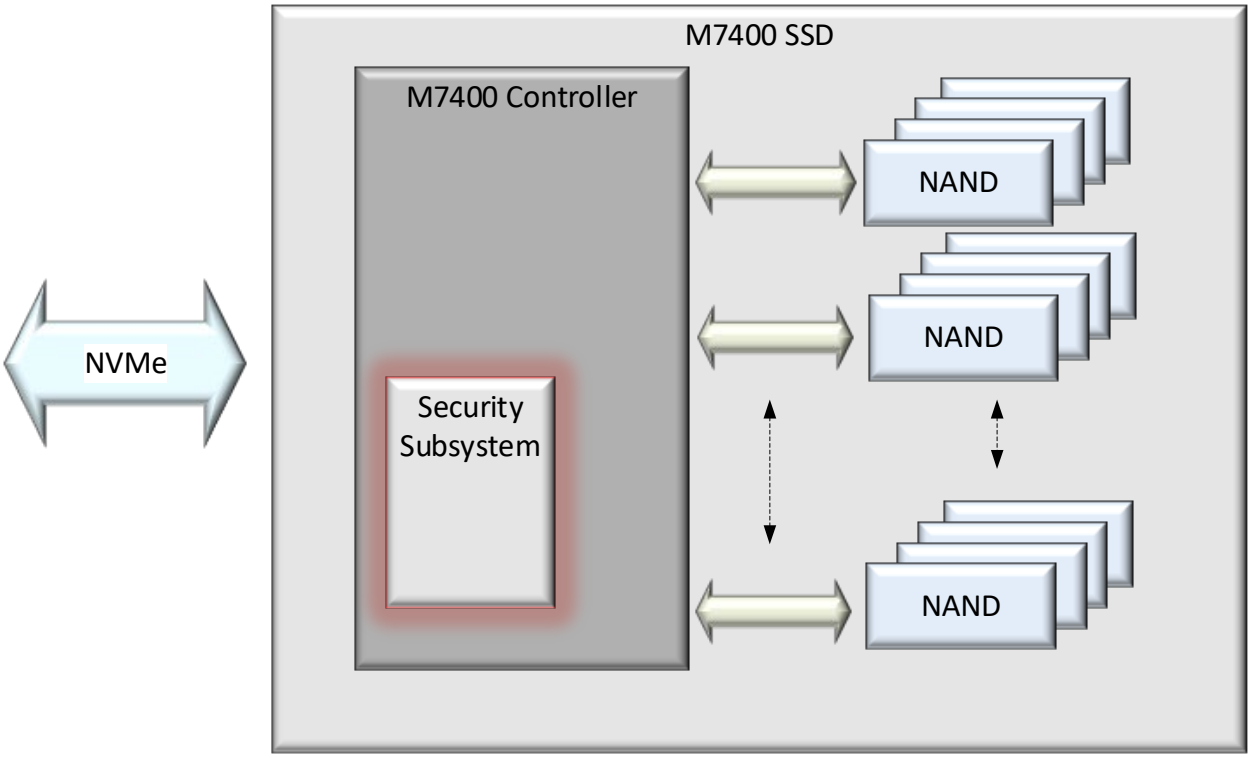

Figure 2 – Module

2.3 Modes of Operation

The Module only supports an Approved mode and cannot be configured to operate otherwise. To verify that the Module is in the Approved mode of operation, the operator may invoke the "Get Status" service, which will indicate the Approved mode of operation, as well as the version information for the Module.

The following states are defined for the module.

- Firmware Load State – In this state, the Module is capable of performing self-tests, key manifest verification, and firmware loading.
- NVMe State – In this operating state, TCG ownership of the drive has not been taken. In this state the SSD provides services through NVME industry standard commands.
- TCG State – Once TCG ownership has been taken the Module shall operate in this state. In this state the SSD provides services through NVME industry standard commands as well as TCG commands addressed to both the TCG Admin SP and the TCG locking SP. In addition, extra features are provided through the TCG commands. These commands are processed within the controller and are translated into security subsystem services. The Module provides these services to support the TCG mode of operation but is not responsible for TCG management functions. To initialize in this mode, the Module owner must take ownership of the device by invoking the Activate method on the Locking SP. This State has the capability to have multiple Users with independent access control to read, write or erase the data areas (LBA ranges).

Note: By default, the drive is issued with a single namespace encompassing the whole capacity of the drive. Once the drive is TCG activated this default namespace's attributes are managed by the TCG "Global Range".

2.4 Security Functions

The Module implements the cryptographic functions listed in table 3 below. The numbers and letters within square brackets reference standards which are defined in the References and Definitions section of this Security Policy.

Table 3 – Approved Algorithms

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2520	AES [197]	AES-KW [38F]	Key Sizes: 256	Authenticated Encrypt, Authenticated Decrypt (Uses Auxiliary ECB)
A2522	AES [197]	AES-ECB [38A]	Key Sizes: 256	Encrypt, Decrypt (Auxiliary)
		AES-XTS[1] Testing Revision 2.0 [38E]	Key Sizes: 256	Encrypt, Decrypt (Auxiliary)
A2523	AES [197]	AES-ECB [38A]	Key Sizes: 256	Encrypt, Decrypt (Datapath)
		AES-XTS[1] Testing Revision 2.0 [38E]	Key Sizes: 256	Encrypt, Decrypt (Datapath)
VA	CKG [IG D.H]	[133] Sections 4 and 6.1 Direct symmetric key generation using unmodified DRBG output		Key Generation
		[133] Section 6.2.2 Symmetric Keys Derived from a Pre-existing Key		
		[133] Section 6.2.3 Derivation of symmetric keys from a password		
		[133] Section 6.3 Symmetric Keys Produced by Combining Multiple Keys and Other Data		
A2520	HASH DRBG [90A]	HASH DRBG	SHA2-256	Deterministic Random Bit Generation Security Strength = 256
A2521	HMAC-SHA2-256 [198]	SHA2-256	Key Size: 256 MAC = 256	Key derivation. Data Authentication
A2521	KDF [108]	Counter Mode KDF SP800-108	HMAC-SHA2-256 Supported Lengths: 256 Fixed Data Order: Before Fixed Data	Key Based Key Derivation

[1] The XTS algorithm implementation includes a check to ensure Key_1 ≠ Key_2. XTS may only be used in storage applications.

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
			Counter Length: 8 Custom Key in Length: 0	
A2520	KTS [38F]	AES-KW	Key Sizes: 256	CSP Wrapping/Unwrapping
A2520	KTS-IFC [56Br2]	KTS-OAEP-basic	n = 2048^2 SHA2-256 n = 3072^2 SHA2-256	Key transport methodology provides between 112 and 128 bits of encryption strength; Encapsulation Only.
A2520	PBKDF [132]	Option 1a	sLen = 256 C = 300 HMAC-SHA2-256	Password Based Key Derivation. Keys derived from passwords may only be used in storage applications. Password length is 32 bytes and only five attempts are permitted before a reset is required. The PBKDF iteration count (C) is chosen to be as high as can be tolerated without impacting system boot up performance.
A2521	RSA SigVer [186]	PKCS1_v1.5	n = 2048 SHA2-256 n = 3072 SHA2-256 Public Exponent Mode: Fixed Fixed Public Exponent: 010001	Signature verification
A2522	SHA2-256 [180]	SHA2-256	-	Message Digest Generation

The module does not implement any “Non-Approved Algorithms Allowed in the Approved Mode of Operation” or “Non-Approved Algorithms Not Allowed in the Approved Mode of Operation” per SP800-140B. Only “Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed” are supported per Table 4 below.

Table 4 – Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm	Caveat	Use / Function
RBG	No security claimed per IG 2.4.A.	Generates a 64-byte personalization string for the DRBG. Per [90A], the personalization is entirely optional, is not required to contain any entropy, and may be provided by a non-Approved RBG.

2.5 Security Function Implementation

The following table shows the Security Function Implementations that the module implements:

Table 5 - Security Function Implementation

Name	Type	Description	SF Properties	Algorithms/CAVP Cert
KTS	KTS	AES-KW – AES Cert. #A2520	Key establishment methodology provides 256 bits of encryption strength	AES-KW/Cert. #A2520
KTS-IFC	KTS	KTS-IFC - RSA Cert. #A2520	Key transport methodology provides between 112 and 128 bits of encryption strength	KTS-IFC/Cert. #A2520

2.6 Overall Security Design

1. The Module provides one distinct operator role: Controller, which acts as the Cryptographic Officer
2. The Module provides role-based authentication.
3. The Module clears previous authentications on reset.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module.
6. Power up self-tests do not require any operator action.
7. Data outputs are inhibited during firmware loading, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. There are no restrictions on which keys or SSPs are zeroized by the zeroization service, except for the $K_{ManifestPUB\_ROM}$.
10. The Module does not support concurrent operators.
11. The Module does not support a maintenance interface or role.
12. The Module does not support manual SSP establishment method.
13. The Module does not have any proprietary external input/output devices used for entry/output of data.
14. The Module does not output plaintext CSPs or intermediate key values.

15. The Module does not provide bypass services.
16. The Module zeroizes temporary values generated and used during self-tests.

2.7 Rules of Operation

The Module is embedded within the Micron 7400 controller of the SSD. The Module shall be operated according to Section 11.

3 Cryptographic Module Interfaces

The Module's ports and associated FIPS defined logical interface categories are listed in Table 5 above.

Table 6 – Ports and Interfaces

Physical Port	Logical Interface	Data that passes over port/interface
AESE (encryption engine)	Control in | Data in | Data out | Status out	User data
AESD (decryption engine)	Control in | Data in | Data out | Status out	User data
Mbox (Mailbox)	Control in | Status out	Service info input
Controller output (response to Mbox)	Data out	Service info output
External Interrupt (JTAG, AHB bypass and inter-CPU interrupts)	Disabled	Disabled
Reset/Interrupt	Control in	None
BMG-128 (S-DMA Interface)	Data in | Data out	Service info data (command/response)
Power	Power in	None
JTAG / AHB-32 bypass	Disabled	Disabled
LDPC Decoder	Data In	Firmware Images
UART	Status out	Status Data

4 Roles, Services and Authentication

4.1 Assumption of Roles and Related Services

The Module supports one distinct operator role, Controller (Cryptographic Officer).

Table 6 lists the operator role supported by the Module and their related services. In addition to the services listed in Table 6, the Module also supports a Self-Test service, which is invoked by power cycling the Module.

The Module does not support a maintenance role or bypass capability. The Module does not support concurrent operators.

Table 7 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
Any	Self-Test	N/A	N/A
Controller	SUP Authenticate	Password	Response
Controller	SUP Generate	None	Encrypted blob
Controller	TCG Authenticate	Wrapped RdsKey or SumRdsKey, Password	Response
Controller	Clear TCG Authentications	None	Response
Controller	Random	Size/Location	Random Value
Controller	NVMe Allocate and associate Key	Namespace Information	Response
Controller	NVMe Deallocate and disassociate Key	Namespace information	Response
Controller	NVMe Update Key	Namespace information	Response
Controller	Public HMAC Generation	Target input	HMAC
Controller	Load Range and Key	Range and key (index) Information	Response
Controller	AWOR	None	Encrypted block
Controller	TCG Allocate and associate Key	Range Information	Response
Controller	TCG Deallocate and disassociate Key	Range Information	Response
Controller	TCG Update Key	Range Information	Response
Controller	TCG Set PIN	Password	Response
Controller	TCG Revert, Activate, Reactivate	Command information	Response
Controller	TCG HMAC Generation	Target HMAC	HMAC
Controller	Manifest Load	Manifest	Verification status
Controller	CSP Load	CSP Block	Verification status
Controller	Write/Read	Read/Write Location	Read information Status
Controller	Get Status	None	Status
Controller	Firmware Signature Check	Firmware block	Verification status

Role	Service	Input	Output
Controller	Factory Auth	Signature	Verification status
Controller*	Device Deprovision	Deprovision ID	Status
Controller*	Generate KeyDerivationKey	Mode	Status
Controller*	Zeroize	None	Status

*Requires additional authorization

4.2 Authentication Methods

The role-based authentication methods are defined in Table 8 below.

Table 8 – Roles and Authentication

Role	Authentication Method	Authentication Strength
Controller	Signature Verification	RSA 2048/3072 has a key strength of 112/128 bits. The probability of a successful verification from a single random attempt is at least $1/2^{112}$ which is < 1/1,000,000. This effectively eliminates the possibility of determining the private key through exhaustive methods. Using a conservative estimate of 1ms per verification attempt, the maximum number of attempts which can be made in 1 minute is 60,000. This results in a probability of at least $60,000/2^{112}$ that multiple attempts in a given minute of time is successful, which is less than 1/100,000.

4.3 Services

All services implemented by the Module are listed in the Table 9 below. The services provided by the Module are defined in terms of the services being exposed at the Module (logical) boundary. Each service description also describes the operator roles involved along with the interface command associated with the service.

The SSPs modes of access shown in Table 9 are defined as:

- **G** = Generate: The Module generates or derives the SSP.
- **R** = Read: The SSP is read from the Module (e.g., the SSP is output).
- **W** = Write: The SSP is updated, imported, or written to the Module.
- **E** = Execute: The Module uses the SSP in performing a cryptographic operation. Implicitly include Read.
- **Z** = Zeroize: The Module zeroizes the SSP.

The service indicator for approved services is the return code from an approved security service call (CCS).

CCS = Command completion status, complies with the Approved Security Service Indicator defined in IG 2.4.C, Example Scenario #2.

Table 9 – Approved Services

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Self-Test	Run KAT tests on all cryptographic algorithms.	All	NA	Any This service is unauthenticated.	N/A	CCS
SUP Authenticate	Unwrap SUP blob using PBKDF derived key.	PBKDF, AES-KW	Password; PasswordWrapKey	Controller	W, E G, E	CCS
SUP Generate	KTS-IFC wrap an internally generated random.	DRBG, CKG KTS-IFC, AES-KW, PBKDF	DrbgState; $K_{DeviceWrappingPub;}$ PasswordWrapKey; SUP Seed	Controller	W, E; E; G, E, Z; G, E, Z	CCS
TCG Authenticate	Unwrap TCG SSP using PBKDF derived key.	PBKDF, AES-KW, CKG	Password; SumRDSKey; RdsKey; PasswordWrapKey; AuthenticatedUseHmacKey; EphemeralSumRdskWrapKey	Controller	E; W; W; G, E, Z; E; E	CCS
Clear TCG Authentications	Remove status of all past authentication and their privileges	NA	NA	Controller	N/A	CCS
Random	Returns a 256-bit random number	DRBG	DrbgState	Controller	E, W	CCS
NVMe Allocate and associate Key	Generate a key, wrap key and associate key with an entity.	DRBG, AES-KW, CKG	DrbgState; WrapKey; RdsKey; SumRdsKey; NamespaceDEK; AuthenticatedUseHmacKey; EphemeralSumRdskWrapKey	Controller	E, W; E; G, E, R; G, E, R; G, R; E; E	CCS
NVMe Deallocate and disassociate Key	Zeroize key and disassociate key from an entity.	AES-KW	NamespaceDEK; WrapKey; AuthenticatedUseHmacKey	Controller	Z; E; E	CCS
NVMe Update Key	Erase user data in a namespace by changing the encryption key	DRBG, AES-KW, CKG	DrbgState; WrapKey; RdsKey; SumRdsKey NamespaceDEK; LockingObjectDEK; AuthenticatedUseHmacKey; EphemeralSumRdskWrapKey	Controller	E; E; E; W, E; Z, G, R; Z, G, R; E; E	CCS
Public HMAC Generation	Generate an HMAC over the prescribed content.	HMAC SHA2-256	RootPublicMacKey; PspHmacKey	Controller	E; E	CCS

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Load Range and Key	Load DEK into DPE for indicated range	AES-KW	TweakKey; LockingObjectDEK; NamespaceDEK; RdsKey; SumRdsKey; WrapKey; EphemeralSumRdskWrapKey	Controller	W; W; W; E; W, E; E; E;	CCS
AWOR	Save, restore security operational context.	KDF, AES-KW, HMAC, CKG	AworWrapKey; AworHmacKey; DrbgState; WrapKey; AuthenticatedUseHmacKey; PspHmacKey; TweakKey; RdsKey; SumRdsKey; RootHmacKey; RootKeyWrapKey; RootPublicMacKey; EphemeralSumRdskWrapKey	Controller	E; E; W, R; W, R; W, R; W, R; W, R; W, R; W, R; W, R; W, R; W, R; W, R	CCS
TCG Allocate and associate Key	Generate a key, wrap key and associate key with an entity.	DRBG, AES-KW, CKG	DrbgState; WrapKey; RdsKey; SumRdsKey; LockingObjectDEK; EphemeralSumRdskWrapKey; AuthenticatedUseHmacKey	Controller	E; E; G, E, R; G, E, R; G, R; E; E	CCS
TCG Deallocate and disassociate Key	Zeroize key and disassociate key from an entity.	NA	WrapKey; LockingObjectDEK AuthenticatedUseHmacKey	Controller	E; Z, R; E;	CCS
TCG Update Key	Erase user data in a namespace by changing the encryption key.	DRBG, AES-KW, CKG	DrbgState; WrapKey; RDSKey; SumRDSKey; LockingObjectDEK; EphemeralSumRdskWrapKey; AuthenticatedUseHmacKey	Controller	E; E; E; E, W; Z, G, R; E; E	CCS

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
TCG Set PIN	Set PIN which is used in generating a key to wrap a TCG credential.	PBKDF, DRBG, AES-KW, CKG, HMAC	Password; DrbgState; WrapKey; PasswordWrapKey; RDSKey; SumRDSKey; EphemeralSumRdskWrapKey; AuthenticatedUseHmacKey	Controller	W, E, Z; E; E; G, E, Z; G, W; G, W; E; E	CCS
TCG Revert, Activate, Reactivate	Revert to FOB, Revert to FOB with TCG Activated.	AES-KW, HMAC, DRBG, CKG	RootHmacKey; DrbgState; WrapKey; RdsKey; SumRdsKey; NameSpaceDEK; LockingObjectDEK; AuthenticatedUseHmacKey	Controller	E; E; E; Z; Z; Z, G; Z, G; E	CCS
TCG HMAC Generation	Generate an HMAC over the prescribed TCG content.	HMAC	AuthenticatedUseHmacKey; DrbgState; RootKeyWrapKey; TweakKey; WrapKey; Password; PassordWrapKey	Controller	E; R; E; R; E, R; G, E; G, E	CCS
Manifest Load	RSA Verify trusted list of PKs.	RSA Verify	$K_{ManifestPub\_ROM}$	Controller	E	CCS
CSP Load	Restore persistent SSPs.	AES-KW HMAC	RootHmacKey; RootKeyWrapKey; DrbgState; WrapKey; AuthenticatedUseHmacKey; TweakKey; PspHmacKey	Controller	E; E; W; W; W; W; W	CCS
Write/Read	Encryption / Decryption of user data to / from a user data range.	DPE-AES-XTS	NamespaceDEK; LockingObjectDEK; TweakKey	Controller	E; E; E	CCS
Get Status	Get information about the operational state of the drive. This service provides the requisite data for the Show module's versioning information requirement.	NA	NA	Controller	NA	CCS
Firmware Signature Check	Verify firmware image signature before persisting.	RSA Verify	$K_{FWCBootloaderVerify}$; $K_{FWModuleVerify}$; $K_{FWControllerVerify}$	Controller	E; E; E	CCS

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Factory Auth	Authentication for factory-restricted services.	RSA Verify, DRBG	$K_{AuthPub}$; $K_{VSAuthPub}$; DrbgState	Controller	E; E; E, W	CSS
Device Deprovision	Deprovision the device, zeroize all SSPs.	NA	All CSPs	Controller	Z	CCS
Generate KeyDerivationKey	Generate a new KeyDerivationKey.	DRBG, CKG	DrbgState; KeyDerivationKey; Entropy Input; RootHmacKey; RootKeyWrapKey; RootPublicMacKey; AworHmacKey; AworWrapKey; WrapKey; AuthenticatedUseHmacKey; PspHmacKey; TweakKey	Controller	G, E; G, E; W, E; G, E; G, E; G; G; G; G, E; G, E; G; G	CCS
Zeroize	Destroys all keys. Must be performed under the direct control of the operator.	Factory zeroization process	All CSPs	Controller	Z	CCS

5 Software/Firmware Security

The Module is composed of the following firmware components:

- Security Subsystem Operational: Runtime SCSS V2.3
- Security Subsystem Bootloader: Bootloader V1.0
- Function ROM v2.0
- Boot ROM v1.0

The pre-operational firmware integrity tests are performed using RSA SHA2-256 signature verification with a 2048-bit or 3072-bit key. The bootloader and operational runtime firmware are loadable components and are protected with the authentication technique, RSA SHA2-256 signature verification with a 2048-bit or 3072-bit key. Firmware candidates are isolated from load until they have successfully passed the Firmware Load Test. Firmware load and integrity checks are defined in the self-test section of this security policy.

The ROM components are implemented in Non-Reconfigurable-Memory and are not subject to firmware integrity test per FIPS 140-3 IG 5.A.

The operator can initiate the firmware integrity test on demand by power cycling/resetting the SSD.

6 Operational Environment

The Module has a limited operational environment under the FIPS 140-3 definitions. The tested operational environment is listed in Table 2.

The Module includes a firmware verification and load service to support necessary updates. Firmware versions validated through the FIPS 140-3 CMVP will be explicitly identified on a validation certificate. Any firmware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

7 Physical Security

The Module is a Single Chip Hardware sub-chip cryptographic subsystem, and the embodiment is a single chip. The chip is encapsulated in a standard IC package. The IC packaging itself provides the necessary opacity and tamper evidence required for Level 2 conformance.

Table 10 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
IC packaging	On initial receipt of the device and periodically afterwards	Inspect for evidence of prying or removal of the chip packaging. See Examples below. If tampering is suspected, then the device containing the IC should be removed from service and the site administrator should be contacted.

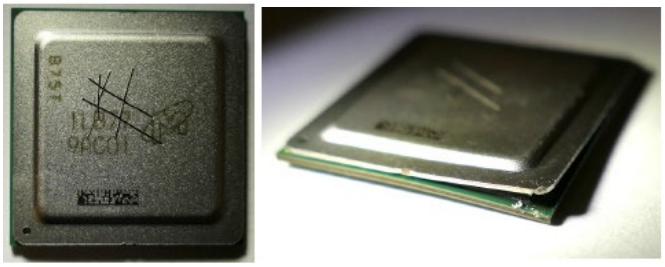

Figure 3 – Tamper Evidence Example

8 Non-Invasive Security

The Module does not implement any mitigation method against non-invasive attack.

9 Sensitive Security Parameter (SSP) Management

The SSPs access methods are described in below.

The SSPs management methods as shown in Table 11 below are defined as:

- **G1** = Externally generated and installed during manufacturing
- **G2** = Internally generated using the DRBG
- **G3** = Derived using SP 800-108 compliant KBKDF
- **G4** = Derived using SP 800-132 compliant PBKDF2
- **S1** = Only stored in volatile memory (RAM).
- **S2** = Stored in e-Fuse in plaintext
- **S3** = Stored in register in plaintext
- **S4** = Stored in ROM in plaintext
- **E1** = Input in plaintext
- **E2** = Input signed and verified using $K_{ManifestPub\_ROM}$
- **E3** = Input using SP800-38F AES key Transport
- **O1** = Output in plaintext public key
- **O2** = Output using SP800-38F Key Transport (specify AES key wrap key)
- **O3** = Output using KTS-IFC [56Br2]
- **Z1** = Zeroized implicitly after use, by Module power cycle, and reset
- **Z2** = Zeroized explicitly by the “zeroize” service by overwriting with a fixed pattern

9.1 Sensitive Security Parameters (SSP)

All CSPs and PSPs used by the Module are described in this section. All usage of these SSPs by the Module is described in the services detailed in Section 4.3. The numbers and letters within square brackets reference standards which are defined in the References and Definitions section of this Security Policy.

Table 11 – SSPs

Key/SSP/Name/Type	Strength	Security Function and Cert. Number	Gene-ration	Import /Export	Establish ment	Storage	Zeroiza-tion	Use & Related keys
AuthenticatedUseHmacKey	256	HMAC #A2521	G2	E3 / O2 by RootKeyWrapKey or AworWrapKey	N/A	S1	Z1, Z2	Integrity verification of TCG table data
AworWrapKey	256	KTS #A2520	G3 from KeyDerivationKey	N/A	N/A	S1	Z1, Z2	Key encryption
AworHmacKey	256	HMAC #A2521	G3 from KeyDerivationKey	N/A	N/A	S1	Z1, Z2	Integrity verification of TCG context data
DrbgState	256	HASH DRBG #A2520	G2	E3 / O2 by RootKeyWrapKey or AworWrapKey	N/A	S1	Z1, Z2	HASH_DRBG internal state (V and C are each 55 bytes)

Key/SSP/Name/Type	Strength	Security Function and Cert. Number	Gene-ration	Import /Export	Establishment	Storage	Zeroiza-tion	Use & Related keys
EphemeralSumRdskWrapKey	256	KTS #A2520	G2	E3 / O2 by AworWrapKey	N/A	S1	Z1, Z2	Key wrap of SumRdsKey
Entropy Input	256	HASH DRBG #A2520	G1	E1	N/A	S1	Z1	128 bytes of Entropy and 64 bytes of Nonce
KeyDerivationKey	256	KDF #A2521	G2	N/A	N/A	S2	Z2	Master key used to derive other keys
LockingObjectDEK	256	AES #A2523	G2	E3 / O2 by RdsKey, SumRdsKey or WrapKey	N/A	S1, S3	Z1, Z2	Data encryption
NamespaceDEK	256	AES #A2523	G2	E3 / O2 by RdsKey, SumRdsKey or WrapKey	N/A	S1, S3	Z1, Z2	Data encryption
Password	256	PBKDF #A2520	N/A	E1	N/A	S1	Z1	Used with PBKDF2 to derive the PasswordWrapKey, Password is 32 bytes in length
PasswordWrapKey	256	KTS #A2520	G4	N/A	N/A	S1	Z1	Key wrap of RdsKey or SumRdsKey
PspHmacKey	256	HMAC #A2521	G2	E3 / O2 by RootKeyWrapKey or AworWrapKey	N/A	S1	Z1, Z2	Integrity verification of public TCG content
RdsKey	256	KTS #A2520	G2	E3 / O2 by PasswordWrapKey or AworWrapKey	N/A	S1	Z1, Z2	Key wrap of LockingObjectDEK and NameSpaceDEK
RootHmacKey	256	HMAC #A2521	G3 from KeyDerivationKey	E3 / O2 by AworWrapKey	N/A	S1	Z1, Z2	Integrity checking
RootKeyWrapKey	256	KTS #A2520	G3 from KeyDerivationKey	E3 / O2 by AworWrapKey	N/A	S1	Z1, Z2	Key wrapping
RootPublicMacKey	256	HMAC #A2521	G3 from KeyDerivationKey	E3 / O2 by AworWrapKey	N/A	S1	Z1, Z2	Integrity verification of external TCG content
SumRdsKey	256	KTS #A2520	G2	E3 / O2 by AworWrapKey, EphemeralSumRdskWrapKey, or by PasswordWrapKey	N/A	S1	Z1, Z2	Key wrap of LockingObjectDEK and NameSpaceDEK

Key/SSP/Name/Type	Strength	Security Function and Cert. Number	Gene-ration	Import /Export	Establishment	Storage	Zeroiza-tion	Use & Related keys
SUP Seed	256	PBKDF #A2520	G2	O3 by $K_{DeviceWrappingPub}$	N/A	S1	Z1	Random value used in password creation
TweakKey	256	AES #A2523	G2	E3 / O2 by RootKeyWrapKey or AworWrapKey	N/A	S1, S3	Z1, Z2	Data encryption
WrapKey	256	KTS #A2520	G2	E3 / O2 by RootKeyWrapKey or AworWrapKey	N/A	S1	Z1, Z2	Key wrap of LockingObjectDEK and NameSpaceDEK
$K_{AuthPub}$	112 128	RSA SigVer (FIPS186-4) #A2521	N/A	E2 / O1	N/A	S1	Z1	RSA 2048/3072 Public Key for Factory-restricted services signature verification
$K_{DeviceWrappingPub}$	112 128	KTS-IFC #A2520	N/A	E2 / O1	N/A	S1	Z1	RSA 2048/3072 Public Key for SUP Generate
$K_{FWCBootloaderVerify}$ (Not an SSP)	112 128	RSA SigVer (FIPS186-4) #A2521	N/A	E2	N/A	S1	Z1	RSA 2048/3072 Public Key for Bootloader firmware signature verification
$K_{FWControllerVerify}$	112 128	RSA SigVer (FIPS186-4) #A2521	N/A	E2	N/A	S1	Z1	RSA 2048/3072 Public Key for Controller signature verification
$K_{FWModuleVerify}$ (Not an SSP)	112 128	RSA SigVer (FIPS186-4) #A2521	N/A	E2	N/A	S1	Z1	RSA 2048/3072 Public Key for runtime firmware signature verification
$K_{ManifestPub\_ROM}$ (Not an SSP)	112 128	RSA SigVer (FIPS186-4) #A2521	N/A	N/A. Pre-installed.	N/A	S4	N/A. Used solely for self-tests and can be revoked	RSA 2048/3072 Public Key for manifest signature verification
$K_{VSAuthPub}$	112 128	RSA SigVer (FIPS186-4) #A2521	N/A	E2 / O1	N/A	S1	Z1	RSA 2048/3072 Public Key for Factory-restricted signature verification

9.2 DRBG Randomness Source

The DRBG Randomness source (i.e., entropy) is loaded at manufacturing. Per IG 9.3.A, Example 2A, there is no assurance of the minimum strength of generated SSPs. The DRBG mechanism is SHA2-256, which has a security strength of 256-bits (per SP800-57, Part 1, Revision 5). The HASH DRBG is seeded with 128 bytes of entropy and 64 bytes of nonce material during manufacturing and is assumed to initialize the HASH DRBG to the full 256-bits security strength.

10 Self-Tests

The Module performs self-tests to ensure the proper operation of the Module. Per FIPS 140-3 these are categorized as either pre-operational self-tests or conditional self-tests.

Pre-operational and conditional self-tests are available on demand by resetting or power cycling the Module.

The self-tests error states and status indicator are described in Table 12 below:

Table 12 – Error States and Indicators

Error state	Description	Indicator
ES1	The Function ROM fails a KAT	Triggered by cryptographic KAT failure. The Module enters the ES1 error state and outputs A Cryptographic Self-Test Failure status in response to any service request
ES2	The Module fails the firmware load test or the Firmware Integrity test	The Module enters the ES2 error state and outputs a verification failure status in response to the firmware load test or the firmware integrity test
ES3	The Module fails conditional KAT self-test. Non-operational state. No services beside status services are allowed	The Module enters the ES3 error state and will output a self-test failure status to any service request

The Module performs the following pre-operational self-tests:

Table 13 – Pre-Operational Self-Test

Security Function	Method	Description	Error state
Bootloader Firmware (Bootloader V1.0) integrity test	RSA SHA2-256 Signature Verification	An RSA 2048 or 3072-bit Signature Verification is executed on the whole Bootloader copied into the Module	ES2
SEE Firmware (Runtime SCSS V2.3) integrity test	RSA SHA2-256 Signature Verification	An RSA 2048 or 3072-bit Signature Verification is executed on the whole Bootloader copied into the Module	ES2

The Module performs the following conditional self-tests:

Table 14 – Conditional Self-Tests

Security Function	Method	Description	Error state
ROM HMAC	HMAC_ SHA2-256	HMAC SHA2-256 KAT. This test occurs before the Pre-Operational firmware integrity test.	ES1
ROM RSA	SHS/RSA	2048 RSA PKCS#1_v1.5 Verification KAT with SHA2-256 KAT, which satisfies the self-test requirements for KTS-IFC per IG D.G; the Module only supports the public key operations for RSA Signature Verification and KTS-IFC Encapsulation. This test occurs before the Pre-Operational firmware integrity test.	ES1
AES – KW (Key Wrap)	KAT	(Auxiliary) AES-256 KW encryption KAT – Inclusive of AES ECB testing with 256-bit key per IG 10.3.B.	ES3
AES – KW (Key Unwrap)	KAT	(Auxiliary) AES-256 KW decryption KAT – Inclusive of AES ECB testing with 256-bit key per IG 10.3.B.	ES3
AES XTS – AUX and DPE Encryption	Comparative	256-bit AES-XTS encryption Comparative Answer Test with the AES-AUX and DPE AES-XTS implementations.	ES3
AES XTS – AUX and DPE Decryption	Comparative	256-bit AES-XTS decryption Comparative Answer Test with the AES-AUX and DPE AES-XTS implementations.	ES3
DRBG	KAT	HASH_DRBG (SHA2-256) instantiation, generate, and reseed KATs performed before the first random data generation.	ES3
PBKDF	KAT	Option 1a using HMAC SHA2-256. Password size is 32 Bytes. Key generated is 256 bits.	ES3
KBKDF	KAT	Known answer test. Inclusive of HMAC-SHA2-256 KAT. Key size requested is 256 bits.	ES3
BootLoader Firmware Load test	RSA PKCS#1_v1.5 SHA2-256	A 2048 or 3072-bit RSA Signature Verification is executed on the bootloader copied into the Module.	ES2
SEE Firmware Load test	RSA PKCS#1_v1.5 SHA2-256	A 2048 or 3072-bit RSA Signature Verification is executed on the SEE firmware copied into the Module.	ES2

DPE self-tests are initiated when functionality is requested. All other self-tests are initiated automatically when the module boots. The self-tests cannot be interrupted and will run to completion.

11 Life-Cycle Assurance

This section documents the operational behavior of the device.

11.1 Security Initialization

The device is shipped from the factory in the Approved mode of operation and no further initialization is required to operate in the Approved mode. Going further, it is not possible to configure the module in such a way that it would operate in a non-compliant state or non-Approved mode. On receipt of the

Module, examine the product to ensure it has not been tampered with during shipping according to the procedures outlined in Section 7.

12 Mitigation of Other Attacks

The Module does not implement any mitigation method against other attacks.

13 References and Definitions

The following standards are referred to in this Security Policy.

Table 15 – References

Abbreviation	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, March 22, 2019
[ISO19790]	*International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017*
[ISO24759]	*International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015*
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, May 16, 2022*
[108]	*NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 2, March 2019*
[132]	*NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, December 2010*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*

Abbreviation	Full Specification Name
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005*
[38E]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, Special Publication 800-38E, January 2010*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56Br2]	*NIST Special Publication 800-56B Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Finite Field Cryptography, March 2019*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*
[ACS-3]	*ACS-3 Reporting Security Compliance December 1,2009*
[TCG-SSC-Opal]	*TCG Storage Security Subsystem Class: Opal, Specification*
[TCG-SACS]	*TCG Storage Architecture Core Specification*
[TCG-SIIS]	*TCG Storage Interface Interactions Specification*

Table 16– Acronyms and Definitions

Acronym	Definition
KAT	Known Answer Test
SSP	Sensitive Security Parameter
AK	Authentication key
DEK	Data Encryption Key
LBA	Logical Block Address
MSID	Manufacturing SID. Public value used as part of the default PIN
PSID	Physical SID, a public unique value for each drive
SED	Self-Encrypting Drive
SID	Security ID, PIN for Drive Owner CO Role - TCG OPAL
TCG	Trusted Computing Group