Micron Technology, Inc.

Micron® MTC21-P4 Controller
Sub Chip Security Subsystem

Non-Proprietary FIPS 140-3 Security Policy

Document Version: 1.6
Date: March 27, 2025

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® MTC21-P4 Controller Sub Chip Security Subsystem module, hereafter denoted 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 Module incorporates numerous hardware and firmware implementations of cryptographic algorithms, as outlined in Section 2.4. The following is an overview of how the cryptographic algorithm implementations relate to the Module:

- CAVP Certificates #A2830, #A2831, #A2832, and #A2834 are hardware implementations of algorithms within the Module.
- CAVP Certificates #A2833 and #A2835 are hardware IP cores implementing the AES algorithm.
- CAVP Certificates #C1278 and #A2272 are firmware implementations provided by Synopsys, which have been ported into the Runtime SCSS firmware for the purposes of entropy generation.
- CAVP Certificates #2826, #A2827, # A2828, #A2829, and #A4269 are firmware implementations implemented in the Runtime SCSS firmware.

Each of the hardware and firmware implementations listed above are independently version controlled from the rest of the hardware and firmware. Any change to the hardware implementation listed above will result in the implementation version update, as well as the Module hardware version update. Any change to the firmware implementation listed above will result in the implementation version update, as well as the Module firmware version update.

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

Table 1 – Security Levels

Section	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
	Overall	2

2 Cryptographic Module Specification

The Module is a Single-Chip Hardware Sub-Chip cryptographic subsystem.

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated cryptographic controllers. The Module is a security subsystem within the ASIC Micron® MTC21-P4 SSD Controller package, whose intended use environment is within an SSD Controller. The Module is the Micron® MTC21-P4 Controller Sub Chip Security Subsystem, P/N and HW Version TC v2.1, Function ROM v3.0, Boot ROM v1.0 with Firmware Versions as indicated in Table 2

Figure 1 – Micron® MTC21-P4 ASIC

2.1 Tested Configuration

The cryptographic module is tested on the following:

Table 2 – Hardware Tested Configuration

Model	Hardware	Firmware Version	Tested Configuration
Micron® MTC21-P4 Controller Sub Chip Security Subsystem	TC v2.1	Runtime SCSS v2.2, Bootloader v1.0, Function ROM v3.0, Boot ROM v1.0	Micron® MTC21-P4 SSD Controller
Micron® MTC21-P4 Controller Sub Chip Security Subsystem	TC v2.1	Runtime SCSS v2.3, Bootloader v1.1, Function ROM v3.0, Boot ROM v1.0	Micron® MTC21-P4 SSD Controller
Micron® MTC21-P4 Controller Sub Chip Security Subsystem	TC v2.1	Runtime SCSS v2.4, Bootloader v1.1, Function ROM v3.0, Boot ROM v1.0	Micron® MTC21-P4 SSD Controller
Micron® MTC21-P4 Controller Sub Chip Security Subsystem	TC v2.1	Runtime SCSS v2.5, Bootloader v1.0a, Function ROM v3.0, Boot ROM v1.0	Micron® MTC21-P4 SSD Controller

The Module versioning information is provided through the “Get Status” service and is returned as TCG Level 0 discovery content.
The Module is Hardware and as such, Tested and Vendor Affirmed Operational Environments do not apply.

2.2 Cryptographic Boundary

The single-chip hardware, Micron® MTC21-P4 ASIC, is depicted in Figure 1 above, which also defines the physical boundary of the Module. The cryptographic boundary of the Module is defined by the Sub Chip Security Subsystem and includes all cryptographic algorithm implementations, as depicted by the red outline line in Figure 2 below. The TOEPP is defined as the area outside of the cryptographic boundary, but within the physical boundary of the single-chip on which the Module is installed.

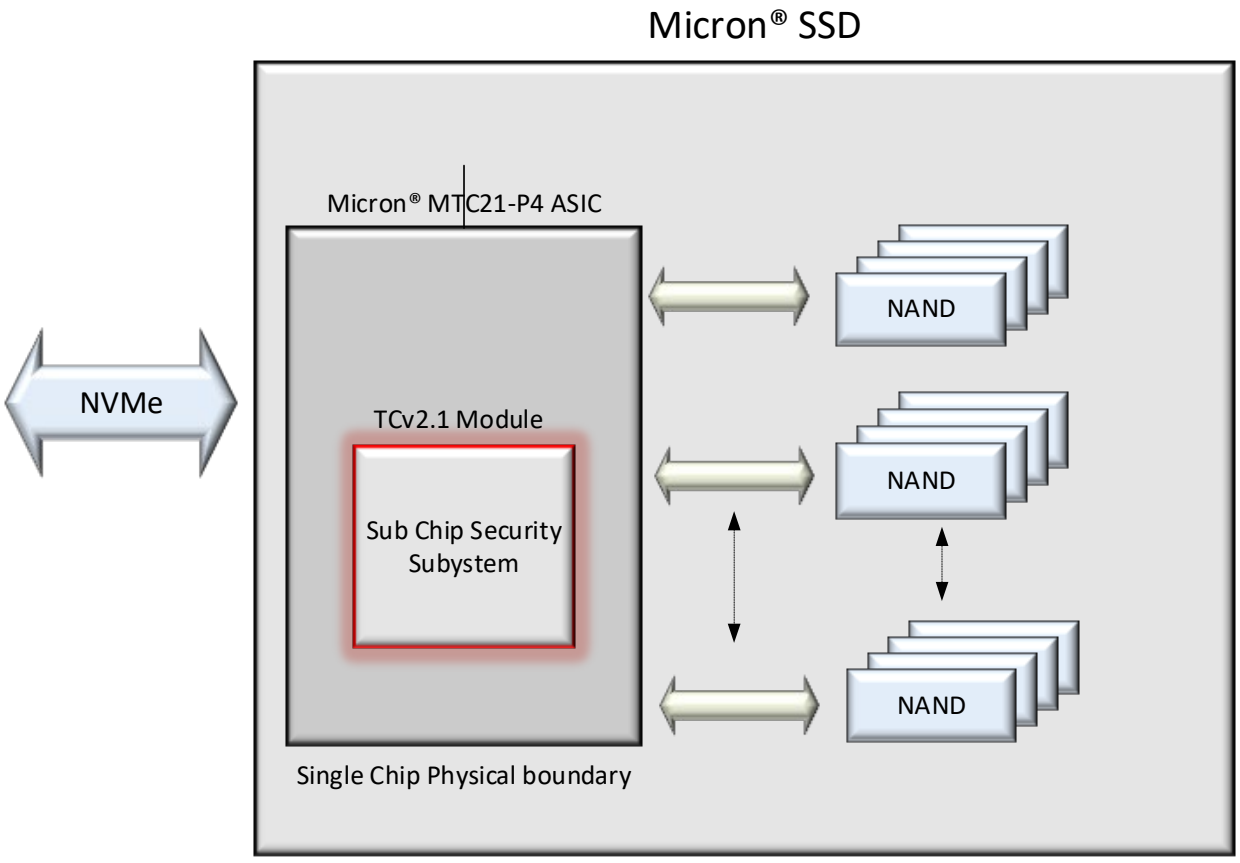

Figure 2 – Module

2.3 Modes of Operation

The Module only supports an Approved mode of operation and is configured to only operate in this Approved mode during manufacturing. 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. No initialization of the Module is required.

The Module provides services through NVME industry standard commands as well as TCG commands. In addition, extra features are provided through the TCG commands. The Module provides these services to support the TCG mode of operation but is not responsible for TCG management functions.

2.4 Security Functions

The Module implements the Approved cryptographic functions listed in the table below. The numbers and letters within square brackets reference standards which are defined in the References and Definitions section of this Security Policy.
Notes: The AES XTS algorithm implementation includes a check to ensure Key_1 ≠ Key_2; Key_1 and Key_2 are generated independently.
AES XTS is only used for storage purposes per SP 800-38E

Table 3 – Approved Algorithms

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size/ Key Strength	Use/Function
A2272	AES [197]	AES 128	Conditioning Component Block Cipher Derivation Function SP800-90B	Conditioning of TRNG data
A2833	AES [197]	AES-ECB [38A]	Key Sizes: 256	Encrypt, Decrypt (Auxiliary)
		AES-XTS Testing Revision 2.0 [38E]	Key Sizes: 256	Encrypt, Decrypt (Auxiliary)
A2835	AES [197]	AES-ECB [38A]	Key Sizes: 256	Encrypt, Decrypt (Datapath)
		AES-XTS Testing Revision 2.0 [38E]	Key Sizes: 256	Encrypt, Decrypt (Datapath)
C1278	AES [197]	AES-ECB [38A]	Key Sizes: 128, 256	Encrypt. Used only within the DRBG. 128-bit key is tested but not used
		AES-CTR [38A]	Key Sizes: 128, 256	Encrypt. Used only within the DRBG. 128-bit key is tested but not used
C1278	Counter DRBG [90A]	Counter DRBG	Counter DRBG AES 256 [38A] Key Size 256 AES 128 with Key Size 128 tested, but not used.	Deterministic Random Bit Generation Security Strength = 256
A2827/ A4269	ECDSA [186]	ECDSA KeyGen	Curve P-384	Key generation for attestation
	ECDSA [186]	ECDSA SigVer	Curve P-384 SHA2-384	Signature verification for authentication
	ECDSA [186]	ECDSA SigGen	Curve P-384 SHA2-384	Signature generation for certificate and measurements
	ECDSA [186]	ECDSA KeyVer	Curve P-384	Key verification
	ENT [(90B]	ENT (P)	Security Strength = 256 bits	Entropy generation

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size/ Key Strength	Use/Function
A2830	HMAC-SHA2-384 [198]	HMAC-SHA2-384	Key Sizes: 384 bits λ = 384	Key derivation. Data Authentication
	HMAC-SHA2-512/256 [198]	HMAC-SHA2-512/256	Key Sizes: 256 bits λ = 256	Key derivation. Data Authentication
	HMAC-SHA2-512 [198]	HMAC-SHA2-512	Key Sizes: 512 bits λ = 512	Key derivation. Data Authentication Tested but not used
A2832	KDF-SP800-108 [108]	Counter	HMAC-SHA2-384 HMAC-SHA2-512/256	Key Based Key Derivation
	KDF-SP800-108 [108]	Counter	HMAC-SHA2-512/256	Key Based Key Derivation
A2828	KTS [38F]	AES-KW	Key Sizes:256	CSP Wrapping/Unwrapping (Uses Auxiliary ECB)
A2829	KTS-IFC [56B]	KTS-OAEP-basic	n = 3072 SHA2-384 n = 4096 SHA2-384	Key transport methodology provides between 128 and 150 bits of encryption strength
A2826	PBKDF [132]	Option 1a	sLen = 256bits C = 300 HMAC- SHA2-512/256 Key Size 256	Password Based Key Derivation. Keys derived from passwords may only be used in storage applications. Derived keys are used as input to AES-KW to wrap and unwrap sensitive data. Password length and format are specified in Table 11 and are 32 bytes long. Use of the derived password in the associated unwrap process is limited to 5 retries at which time the Module will need to be reset. This effectively eliminates the possibility of determining the password through exhaustive methods. The PBKDF iteration count (C) is chosen to be as high as can be tolerated without impacting the performance of the system boot up process
A2831	RSA [186]	RSA SigVer (FIPS186-4) PKCS1_v1.5 PKCS1_PSS	n = 3072 SHA2-384/SHA2-512 n = 4096 SHA2-384/SHA2-512	Signature verification
A2834	SHS [180]	SHA2-384 SHA2-512	SHA2	Message Digest Generation

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size/ Key Strength	Use/Function
		SHA2-512/256		SHA2-512/256 is tested but not used

Table 4 – Vendor Affirmed Approved Algorithms

Algorithm	Caveat	Use/Function
CKG [IG D.H]	[133] Sections 4 and 6.1 Direct symmetric key generation using unmodified DRBG output [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	Key Generation

The module does not support any non-Approved algorithms whatsoever. This includes algorithms that would otherwise be allowed in the Approved mode of operation, allowed in the Approved mode of operation with no security claimed, as well as not allowed in the Approved mode of operation.

The module's entropy was assessed before the ESV program was established and thus an entropy certificate is not applicable.

2.5 Security Function Implementation

The following table shows the Security Function Implementations of the Module:

Table 5 - Security Function Implementation (SFI)

Name	Type	Description	SF Properties	Algorithms/CAVP Cert
KTS	KTS	AES-KW – AES Cert. #A2828	Key establishment methodology provides 256 bits of encryption strength Key size: 256 bits	AES-KW/Cert. #A2828
KTS-IFC	KTS	KTS-IFC - RSA Cert. #A2829	Key transport methodology provides between 128 and 150 bits of encryption strength. Modulo: 3072, 4096 KTS-OAEP-basic Hash Algorithm: SHA2-384	KTS-IFC/Cert. #A2829

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 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.

2.7 Rules of Operation

The Module is embedded within the Micron® MTC21-P4 controller of the SSD. The Module shall be operated according to Section 11.

3 Cryptographic Module Interfaces

The Module's ports and associated logical interface categories are listed in Table 6.

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, the Controller (Cryptographic Officer).
Table 6 lists the Controller (Cryptographic Officer) 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. All services are associated with the Controller (Cryptographic Officer) role with a sub-set of Controller services requiring an additional layer of authentication described in Table 7 below as “factory-restricted”. These “factory-restricted” services require a second signature verification.
The Module does not support a maintenance role or bypass capability. The Module does not support concurrent operators.

Table 7 – Roles, Services, Input, and Output

Roles	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
Controller	Factory Auth	Signature	Verification status
Controller	Attestation	Attestation Request Information	Attestation response Info
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 7 below.

Table 8 – Roles and Authentication

Role	Authentication Method	Authentication Strength
Controller	Signature Verification	RSA 3072/4096 has a key strength of 128/150 bits. The probability of a successful verification from a single random attempt is at least $1/2^{128}$ which is < 1/1,000,000. This effectively eliminates the possibility of determining the private key through exhaustive methods. Each verification attempt takes 8ms, the maximum number of attempts which can be made in 1 minute is 7500, which results in a probability of $7500/2^{128}$ that a brute force attack within a given minute of time will be successful. For the factory-restricted services, the Controller must authenticate with a second RSA 3072/4096 key. This verification has an associated retry limit of 5. This controls the number of unsuccessful attempts before authentication is blocked until a system restart occurs.

The RSA keys used for Controller authentication are loaded into the Module as part of a key manifest. The key manifest is itself verified by the Module using RSA signature verification with a key installed during manufacturing, $K_{ManifestPub\_ROM}$.

4.3 Services

All services implemented by the Module are listed in the Table 8 below. 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 8 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 and 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/SSPs	Roles	Access rights to Keys/SSPs	Indicator
Self-Test	Run KAT tests on all cryptographic algorithms	All	Entropy Input	Any	G,E	CCS
			DrbgSeed		G,E	
			DrbgState		G	
SUP Authenticate	Unwrap SUP blob using PBKDF derived key	PBKDF, AES-KW	Password	Controller	W, E	CCS
			PasswordWrapKey		G, E	
SUP Generate	KTS-RSA wrap an internally generated random	DRBG, CKG, KTS-RSA, AES-KW, PBKDF	DrbgState	Controller	W, E	CCS
			$K_{DeviceWrappingPub;}$		E	
			PasswordWrapKey		G, E, Z	
			SUP Seed		G, E, Z	
TCG Authenticate	Unwrap TCG SSP using PBKDF derived key	PBKDF, AES-KW, CKG	Password	Controller	E	CCS
			SumRdsKey		W	
			RdsKey		W	
			PasswordWrapKey		G, E, Z	
			AuthenticatedUseHmacKey		E	
			EphemeralSumRdskWrapKey		E	
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	Controller	E, W	CCS
			WrapKey		E	
			RdsKey		G, E, R	
			SumRdsKey		G, E, R	
			NamespaceDEK		G, R	
			AuthenticatedUseHmacKey		E	
			EphemeralSumRdskWrapKey		E	
NVMe Deallocate and disassociate Key	Zeroize key and disassociate key from an entity	AES, AES-KW	NamespaceDEK	Controller	Z	CCS
			WrapKey		E	
			AuthenticatedUseHmacKey		E	
NVMe Update Key	Erase user data in a namespace by changing the encryption key	DRBG, AES-KW, CKG	DrbgState	Controller	E	CCS
			WrapKey		E	
			RdsKey		E	
			SumRdsKey		W, E	
			NamespaceDEK		Z, G, R	
			LockingObjectDEK		Z, G, R	
			AuthenticatedUseHmacKey		E	
			EphemeralSumRdskWrapKey		E	
Public HMAC Generation	Generate an HMAC over the prescribed content	HMAC SHA256	RootPublicMacKey	Controller	E	CCS
			PspHmacKey		E	
Load Range and Key	Load DEK into DPE for indicated range	AES-KW	TweakKey	Controller	W	CCS
			LockingObjectDEK		W	
			NamespaceDEK		W	
			RdsKey		E	
			SumRdsKey		W, E	
			WrapKey		E	
			EphemeralSumRdskWrapKey		E	
			AworWrapKey;		E	

Service	Description	Approved Security Functions	Keys/SSPs	Roles	Access rights to Keys/SSPs	Indicator
AWOR	Save, restore security operational context	KBKDF, AES-KW, HMAC, CKG	AworHmacKey	Controller	E	CCS
			WrapKey		W, R	
			AuthenticatedUseHmacKey		W, R	
			PspHmacKey		W, R	
			TweakKey		W, R	
			RdsKey		W, R	
			SumRdsKey		W, R	
			RootHmacKey		W, R	
			RootKeyWrapKey		W, R	
			RootPublicMacKey		W, R	
			EphemeralSumRdskWrapKey		W, R	
TCG Allocate and associate Key	Generate a key, wrap key and associate key with an entity	DRBG, AES-KW, CKG	DrbgState	Controller	E	CCS
			WrapKey		E	
			RdsKey		G, E, R	
			SumRdsKey		G, E, R	
			LockingObjectDEK		G, R	
			EphemeralSumRdskWrapKey		E	
			AuthenticatedUseHmacKey		E	
TCG Deallocate and disassociate Key	Zeroize key and disassociate key from an entity	NA	WrapKey	Controller	E	CCS
			LockingObjectDEK		Z, R	
			AuthenticatedUseHmacKey		E	
TCG Update Key	Erase user data in a namespace by changing the encryption key	DRBG, AES-KW, CKG	DrbgState	Controller	E	CCS
			WrapKey		E	
			RdsKey		E	
			SumRdsKey;		E, W	
			LockingObjectDEK		Z, G, R	
			EphemeralSumRdskWrapKey		E	
			AuthenticatedUseHmacKey		E	
TCG Set PIN	Set PIN which is used in generating a key to wrap a TCG credential	PBKDF, DRBG, AES-KW, CKG, HMAC	Password	Controller	W, E, Z	CCS
			DrbgState		E	
			WrapKey		E	
			PasswordWrapKey		G, E, Z	
			RdsKey		G, W	
			SumRdsKey		G, W	
			EphemeralSumRdskWrapKey		E	
			AuthenticatedUseHmacKey		E	
TCG Revert, Activate, Reactivate	Revert to FOB, Revert to FOB with TCG Activated	AES-KW, HMAC, DRBG, CKG	RootHmacKey	Controller	E	CCS
			DrbgState		E	
			WrapKey		E;	
			RdsKey		Z	
			SumRdsKey		Z	
			NameSpaceDEK		Z, G	
			LockingObjecDEK		Z, G	
			AuthenticatedUseHmacKey		E	
TCG HMAC Generation	Generate an HMAC over the prescribed TCG content	HMAC	AuthenticatedUseHmacKey	Controller	E	CCS
			DrbgState		R	
			RootKeyWrapKey		E	
			TweakKey		R	
			WrapKey		E, R	
			Password		G, E	
			PassordWrapKey		G, E	
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	Controller	E	CCS
			RootKeyWrapKey		E	
			DrbgState		W	

Service	Description	Approved Security Functions	Keys/SSPs	Roles	Access rights to Keys/SSPs	Indicator
			WrapKey		W	
			AuthenticatedUseHmacKey		W	
			TweakKey		W	
			PspHmacKey		W	
Write/Read	Encryption / Decryption of user data to / from a user data range	DPE-AES-XTS	NamespaceDEK	Controller	E	CCS
			LockingObjectDEK		E	
			TweakKey		E	
Get Status	Get information about the operational state of the drive, as well as versioning information.	NA	NA	Controller	NA	CCS
Firmware Signature Check	Verify firmware image signature before persisting	RSA Verify	$K_{FWCBootloaderVerify}$	Controller	E	CCS
			$K_{FWModuleVerify}$		E	
			$K_{FWControllerVerify}$		E	
Factory Auth	Authentication for factory-restricted services	RSA Verify, DRBG	$K_{AuthPub}$	Controller	E	CSS
			$K_{VSAuthPub}$		E	
			DrbgState		E	
Device Deprovision	Deprovision the device, zeroize all SSPs	NA	All CSPs	Controller	Z	CCS
Generate KeyDerivationKey	Generate a new KeyDerivationKey	DRBG, CKG	DrbgState	Controller	G, E	CCS
			KeyDerivationKey		G, E	
			RootHmacKey		G, E	
			RootKeyWrapKey		G, E	
			RootPublicMacKey		G	
			AworHmacKey		G	
			AworWrapKey		G	
			WrapKey		G, E	
			AuthenticatedUseHmacKey		G, E	
			PspHmacKey		G	
			TweakKey		G	
Zeroize	Destroys all keys. Must be performed under the direct control of the operator	Factory zeroization process	All CSPs	Controller	Z	CCS
Attestation	Device cryptographic identity and attestation	EC-DSA Generate, EC-DSA Sign, DRBG, AES-KW, SHS	$K_{DeviceIDPrivate}$	Controller	G, E, R, W, Z	CCS
			$K_{DeviceIDPublic}$		G, R	
			$K_{AliasPrivate}$		G, E	
			$K_{AliasPublic}$		G, R	
			DrbgState		E	
			$K_{DeviceIDWrapKey}$		G, E, Z	
			UDS		G,E	
			UDS_KDK		E	

The module does not support any non-Approved services, as it does not support a non-Approved mode of operation.

5 Software/Firmware Security

The Module is composed of the following component(s):

- Security Subsystem Operational: Runtime SCSS firmware
- Security Subsystem Bootloader: Bootloader firmware
- Function ROM v3.0
- Boot ROM v1.0

The Runtime SCSS firmware and Bootloader firmware are loadable components and are protected with the firmware load test using RSA signatures with a 3072-bit or 4096-bit key. This signature is also used to verify the integrity of the firmware prior to firmware execution. 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 tests per FIPS 140-3 IG 5.A

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

6 Operational Environment

The Module has a limited operational environment under the FIPS 140-3 definitions. The hardware tested configuration 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, and the embodiment is a production grade 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. If tampering is suspected, then the device containing the IC should be removed from service and the site administrator should be contacted. See Example below

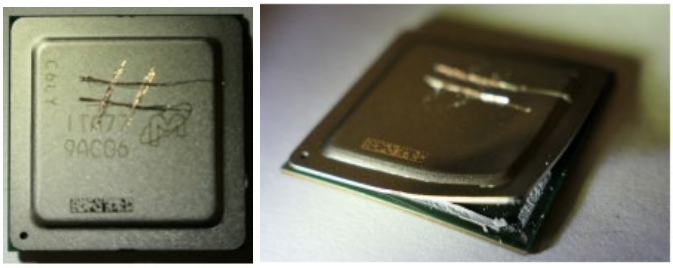

Figure 3 – Tamper Evidence Example

The module does not support EFP/EFT mechanisms, as EFP/EFT are only applicable at Level 3 and the module only asserts Level 2 compliance.
Hardness testing was not performed as it is only applicable at Level 3 and the module only asserts Level 2 compliance.

8 Non-Invasive Security

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

9 Sensitive Security Parameter (SSP) Management

The SSPs management methods as shown Table 10 are defined as:

- **G1** = Externally generated using the DRBG during manufacturing
- **G2** = Internally generated using the DRBG
- **G3** = Derived using SP 800-108 compliant KBKDF
- **G4** = Derived using SP 800-132 compliant PBKDF2
- **G5** = Generated from an SP 800-90B compliant entropy source
- **S1** = Only stored in dynamic, volatile memory (RAM) in plaintext
- **S2** = Stored in static e-Fuse in plaintext
- **S3** = Stored in static register in plaintext
- **S4** = Stored in static ROM in plaintext
- **E1** = Input in plaintext
- **E2** = Input signed and verified using $K_{ManifestPub\_ROM}$
- **E3** = Input using KTS (AES-KW)
- **O1** = Output in plaintext public key
- **O2** = Output using SP800-38F Key Transport (specify AES key wrap key)
- **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, PSPs, and non-SSPs used by the Module are described in this section. All usage of these SSPs by the Module is described in the services detailed in 4.3..

Table 11 – SSPs

Key/SSP/Name/Type	Strength	Security Function Cert. Number	Generat-ion	Import/Export	Establish-ment	Storage	Zeroiza-tion	Use & Related keys
AuthenticatedUseHmacKey (HMAC SHA2-256)	256	HMAC / A2830	G2	E3 / O2 by RootKeyWrapKey or AworWrapKey	N/A	S1	Z1, Z2	Integrity generation and checking of TCG table data
AworWrapKey (AES-KW)	256	KTS / A2828	G3 from KeyDerivationKey	N/A	N/A	S1	Z1, Z2	Key encryption
AworHmacKey (HMAC SHA2-512/256)	256	HMAC / A2830	G3 from KeyDerivationKey	N/A	N/A	S1	Z1, Z2	Integrity generation and checking of TCG context data
DrbgState	256	DRBG / C1278	G2	N/A	N/A	S1	Z1, Z2	CTR_DRBG internal state Key and V

Key/SSP/Name/Type	Strength	Security Function Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization	Use & Related keys
DrbgSeed	256	DRBG / C1278	G5	N/A	N/A	S1	Z1, Z2	Used to seed the DRBG.
EphemeralSumRdskWrapKey (AES-KW)	256	KTS /A2828	G2	E3 / O2 by AworWrapKey	N/A	S1	Z1, Z2	Key wrap of: SumRdsKeys,
Entropy Input	256	ENT (P)	G5	N/A	N/A	S1	Z1	Used to create DrbgSeed.
KeyDerivationKey	256	KDF SP800-108 / A2832	G1	N/A	N/A	S2	Z2	Master key used to derive other keys
LockingObjectDEK (AES-XTS)	256	AES-XTS Testing Revision 2.0 / A2833	G2	E3 / O2 by RdsKey, SumRdsKey, or WrapKey	N/A	S1, S3	Z1, Z2	Data encryption
NamespaceDEK (AES-XTS)	256	AES-XTS Testing Revision 2.0 / A2833	G2	E3 / O2 by RdsKey, SumRdsKey, or WrapKey	N/A	S1, S3	Z1, Z2	Data encryption
Password	256	PBKDF2/ A2826	N/A	E1	N/A	S1	Z1	Used with PBKDF2 to derive the PasswordWrapKey Password is 32 bytes of binary data
PasswordWrapKey (AES-KW)	256	KTS /A2828	G4	N/A	N/A	S1	Z1	Derived using PBKDF and Password. Key encryption of: RdsKey or SumRdsKey
PspHmacKey (HMAC SHA2-512/256)	256	HMAC /A2830	G2	E3 / O2 by AworWrapKey or RootKeyWrapKey	N/A	S1	Z1, Z2	Integrity generation and checking public TCG content
RdsKey (AES-KW)	256	KTS /A2828	G2	E3 / O2 PasswordWrapKey or AworWrapKey	N/A	S1	Z1, Z2	Key encryption of: LockingObjectDEK, NameSpaceDEK
RootHmacKey (HMAC SHA2-512/256)	256	HMAC / A2830	G3 from KeyDerivationKey	E3 / O2 by AworWrapKey	N/A	S1	Z1, Z2	Integrity checking

Key/SSP/Name/Type	Strength	Security Function Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization	Use & Related keys
RootKeyWrapKey (AES-KW)	256	KTS /A2828	G3 from KeyDerivationKey	E3 / O2 by AworWrapKey	N/A	S1	Z1, Z2	Key encryption of: DrbgState WrapKey, AuthenticatedUseHmacKey TweakKey, RdsKey,
RootPublicMacKey (HMAC SHA2-512/256)	256	HMAC / A2830	G3 from KeyDerivationKey	E3 / O2 by AworWrapKey	N/A	S1	Z1, Z2	Integrity checking of TCG content of files stored outside of the boundary.
SumRdsKey (AES-KW)	256	KTS /A2828	G2	E3 / O2 by AworWrapKey, EphemeralSumRdskWrapKey, or PasswordWrapKey	N/A	S1	Z1, Z2	Key encryption of: LockingObjectDEK, NameSpaceDEK
SUP Seed	256	PBKDF2 / A2826	G2	O3 by $K_{DeviceWrappingPub}$	N/A	S1	Z1	Random value used to create an internal password.
TweakKey (AES-XTS)	256	AES-XTS Testing Revision 2.0 /A2833	G2	E3 / O2 by RootKeyWrapKey or by AworWrapKey	N/A	S1, S3	Z1, Z2	Data encryption in conjuction with: LockingObjectDEK or NameSpaceDEK
WrapKey (AES-KW)	256	KTS /A2828	G2	E3 / O2 by RootKeyWrapKey or by AworWrapKey	N/A	S1	Z1, Z2	Key encryption of: LockingObjectDEK, NameSpaceDEK
$K_{FWModuleVerify}$ (Non-SSP)	150 128	RSA SigVer (FIPS186-4) / A2831	N/A	E2	N/A	S1	Z1	RSA 3072/4096 Public Key for the Module runtime firmware signature verification
$K_{FWControllerVerify}$	150 128	RSA SigVer (FIPS186-4) / A2831	N/A	E2	N/A	S1	Z1	RSA 3072/4096 Public Key used to authenticate the Controller.
$K_{AuthPub}$	150	RSA SigVer	N/A	E2 / O1	N/A	S1	Z1	RSA 3072/4096 Public Key used

Key/SSP/Name/Type	Strength	Security Function Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization	Use & Related keys
	128	(FIPS186-4) / A2831						to authenticate the Controller for factory-restricted hardware configuration services.
$K_{VSAuthPub}$	150 128	RSA-SigVer (FIPS186-4) / A2831	N/A	E2 / O1	N/A	S1	Z1	RSA 3072/4096 Public Key used to authenticate the Controller for factory restricted system configuration services
$K_{DeviceWrappingPub}$	150 128	KTS-IFC / A2829	N/A	E2 / O1	N/A	S1	Z1	RSA 3072/4096 Public Key for SUP Generate
$K_{ManifestPub\_ROM}$ (Non-SSP)	150 128	RSA SigVer (FIPS186-4) / A2831	N/A	N/A. Pre-installed.	N/A	S4	N/A. Used solely for self-tests and can be revoked	RSA 3072/4096 Public Key for manifest signature verification
$K_{FWCBootloaderVerify}$ (Non-SSP)	150 128	RSA SigVer (FIPS186-4) / A2831	N/A	E2	N/A	S1	Z1	RSA 3072/4096 Public Key for Bootloader firmware signature verification
UDS-KDK	384	KDF SP800-108 / A2832	G1	N/A	N/A	S2	Z2	UDS derivation
UDS (HMAC SHA2-384)	384	HMAC / A2830	G3 from UDS-KDK	N/A	N/A	S1	Z1	CDI calculation, which is used in attestations.
$K_{DeviceIDWrapKey}$ (AES-KW)	256	KTS /A2828	G3 from KDK	N/A	N/A	S1	Z1	Key encryption
$K_{DeviceIDPrivate}$	192	ECDSA SigGen / A2827 or A4269	G2	E3 / O2 by $K_{DeviceIDWrapKey}$	N/A	S1	Z1	Signature generation to validate Alias Certificate

Key/SSP/Name/Type	Strength	Security Function Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization	Use & Related keys
$K_{AliasPrivate}$	192	ECDSA SigGen / A2827 or A4269	G2	N/A	N/A	S1	Z1	Signature generation to validate system measurements
$K_{DeviceIDPublic}$	192	ECDSA SigVer / A2827 or A4269	G2	O1	N/A	S1	Z1	External Signature verification/authentication
$K_{AliasPublic}$	192	EC-DSA SigVer / A2827 or A4269	G2	O1	N/A	S1	Z1	External Signature verification/Authentication

9.2 DRBG Randomness Source

The DRBG Randomness source (i.e., entropy) is using an internal ENT (P) source conformant to [90B].

Table 12 – Non-Deterministic Random Number Generation Specification

Entropy Sources	Minimum number of bits of entropy	Details
ENT (P)	256-bits of entropy	Ring oscillator-based entropy source, which utilizes an AES-128 vetted conditioner and instantiates the AES-256 CTR-DRBG to a security strength of 256-bits.

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 both available on demand by resetting or power cycling the Module. All Conditional self-tests are performed before first use of the associated algorithm they are designed to test.
The self-tests error states and status indicator are described in Table 13 below:

Table 13 – Error States

State Name	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

State Name	Description	Indicator
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 (Please note the Function ROM v3.0 and Boot ROM v1.0 are implemented in non-reconfigurable-memory and are not subject to the firmware integrity test requirements per IG 5.A):

Table 14 – Pre-Operational Self-Test

Security Function	Method	Description	Error state
Bootloader Firmware integrity test	RSA PKCS#1_v1.5 /PSS SHA2-384 /SHA2-512	An RSA 3072 or 4096-bit Signature Verification is executed on the whole Bootloader copied into the Module using $K_{FWCBootloaderVerify}$	ES2
Runtime SCSS Firmware integrity test	RSA PKCS#1_v1.5 /PSS SHA2-384 /SHA2-512	An RSA 3072 or 4096-bit Signature Verification is executed on the whole Runtime SCSS firmware copied into the Module using $K_{FWModuleVerify}$	ES2

The Module performs the following conditional self-tests:

Table 15 – Conditional Self-Tests

Security Function	Method	Description	Error state
ROM SHS	KAT	SHA2-512 SHS KAT, which satisfies the self-test requirements for SHA2-384, SHA2-512, and SHA2-512/256.	ES1
ROM HMAC	KAT	HMAC SHA2-384 HMAC KAT	ES3
ROM RSA	KAT	3072 RSA PKCS#1_v1.5 Verification with SHA-384 KAT, which satisfies the self-test requirements for KTS-RSA per IG D.G; the Module only supports the public key operations for RSA Signature Verification and KTS-RSA Wrap This test occurs before the Pre-Operational firmware integrity test.	ES1
AES – KW	KAT	(Auxiliary) AES-256 KW Encrypt KAT – Inclusive of AES ECB testing with 256-bit key per IG 10.3.B	ES3
AES – KW	KAT	(Auxiliary) AES-256 Decrypt KAT – Inclusive of AES ECB testing with 256-bit key per IG 10.3.B	ES3
AES XTS – AUX and DPE	Comparative	256-bit AES-XTS encryption Comparative Answer Test with the AES-AUX and DPE AES-XTS implementations	ES3
AES XTS – AUX and DPE	Comparative	256-bit AES-XTS decryption Comparative Answer Test with the AES-AUX and DPE AES-XTS implementations	ES3
DRBG	KAT	AES-256 CTR_DRBG KAT SP800-90A Health Tests	ES3
Conditioner AES	KAT	SP800-90B Conditioning Component (AES-128)	ES3
KBKDF	KAT	Counter mode KBKDF KAT. Inclusive of HMAC-SHA2-384 KAT.	ES3

Security Function	Method	Description	Error state
ENT (P) Startup and Health tests	APT and RCT	ENT (P) SP800-90B APT and RCT.	ES3
PBKDF	KAT	Option 1a using HMAC SHA2-512/256	ES3
BootLoader Firmware Load test	RSA PKCS#1_v1.5 /PSS SHA2-384 /SHA2-512 Signature Verification	A 3072 or 4096-bit RSA Signature Verification is executed on the bootloader copied into the Module	ES2
Runtime SCSS Firmware Load test	RSA PKCS#1_v1.5 /PSS SHA2-384 /SHA2-512 Signature Verification	A 3072 or 4096-bit RSA Signature Verification is executed on the Runtime SCSS firmware copied into the Module	ES2
EC-DSA Key generation	EC-DSA Sign/Verify Pairwise Consistency Test	A pairwise consistency check is performed on EC-DSA private/public key on generation	ES3
EC-DSA Signature generation/Verification	KAT	P-384 Signature Generation/Verification KAT with SHA-384	ES3

11 Life-Cycle Assurance

This section documents the operational behavior of the Module.

11.1 Operational Behavior of the Device

1. The Module clears previous authentications on power cycle.
2. Data output is inhibited during key generation, firmware loading, self-tests, zeroization, and error states.
3. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
4. The Module zeroizes temporary values generated and used during self-tests.
5. The Module does not support a maintenance interface or role.
6. The Module does not support manual key entry.
7. The Module does not provide access to internal data structures.

11.2 Security Initialization

The device is shipped from the factory in the Approved mode of operation. The keys generated during manufacturing are used to encrypt/decrypt data. 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 16 – 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, October 7, 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*
[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*

Abbreviation	Full Specification Name
[TCG-SIIS]	*TCG Storage Interface Interactions Specification*

Table 17 – Acronyms and Definitions

Acronym	Definition
KAT	Known Answer Test
SSP	Sensitive Security Parameter
AK	Authentication key
DEK	Data Encryption Key
LBA	Logical Block Address
SED	Self-Encrypting Drive
SID	Security ID, PIN for Drive Owner CO Role – TCG OPAL
TCG	Trusted Computing Group