

Micron Technology, Inc.

Micron® MTC22-P4 Controller Sub Chip Security Subsystem

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 0.5

Date: 06/12/2025

Table of Contents

1 – General	5
1.1 Overview	5
1.2 Security Levels	5
2 – Cryptographic Module Specification	6
2.1 Description	6
2.2 Tested and Vendor Affirmed Module Version and Identification	7
2.3 Excluded Components.....	8
2.4 Modes of Operation	8
2.5 Algorithms	8
2.6 Security Function Implementations	12
2.7 Algorithm Specific Information	14
2.8 RBG and Entropy	14
2.9 Key Generation.....	15
2.10 Key Establishment.....	15
2.11 Industry Protocols.....	16
3 Cryptographic Module Interfaces.....	17
3.1 Ports and Interfaces	17
4 Roles, Services, and Authentication.....	18
4.1 Authentication Methods	18
4.2 Roles	18
4.3 Approved Services	18
4.4 Non-Approved Services.....	27
4.5 External Software/Firmware Loaded.....	28
5 External Software/Firmware Loaded	29
5.1 Integrity Techniques	29
5.2 Initiate on Demand	29
6 Operational Environment.....	30
6.1 Operational Environment Type and Requirements	30
7 Physical Security.....	31
7.1 Mechanisms and Actions Required.....	31
8 Non-Invasive Security	32
8.1 Mitigation Techniques.....	32
9 Sensitive Security Parameters Management.....	33
9.1 Storage Areas	33

9.2 SSP Input-Output Methods	33
9.3 SSP Zeroization Methods	34
9.4 SSPs	35
10 Self-Tests	46
10.1 Pre-Operational Self-Tests	46
10.2 Conditional Self-Tests	46
10.3 Periodic Self-Test Information	49
10.4 Error States	51
10.5 Operator Initiation of Self-Tests	52
11 Life-Cycle Assurance	53
11.1 Installation, Initialization, and Startup Procedures	53
11.2 Administrator Guidance	53
11.3 Non-Administrator Guidance	54
11.4 Design and Rules	54
12 Mitigation of Other Attacks	55
References and Definitions	56

List of Tables

Table 1: Security Levels	5
Table 2: Tested Module Identification – Hardware	8
Table 3: Modes List and Description	8
Table 4: Approved Algorithms	11
Table 5: Vendor-Affirmed Algorithms	11
Table 6: Security Function Implementations.....	14
Table 7: Entropy Certificates	14
Table 8: Entropy Sources.....	15
Table 9: Ports and Interfaces	17
Table 10: Authentication Methods.....	18
Table 11: Roles.....	18
Table 12: Approved Services	27
Table 13: Mechanisms and Actions Required	31
Table 14: Storage Areas	33
Table 15: SSP Input-Output Methods.....	33
Table 16: SSP Zeroization Methods.....	34
Table 17: SSP Table 1	39
Table 18: SSP Table 2	45
Table 19: Pre-Operational Self-Tests	46
Table 20: Conditional Self-Tests	49
Table 21: Pre-Operational Periodic Information.....	49
Table 22: Conditional Periodic Information.....	51
Table 23: Error States	51
Table 24: References.....	57
Table 25: Acronyms and Definitions	58

List of Figures

Figure 1 – Cryptographic Boundary (red) and TOEPP	7
Figure 2 – Physical Perimeter / boundary.....	7
Figure 3 – Tamper Evidence	31

1 – General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version MTC22-P4 of the Micron Technology, Inc. Micron® SSD Controller Sub Chip Security Subsystem. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 2 module.

1.2 Security Levels

The FIPS 140-3 security levels for the Module are as follows from Table 1:

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

2 – Cryptographic Module Specification

This Micron® MTC22-P4 Controller Sub Chip Security Subsystem module, hereafter denoted as the Module is a Single-Chip Hardware sub-chip cryptographic subsystem, as defined in FIPS 140-3 Implementation Guidance 2.3.B.

2.1 Description

Purpose and Use:

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated SSD Controllers. The Module is intended to be used in a SSD system.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics: SubChip

Cryptographic Boundary:

The physical form of the Module is depicted in Figure 2. The Module is a single chip embodiment. The cryptographic boundary is the logical cryptographic boundary of the module as defined by the Security Subsystem and includes all cryptographic algorithm implementations. The physical cryptographic boundary is the Micron® MTC22-P4 ASIC and includes its package. The cryptographic boundary is depicted by the red outline line in Figure 1.

Tested Operational Environment's Physical Perimeter (TOEPP):

The Tested Operational Environment's Physical Perimeter is the physical boundary of the module which is the Micron® MTC22-P4 ASIC package.



Figure 1 – Cryptographic Boundary (red) and TOEPP



Figure 2 – Physical Perimeter / boundary

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

The cryptographic module is tested on the following operational environment:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Micron® MTC22-P4 Controller Sub Chip Security Subsystem	0x20201112	Function ROM v3.0 Boot ROM v1.0 Bootloader V2.0 Runtime SCCS v3.0	Micron® MTC-22 P4	NVMe interface at the physical boundary

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

No components were excluded from the cryptographic boundary.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
NMO	Normal mode of operation. This is the only Approved mode of operation supported by the module	Approved	fipsApprovedMode: 1

Table 3: Modes List and Description

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.

The Module provides services to support NVMe industry standard commands as well as TCG commands. The Module provides these services to support the deployment of devices which support the TCG mode of operation but is not responsible for TCG management functions.

2.5 Algorithms

Approved Algorithms:

The Module implements the Approved cryptographic algorithms listed the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CTR, AES-ECB	C1278	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A5543, A5545	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-KW	A5550	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 256 Payload Length - Payload Length: 256-4096 Increment 64	SP 800-38F
AES-XTS Testing Revision 2.0	A5543, A5545	Direction - Decrypt, Encrypt Key Length - 256 Payload Length - Payload Length: 4096-32896 Increment 128 Tweak Mode - Number Data Unit Length Matches Payload Length - Yes	SP 800-38E
Conditioning Component Block Cipher Derivation Function SP800-90B	A2272	Key Length - 128 Payload Length - Payload Length: 512	SP 800-90B
Counter DRBG	C1278	Prediction Resistance - No, Yes Supports Reseed - Yes Mode - AES-128, AES-256 Derivation Function Enabled - No Additional Input - Additional Input: 0-256, Additional Input: 0-384 Entropy Input - Entropy Input: 256, Entropy Input: 384 Nonce - Nonce: 0 Personalization String Length - Personalization String Length: 0-256, Personalization String Length: 0-384 Returned Bits - 512	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A5551	Curve - P-384 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A5551	Curve - P-384	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A5551	Curve - P-384 Hash Algorithm - SHA2-384 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A5551	Component - No Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
HMAC-SHA2-384	A5548	MAC - MAC: 384 Key Length - Key Length: 384	FIPS 198-1
HMAC-SHA2-512	A5548	MAC - MAC: 512 Key Length - Key Length: 512	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-512/256	A5548	MAC - MAC: 256 Key Length - Key Length: 256	FIPS 198-1
KDF SP800-108	A5546	KDF Mode - Counter MAC Mode - HMAC-SHA2-384, HMAC-SHA2-512/256 Supported Lengths - Supported Lengths: 384 Fixed Data Order - Before Fixed Data Counter Length - 8 Supports Empty IV - No Requires Empty IV - No Custom Key In Length - 0	SP 800-108 Rev. 1
KTS-IFC	A5549	Function - partialVal IUT ID - 6500 Modulo - 3072, 4096 Key Generation Methods - rsakpg1-basic Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - initiator Key Transport Method - Hash Algorithms - SHA2-384 Supports Null Associated Data - Yes Associated Data Pattern - uPartyInfo vPartyInfo Associated Data Encoding - concatenation Key Length - 256	SP 800-56B Rev. 2
PBKDF	A5552	Iteration Count - Iteration Count: 100-1000 Increment 1 HMAC Algorithm - SHA2-512/256 Password Length - Password Length: 8-32 Increment 1 Salt Length - Salt Length: 128-3952 Increment 8 Key Data Length - Key Data Length: 256	SP 800-132
RSA SigVer (FIPS186-5)	A5547	Hash Pair - Hash Algorithm - SHA2-384 Modulo - 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1 Fixed Public Exponent - 010001 Public Exponent Mode - fixed	FIPS 186-5
SHA2-384	A5544	Message Length - Message Length: 384, 8-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-512	A5544	Message Length - Message Length: 512, 8-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4
SHA2-512/256	A5544	Message Length - Message Length: 256, 8-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

The Module implements the FIPS Vendor Affirmed cryptographic algorithms listed.

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric and Symmetric	N/A	SP800-133rev2 Section 4 example 1 and IG D.H
CKG-Combined	Key Type:Symmetric Key Generation for AES-XTS usage	N/A	SP 800-133rev2 Section 6.3 example #1 and IG C.I

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
KTS1	KTS-Unwrap KTS-Wrap	Key Transport Wrapping	IG D.G: Approved Key Wrapping Caveat:Key establishment methodology provides 256 bits of encryption strength	AES-KW: (A5550)
KTS2	KTS-Encap	Key Transport Encapsulation	IG:D.G Key confirmation:No Caveat:Caveat: Key establishment methodology provides between 128 and 150 bits of encryption strength	KTS-IFC: (A5549)
RNG	DRBG	DRBG		Counter DRBG: (C1278) AES-CTR: (C1278) AES-ECB: (C1278)
ENT	ENT-Cond ENT-ESV	Entropy Source		Conditioning Component Block Cipher Derivation Function SP800-90B: (A2272) Counter DRBG: (C1278) AES-CTR: (C1278) AES-ECB: (C1278)
SHS	SHA	Message hashing		SHA2-384: (A5544) SHA2-512: (A5544) SHA2-512/256: (A5544)
HMAC	MAC	Message authentication code generation		HMAC-SHA2-384: (A5548) HMAC-SHA2-512: (A5548) HMAC-SHA2-

Name	Type	Description	Properties	Algorithms
				512/256: (A5548)
DPE	BC-UnAuth	User Data encryption		AES-ECB: (A5543) AES-XTS Testing Revision 2.0: (A5543, A5545)
DPD	BC-UnAuth	User Data decryption		AES-ECB: (A5543) AES-XTS Testing Revision 2.0: (A5543, A5545)
KDF	KBKDF	Key-Based Key Derivation		KDF SP800-108: (A5546) HMAC-SHA2-384: (A5548) HMAC-SHA2-512: (A5548) HMAC-SHA2-512/256: (A5548)
PBKDF	PBKDF	Password Based Key Derivation		PBKDF: (A5552)
RSASigVer	DigSig-SigVer	Signature verification		RSA SigVer (FIPS186-5): (A5547)
ECDSASigVer	DigSig-SigVer	Signature verification		ECDSA SigVer (FIPS186-5): (A5551)
ECDSASigGen	DigSig-SigGen	Signature generation		ECDSA SigGen (FIPS186-5): (A5551)
ECDSA-KeyGen	AsymKeyPair-KeyGen AsymKeyPair-KeyVer	Key generation		ECDSA KeyGen (FIPS186-5): (A5551) ECDSA KeyVer (FIPS186-5): (A5551) CKG: () Key Type: Asymmetric and Symmetric
CKG	CKG	AES-256 Symmetric Key Generation from		AES-ECB: (A5545) CKG: ()

Name	Type	Description	Properties	Algorithms
		the direct output of the DRBG		Key Type: Asymmetric and Symmetric
CKG - Combined	CKG	AES-256 Symmetric Key Generation combining 2 or more keys		AES-XTS Testing Revision 2.0: (A5543) CKG- Combined: () AES 256: Symmetric Key Generation for AES-XTS usage

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

AES-XTS:

The module complies with FIPS 140-3 IG C.I by:

- AES-XTS is only used for storage purposes.
- The XTS algorithm implementation includes a check to ensure Key_1 ≠ Key_2. Per IG C.I
- AES-XTS Key_1 and Key_2 are generated independently according to the rules for component symmetric keys from NIST SP 800-133rev2, Sec. 6.3, for an approved use of AES-XTS.

PBKDF:

- Keys derived from passwords may only be used in storage applications.
- Per Option 2a, derived keys are used as input to AES-KW to wrap and unwrap sensitive data.
- Password length and format are specified in the SSP table and are 32 bytes long. Use of the derived password in the associated unwrap process is limited to five (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.

2.8 RBG and Entropy

Cert Number	Vendor Name
E168	Micron Technology, Inc.

Table 7: Entropy Certificates

The Module uses the following entropy source.

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Micron ® MTC22-P4 SSD Controller Sub Chip Security Subsystem ENT	Physical	MTC22-P4 SSD Controller	128 bit	Full entropy	A2272 (BlockCipher_DF)

Table 8: Entropy Sources

2.9 Key Generation

The module generates RSA and ECDSA asymmetric key pairs compliant with FIPS 186-5, using a NIST SP 800-90Arev1 CTR_DRBG for random number generation.

The module implements Cryptographic Key Generation (CKG, vendor affirmed), compliant with SP 800-133r2. When random values are required, they are obtained from the SP 800-90Ar1 approved DRBG, compliant with Section 4 of SP 800-133r2. The following methods are implemented:

- Direct generation of symmetric keys: compliant with SP 800-133rev2, Section 6.1.
- Symmetric Keys Produced by Combining (Multiple) Keys: Compliant with SP 800-133rev2, Section 6.3.
- RSA and ECDSA key pair generation: compliant with SP 800-133rev2, Section 5.1, which maps to FIPS 186-5.
- RSA key pair generation (KTS-IFC): compliant with SP 800-133rev2, Section 5.2, which maps to FIPS 186-5.

Additionally, the module implements the following key derivation methods:

- KDF SP800-108: compliant with section 4.1 “KDF in Counter Mode” of SP 800-108rev1.
- PBKDF: compliant with Section 5.4 “Option 1a” of SP800-132

2.10 Key Establishment

Key Agreement Information

N/A – The module does not perform Key Agreement.

Key Transport Information

- The module implements a KTS in conformance with NIST SP 800-56Vr2 using KTS-OAEP-BASIC (Cert. #A5549)
- The module implements KTS versions using AES-KW in conformance with SP800-38F and IG D.G. (Cert. #5550)

2.11 Industry Protocols

The module does not implement any Industry Protocols

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The Module's ports and associated FIPS defined logical interface categories are listed below.

Physical Port	Logical Interface(s)	Data That Passes
AESE (encryption engine)	Data Input Data Output Control Input Status Output	User Data
AESD (encryption engine)	Data Input Data Output Control Input Status Output	User Data
Mbox (Mailbox)	Control Input Status Output	Service info input
Controller output (response to Mbox)	Data Output	Service info output
Reset/Interrupt	Control Input	None
BMG-128 (S-DMA Interface)	Data Input Data Output	Service info data (command/response)
Power	Power	None
LDPC Decoder	Data Input	Firmware Images
UART	Status Output	Status Data

Table 9: Ports and Interfaces

The module does not provide control output.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The Module's authentication methods are listed in the table below.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Controller authentication	The User role is authenticated to the msg in interface with cryptographic signature generation	RSASVer	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 $1/2^{128}$. This effectively eliminates the possibility of determining the private key through exhaustive methods.	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. This results in a probability of $5/2^{128}$ that multiple attempts in a given minute of time is successful.

Table 10: Authentication Methods

4.2 Roles

The Module supports one distinct operator role, the Controller (Cryptographic Officer). One authentication is allowed per Module reset.

The Roles Table below lists all operator roles supported by the Module.

The Module does not support concurrent operators. Authentications are cleared on module reset.

Name	Type	Operator Type	Authentication Methods
Controller	Role	CO	Controller authentication

Table 11: Roles

4.3 Approved Services

All approved services implemented by the Module are listed in the table below:

In addition to the services listed, 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 describe these “factory-restricted” services and requires a second signature verification.

The SSPs modes of access shown in the table below 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 (SSP is input).
- E = Execute: The Module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The Module zeroizes the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Module Self-Test	Run KAT tests on all cryptographic algorithms and firmware integrity test	CCS	Power	Pass/Fail status	KTS1 KTS2 RNG ENT SHS HMAC DPE DPD KDF PBKDF RSASigVer ECDSASigVer ECDSASigGen ECDSA-KeyGen CKG CKG - Combined	Controller
Get Status	Get information about the operational state of the drive This includes Module identifier, hardware and firmware	CCS	Command	Command response with module status information	None	Controller

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	revision values.					
TCG Authenticate	Unwrap TCG SSP using PBKDF derived key	CCS	Password	Pass/Fail Status	KTS1 KDF PBKDF CKG	Controller - Password: E - SumRdsKey: W - RdsKey: W - PasswordWrapKey: G,E,Z - AuthenticatedUseHmacKey: E - EphemeralSumRdsKeyWrapKey: E
Clear TCG Authentications	Remove status of all past authentication and their privileges	CCS	End Session	Pass/Fail Status	None	Controller
NVMe Allocate and associate Key	Generate a key, wrap key and associate key with an entity	CCS	Access control list	Pass/Fail Status	KTS1 RNG CKG	Controller - SumRdsKey: G,E,R - RdsKey: G,E,R - DRBG-State: E - WrapKey: E - NamespaceDEK: G,R - AuthenticatedUseHmacKey: E - EphemeralSumRdsKeyWrapKey: E
NVMe Deallocate and disassociate Key	Zeroize key and disassociate key from an entity	CCS	Access control list	Pass/Fail Status	KTS1 DPE	Controller - WrapKey: E - NamespaceDEK: Z - AuthenticatedUseHmacKey: E
NVMe Update Key	Erase user data in a namespace by changing the	CCS	Access control list	Pass/Fail Status	KTS1 RNG CKG	Controller - SumRdsKey: W,E - RdsKey: E - DRBG-State: E - WrapKey: E - NamespaceDEK:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	encryption key					G,R,Z - LockingObjectDEK: G,R,Z - AuthenticatedUseHmacKey: E - EphemeralSumRdskWrapKey: E
Public HMAC Generation	Generate an HMAC over the prescribed content	CCS	Content	Mac of content	HMAC	Controller - RootPublicMacKey: E - PspHmacKey: E
Load Range and Key	Load DEK into DPE for indicated range	CCS	Range and Keyinfo	Status Indicator	KTS1	Controller - SumRdsKey: W,E - RdsKey: E - TweakKey: W - WrapKey: E - NamespaceDEK: W - LockingObjectDEK: W - EphemeralSumRdskWrapKey: E
AWOR	Save, restore security operational context	CCS	Content pointer	Status Indicator	KTS1 HMAC KDF CKG CKG - Combined	Controller - SumRdsKey: W,R - RdsKey: W,R - TweakKey: W,R - PspHmacKey: W,R - RootHmacKey: E - RootKeyWrapKey: G,E - RootPublicMacKey: E - EphemeralSumRdskWrapKey: W,R
TCG Allocate and associate Key	Generate a key, wrap key and associate	CCS	Access control list	Status Indicator	KTS1 RNG CKG	Controller - SumRdsKey: G,E,R - RdsKey: G,E,R - DRBG-State: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	key with an entity					- WrapKey: E - LockingObjectDEK: G,R - AuthenticatedUseHmacKey: E - EphemeralSumRdsK WrapKey: E
TCG Deallocate and disassociate Key	Zeroize key and disassociate key from an entity	CCS	Access control list	Status Indicator	KTS1	Controller - WrapKey: E - LockingObjectDEK: Z,R - AuthenticatedUseHmacKey: E
TCG Update Key	Erase user data in a namespace by changing the encryption key	CCS	Access control list	Status Indicator	KTS1 RNG CKG	Controller - SumRdsKey: W,E - RdsKey: E - DRBG-State: E - WrapKey: E - LockingObjectDEK: G,R,Z - AuthenticatedUseHmacKey: E - EphemeralSumRdsK WrapKey: E
TCG Set PIN	Set PIN which is used in generating a key to wrap a TCG credential	CCS	Password and password length	Status indicator	KTS1 RNG HMAC KDF PBKDF CKG	Controller - SumRdsKey: W,G - RdsKey: W,G - DRBG-State: E - WrapKey: E - Password: W,E,Z - PasswordWrapKey: G,E,Z - AuthenticatedUseHmacKey: E - EphemeralSumRdsK WrapKey: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TCG Revert, Activate, Reactivate	Revert to FOB, Revert to FOB with TCG Activated	CCS	Access control list	Status Indicator	KTS1 RNG HMAC CKG	Controller - SumRdsKey: Z - RdsKey: Z - WrapKey: E - DRBG-State: E - NamespaceDEK: G,Z - RootHmacKey: E - LockingObjectDEK: G,Z - AuthenticatedUseHmacKey: E
CSP Load	Restore Persistent CSP	CCS	CSP List	Status Indicator	KTS1 HMAC	Controller - RootHmacKey: E - RootKeyWrapKey: E - WrapKey: W - DRBG-State: E - TweakKey: W - PspHmacKey: W
Generate KeyDerivationKey	Generate a new KeyDerivationKey	CCS	Value	Status Indicator	KDF CKG	Controller - RootHmacKey: G,E - RootKeyWrapKey: G,E - RootPublicMacKey: G - WrapKey: G,E - KeyDerivationKey: G,E - Entropy Input and Seed: E - DRBG-State: G,E - TweakKey: G - PspHmacKey: G - AuthenticatedUseHmacKey: G,E - EphemeralSumRdsKeyWrapKey: G,E
Attestation	Device cryptographic identity	CCS	Index	Status Indicator	KTS1 RNG SHS	Controller - KDeviceIDPrivate: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	and attestation				ECDSASigVer ECDSASigGen ECDSA-KeyGen CKG - Combined	- KDeviceIDPublic: G - KAliasPrivate: G,E - KAliasPublic: G - KDeviceIDWrapKey: G,E,Z - DRBG-State: E - UDS: G,E,Z
User Write/Read	Encryption / Decryption of user data to / from a user data range	CCS	Data packet	Data Packet	DPE DPD	Controller - NamespaceDEK: E - LockingObjectDEK: E - TweakKey: E
SUP Generate	KTS-RSA wrap an internally generated random	CCS	None	Encrypted password context Status	KTS1 KTS2 RNG KDF PBKDF CKG	Controller - KDeviceWrappingPub: E - PasswordWrapKey: G,E,Z - SUP Seed: G,R - DRBG-State: E
SUP Authenticate	Unwrap SUP blob using KBKDF derived key	CCS	Password	Authentication result	KTS1 KDF PBKDF	Controller - PasswordWrapKey: G,E - Password: W,E
Random	Returns a 256-bit random number	CCS	Size	DRBG output	RNG	Controller - DRBG-State: E
Zeroize	Destroys all keys. Must be performed under the direct control of the operator	CCS	None	None	None	Controller - AuthenticatedUseHmacKey: Z - DRBG-State: Z - EphemeralSumRdskWrapKey: Z - Entropy Input and Seed: Z - KeyDerivationKey: Z -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						LockingObjectDEK: Z - NamespaceDEK: Z - Password: Z - PasswordWrapKey: Z - PspHmacKey: Z - RdsKey: Z - RootHmacKey: Z - RootKeyWrapKey: Z - SumRdsKey: Z - SUP Seed: Z - TweakKey: Z - WrapKey: Z - KFWModuleVerify: Z - KFWControllerVerify: Z - KAuthPub: Z - KVSAuthPub: Z - KDeviceWrappingPub: Z - KManifestPub: Z - KFWCBootloaderVerify: Z - UDS: Z - KDeviceIDWrapKey: Z - KDeviceIDPrivate: Z - KAliasPrivate: Z - KDeviceIDPublic: Z - KAliasPublic: Z - RootPublicMacKey: Z
Module Deprovision	Deprovision the device, zeroize all SSPs	CCS	None	None	None	Controller - AuthenticatedUseHmacKey: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG-State: Z - EphemeralSumRdsKeyWrapKey: Z - Entropy Input and Seed: Z - LockingObjectDEK: Z - NamespaceDEK: Z - Password: Z - PasswordWrapKey: Z - PspHmacKey: Z - RdsKey: Z - RootHmacKey: Z - RootKeyWrapKey: Z - SumRdsKey: Z - SUP Seed: Z - TweakKey: Z - WrapKey: Z - KFWModuleVerify: Z - KFWControllerVerify: Z - KAuthPub: Z - KVSAuthPub: Z - KDeviceWrappingPub: Z - KManifestPub: Z - KFWCBootloaderVerify: Z - KDeviceIDWrapKey: Z - KDeviceIDPrivate: Z - KAliasPrivate: Z - KDeviceIDPublic: Z - KAliasPublic: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						RootPublicMacKey: Z
Factory Auth	Authentication for factory-restricted services	CCS	Authorization signature	Random Value	RNG RSAVer	Controller - KAuthPub: E - KVSAuthPub: E - DRBG-State: E
Firmware Signature Check	Verify firmware image signature	CCS	Firmware Image Location	Status	RSASVer	Controller - KFWModuleVerify: E - KFWControllerVerify: E - KFWCBootloaderVerify: E
Manifest Load	Verify and load trusted set of PKS	CCS	Manifest Location	Status	RSASVer	Controller - KManifestPub_ROM: E - KManifestPub: E - KDeviceWrappingPub: R - KFWCBootloaderVerify: R - KFWModuleVerify: R - KVSAuthPub: R - KAuthPub: R - KFWControllerVerify: R

Table 12: Approved Services

4.4 Non-Approved Services

There are no Non-Approved services available.

N/A for this module.

4.5 External Software/Firmware Loaded

This module supports the loading of external firmware via the Program Update service. Execution of the successfully loaded firmware is only effective after the next reset of the security module. Any firmware loaded into the module other than that listed in Section 2.2 Tested and Vendor Affirmed Module Version and Identification, is outside the scope of this Security Policy and requires a separate FIPS 140-3 validation.

The module validates the integrity of the externally loaded firmware via procedures described in section 5.1 Integrity Techniques

5 External Software/Firmware Loaded

External firmware is loaded during the boot process. The firmware is validated using an RSA 3072 or 4096-bit signature verification after the image is copied into the module. It shall only be executed if the signature verification passes. Otherwise, it is removed from the module's Software/Firmware Security. The Module includes a firmware load service to support boot and any 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.

5.1 Integrity Techniques

The Module contains the following firmware component(s):

- Component 1: non reconfigurable Masked ROM per IG 5.A
- Component 2: limited bootloader - binary
- Component 3: limited run time firmware - binary

The firmware components are protected with one of the following authentication techniques described in Section 10.1.

- RSA 3072/4096 PKCS1_v1.5 (SHA2-384/SHA2-512)
- RSA 3072/4096 PKCS1_PSS (SHA2-384/SHA2-512)

Please note the module ROM is implemented in non-reconfigurable memory and is not subject to the firmware integrity test requirements per IG 5.A.

5.2 Initiate on Demand

The integrity test is performed as part of the Pre-Operational Self-Tests. It is automatically executed at power-on. The operator can initiate the integrity test on demand by resetting the device.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

The Module has a limited operational environment under the FIPS 140-3 definitions therefore this section is N/A.

7 Physical Security

7.1 Mechanisms and Actions Required

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

Mechanism	Inspection Frequency	Inspection Guidance
IC packaging	On initial receipt of the device and yearly 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.

Table 13: Mechanisms and Actions Required

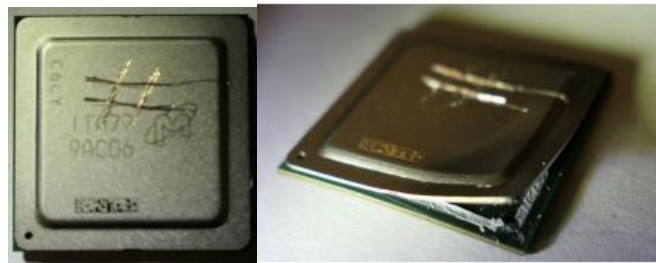


Figure 3 – Tamper Evidence

8 Non-Invasive Security

8.1 Mitigation Techniques

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

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Sub Chip security sub system RAM (S1)	Stored in volatile memory (RAM).	Dynamic
Sub Chip security sub system e-Fuse (S2)	Stored in e-fuse in Plaintext	Static
Sub Chip security sub system register (S3)	Stored in register in Plaintext	Dynamic

Table 14: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input in Plaintext(IO1)	Outside the module boundary in ASIC Internal SRAM	Sub Chip security sub system RAM (S1)	Plaintext	Automated	Electronic	
Input using SP800-38F AES key Transport (IO2)	Outside the module boundary in ASIC Internal SRAM	Sub Chip security sub system RAM (S1)	Encrypted	Automated	Electronic	KTS1
Output using SP800-38F Key Transport (IO3)	Sub Chip security sub system RAM (S1)	Outside the module boundary in ASIC Internal SRAM	Encrypted	Automated	Electronic	KTS1
Output encapsulated by RSA (IO4)	Sub Chip security sub system RAM (S1)	Outside the module boundary in ASIC Internal SRAM	Encrypted	Automated	Electronic	KTS2

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Zeroized by Module power cycle or hard reset.	When module is reset, all data stored in volatile module memory (RAM) will be lost	Implicit
Z2	Zeroized by the zeroization service by overwriting with a fixed pattern of zeros.	Each SSP is overwritten with a fixed value of 1s or 0s	Explicit

Table 16: SSP Zeroization Methods

9.4 SSPs

All usage of these SSPs by the Module are described in the services detailed in Section 4.3

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AuthenticatedUseHmacKey	Integrity checking of TCG table data	256 - 256	HMAC Key - CSP	CKG		HMAC
DRBG-State	CTR_DRBG internal state: V (128 bits) and Key (AES 256)	256 - 256	N/A - CSP	RNG		HMAC ECDSA- KeyGen CKG CKG - Combined
EphemeralSumRdsWrapKey	Key wrap of: SumRdsKeys,	256 - 256	Transport Key - CSP	CKG		KTS1
Entropy Input and Seed	CTR_DRBG entropy input.	384 - N/A	N/A - CSP	ENT		RNG
KeyDerivationKey	Master key used to derive other keys	256 - 256	Key Derivation Key - CSP	CKG		KDF
LockingObjectDEK	User Data Encryption Key	256 - 256	Encryption Key - CSP	CKG		DPE DPD
NamespaceDEK	User Data Encryption Key	256 - 256	Encryption Key - CSP	CKG		DPE DPD
Password	Used with KDF to derive the PasswordWrapKey	256 - 256	Plaintext password - CSP			KDF
PasswordWrapKey	Derived using KDF and Password and used to wrap/unwrap credential.	256 - 256	Transport Key - CSP	KDF		KTS1 KTS2
PspHmacKey	Verify the integrity of public TCG content	256 - 256	HMAC Key - CSP	CKG		HMAC
RdsKey	CSP transport Key	256 - 256	Transport Key - CSP	CKG		KTS1

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
RootHmacKey	Integrity checking	256 - 256	HMAC Key - CSP	KDF		HMAC
RootKeyWrapKey	key-wrap using SP800-38F AES KTS persistent secret content stored outside of the boundary.	256 - 256	Transport Key - CSP	KDF		KTS1
RootPublicMacKey	Integrity checking of TCG content	256 - 256	HMAC Key - CSP	KDF		HMAC
SumRdsKey	CSP transport Key	256 - 256	Transport Key - CSP	CKG		KTS1
SUP Seed	Random value used to generate an internal password	256 - 256	Symmetric Key - CSP	CKG		KTS2
TweakKey	Data encryption in conjunction with: LockingObjectDEK or NamespaceDEK	256 - 256	Data Encryption Key - CSP	CKG		DPE DPD
WrapKey	Key encryption of: LockingObjectDEK, NamespaceDEK	256 - 256	Symmetric Key - CSP	CKG		KTS1
KFWModuleVerify	Module firmware verification key	Modulus: 3072/4096 - RSA: 150,128, RSA-PKCS-1.5, RSA-PSS	Signature verification - PSP			RSASVer
KFWControllerVerify	Controller signature verification Key	Modulus: 3072/4096 - RSA: 150,128, RSA-	Signature verification - PSP			RSASVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		PKCS-1.5, RSA-PSS				
KAuthPub	Key for Factory-restricted services signature verification	Modulus: 3072/4096 - RSA: 150,128, RSA-PKCS-1.5, RSA-PSS	Signature verification - PSP			RSASVer
KVSAAuthPub	Key for Factory-restricted signature verification for SEE module	Modulus: 3072/4096 - RSA: 150,128, RSA-PKCS-1.5, RSA-PSS	Signature verification - PSP			RSASVer
KDeviceWrappingPub	Public Key for SUP Generate	Modulus: 3072/4096 - RSA: 150,128, RSA-PKCS-1.5, RSA-PSS	Signature verification - PSP			KTS2
KManifestPub_ROM	Public Key for manifest signature verification	Modulus: 3072/4096 - RSA: 150,128, RSA-PKCS-	Signature verification - PSP	Input at Manufacturing		RSASVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		1.5, RSA-PSS				
KManifestPub	Public Key for manifest signature verification	Modulus: 3072/4096 - RSA: 150,128, RSA-PKCS-1.5, RSA-PSS	Signature verification - PSP	Input at Manufacturing		RSASigVer
KFWCBootloaderVerify	Key for bootloader firmware signature verification	Modulus: 3072/4096 - RSA: 150,128, RSA-PKCS-1.5, RSA-PSS	Signature verification - PSP			RSASigVer
UDS	Unique Device Secret. Used to generate CDI	384 - 256	Key Derivation - CSP	RNG		KDF
KDeviceIDWrapKey	key used for -wrapping the DeviceIDPrivate ECDSA key	256 - 256	Transport Key - CSP	KDF		KTS1
KDeviceIDPrivate	ECDSA signature generation to verify Alias Certificate	384 - 192	Asymmetric Signature Key - CSP	ECDSA-KeyGen		ECDSASigGen
KAliasPrivate	Signature generation to validate system measurements	384 - 192	Asymmetric Signature Key - CSP	ECDSA-KeyGen		ECDSASigGen
KDeviceIDPublic	External Signature verification/authentication	384 - 192	Asymmetric Signature	ECDSA-KeyGen		ECDSASigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
			Verification - PSP			
KAliasPublic	External Signature verification/Authentication	384 - 192	Asymmetric Signature Verification - PSP	ECDSA-KeyGen		ECDSASigVer

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AuthenticatedUseHmacKey		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	RootKeyWrapKey:Wraps using KTS1
DRBG-State		Sub Chip security sub system RAM (S1):Plaintext	Until reboot or reseed	Z1	Entropy Input and Seed:Derived From KeyDerivationKey:directly generated from Drbg-State LockingObjectDEK:directly generated from DrbgState NamespaceDEK:directly generated from DrbgState RdsKey:directly generated from DrbgState PspHmacKey:directly generated from DrbgState AuthenticatedUseHmacKey:directly generated from DrbgState SumRdsKey:directly generated from DrbgState SUP Seed:directly generated from DrbgState

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					TweakKey:directly generated from DrbgState WrapKey:directly generated from DrbgState
EphemeralSumRdsWrapKey	Input using SP800-38F AES key Transport (IO2) Output using SP800-38F Key Transport (IO3)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	SumRdsKey:used to wrap/unwrap SumRdsKeys DRBG-State:directly generated by the DRBG
Entropy Input and Seed		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	DRBG-State:Used With
KeyDerivationKey		Sub Chip security sub system e-Fuse (S2):Plaintext		Z2	RootHmacKey:Derived From RootKeyWrapKey:Derived From RootPublicMacKey:Derived From
LockingObjectDEK	Input using SP800-38F AES key Transport (IO2) Output using SP800-38F Key Transport (IO3)	Sub Chip security sub system RAM (S1):Plaintext Sub Chip security sub system register (S3):Plaintext	Until reboot	Z1 Z2	WrapKey:Wrapped by RdsKey:Wrapped by SumRdsKey:Wrapped by DRBG-State:directly generated by the DRBG TweakKey:Used to perform the Write/Read service
NamespaceDEK	Input in Plaintext(IO1)	Sub Chip security sub	Until reboot	Z1 Z2	WrapKey:Wrapped by RdsKey:Wrapped by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Input using SP800-38F AES key Transport (IO2) Output using SP800-38F Key Transport (IO3)	system RAM (S1):Plaintext Sub Chip security sub system register (S3):Plaintext			SumRdsKey:Wrapped by DRBG-State:directly generated by the DRBG TweakKey:Used to perform the Write/Read service
Password	Input in Plaintext(IO1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	PasswordWrapKey:used to generate using KDF
PasswordWrapKey		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	Password:Derived From RdsKey:Wraps this key SumRdsKey:Wraps this key
PspHmacKey	Input using SP800-38F AES key Transport (IO2) Output using SP800-38F Key Transport (IO3)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	RootKeyWrapKey:wrapped by using KTS1 DRBG-State:directly generated by the DRBG
RdsKey	Input in Plaintext(IO1) Input using SP800-38F AES key Transport (IO2)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	LockingObjectDEK:key-wraps this key NamespaceDEK:key-wraps this key PasswordWrapKey:Import/export by RootKeyWrapKey:Import/export by DRBG-State:directly generated by the DRBG

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Output using SP800-38F Key Transport (IO3)				
RootHmacKey		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KeyDerivationKey:Derived From
RootKeyWrapKey		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KeyDerivationKey:Derived From WrapKey:Wraps the SSP PspHmacKey:Wraps the SSP AuthenticatedUseHmacKey:Wraps the SSP TweakKey:Wraps the SSP RdsKey:Wraps the SSP
RootPublicMacKey		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KeyDerivationKey:Derived From
SumRdsKey	Input in Plaintext(IO1) Input using SP800-38F AES key Transport (IO2) Output using SP800-38F Key Transport (IO3)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	LockingObjectDEK:wrapped by SumRdsKey under certain conditions using KTS1 NamespaceDEK:wrapped by SumRdsKey under certain conditions using KTS1 DRBG-State:directly generated by the DRBG
SUP Seed	Output encapsulated by RSA (IO4)	Sub Chip security sub	Until reboot	Z1 Z2	KDeviceWrappingPub:Derived From DRBG-State:directly generated by the DRBG

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
		system RAM (S1):Plaintext			
TweakKey	Input using SP800-38F AES key Transport (IO2) Output using SP800-38F Key Transport (IO3)	Sub Chip security sub system RAM (S1):Plaintext Sub Chip security sub system register (S3):Plaintext	Until reboot	Z1 Z2	LockingObjectDEK:Used With NamespaceDEK:Used With DRBG-State:directly generated by the DRBG
WrapKey		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	LockingObjectDEK:Encrypts NamespaceDEK:Encrypts DRBG-State:directly generated by the DRBG RootKeyWrapKey:Wrapped by
KFWModuleVerify	Input in Plaintext(IO1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	
KFWControllerVerify	Input in Plaintext(IO1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KManifestPub:Used to establish trust by checking signature on Key Manifest
KAuthPub	Input in Plaintext(IO1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KManifestPub:Used to establish trust by checking signature on Key Manifest
KVSAuthPub	Input in Plaintext(IO1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KManifestPub:Used to establish trust by checking signature on Key Manifest

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
KDeviceWrappingPub	Input in Plaintext(IO1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	SUP Seed:Encrypts KManifestPub:Used to establish trust by checking signature on Key Manifest
KManifestPub_ROM	Input in Plaintext(IO1)	Sub Chip security sub system e-Fuse (S2):Plaintext	Until reboot	Z1 Z2	
KManifestPub	Input in Plaintext(IO1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KAuthPub:Verified as trusted by using MVK to verify signature of a Key Manifest KVSAuthPub:Verified as trusted by using MVK to verify signature of a Key Manifest KDeviceWrappingPub:Verified as trusted by using MVK to verify signature of a Key Manifest KFWCBootloaderVerify:Verified as trusted by using MVK to verify signature of a Key Manifest KFWControllerVerify:Verified as trusted by using MVK to verify signature of a Key Manifest
KFWCBootloaderVerify	Input in Plaintext(IO1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KManifestPub:Used to establish trust by checking signature on Key Manifest
UDS		Sub Chip security sub system e-Fuse (S2):Plaintext		Z2	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
KDeviceIDWrapKey		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	KeyDerivationKey:Derived From KDeviceIDWrapKey:After KDF, the key wraps the KDeviceIDPrivate
KDeviceIDPrivate		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	KDeviceIDWrapKey:Used to wrap/unwrap KDeviceIDPrivate KDeviceIDPublic:Used With
KAliasPrivate		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KAliasPublic:Used With
KDeviceIDPublic		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KDeviceIDPrivate:Used With
KAliasPublic		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KAliasPrivate:Used With

Table 18: SSP Table 2

10 Self-Tests

10.1 Pre-Operational 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 self-tests are available on demand by power cycling the Module.

The Module performs the following pre-operational self-tests in table below:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Bootloader Firmware integrity test	RSA SigVer PKCS1_v1.5 or PSS (FIPS186-5) (A5547)	KAT	SW/FW Integrity	Success or Failure Code	Executed on the whole firmware stored in the Module
Module run time firmware integrity test	RSA SigVer PKCS1_v1.5 or PSS (FIPS186-5) (A5547)	KAT	SW/FW Integrity	Success or Failure Code	Executed on the whole firmware stored in the Module

Table 19: Pre-Operational Self-Tests

Note that the module ROM is implemented in non-reconfigurable-memory and are not subject to the firmware integrity test requirements per IG 5.A:

10.2 Conditional Self-Tests

The Module performs the following conditional self-tests in the table below

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-KW (A5550) - Encrypt	AES-256	KAT	CAST	Success or Failure Code	(Auxiliary) AES-256 KW Encrypt KAT	At boot up
AES-KW (A5550) - Decrypt	AES-256	KAT	CAST	Success or Failure Code	(Auxiliary) AES-256 KW Decrypt KAT	At boot up
AES-XTS Testing Revision 2.0 - Encryption	AES-256	Comparison	CAST	Success or Failure Code	256-bit AES-XTS encryption KAT	At boot up
AES-XTS Testing Revision 2.0 - Decryption	AES-256	Comparison	CAST	Success or Failure Code	256-bit AES-XTS decryption KAT	At boot up
Conditioning Component Block Cipher Derivation Function SP800-90B (A2272)	AES 128	KAT	CAST	Success or Failure Code	SP800-90B Conditioning Component (AES-128)	At boot up
Counter DRBG (C1278)	Counter DRBG - AES 256	KAT	CAST	Success or Failure Code	AES-256 CTR_DRBG KAT SP800-90A Health Tests. Instantiate, Reseed, Generate as a full test	At boot up
ECDSA KeyGen (FIPS186-5) (A5551)	ECDSA P-384	PCT	PCT	Success or Failure Code	A pairwise consistency check is performed on ECDSA private/public key on	When a new ECDSA key pair is generated
ECDSA SigGen (FIPS186-5) (A5551)	ECDSA P-384	KAT	CAST	Success or Failure Code	P-384 Signature Generation KAT with SHA-384	At boot up
ECDSA SigVer (FIPS186-5) (A5551)	ECDSA P-384	KAT	CAST	Success or Failure Code	P-384 Signature Verification KAT with SHA-384	At boot up
HMAC-SHA2-384 (A5548)	HMAC SHA2-384	KAT	CAST	Success or Failure Code	HMAC SHA2-384 KAT performed prior to Firmware Integrity test	At boot up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-512 (A5548)	HMAC SHA2-512	KAT	CAST	Success or Failure Code	HMAC SHA2-512 KAT	At boot up
KDF SP800-108 (A5546)	HMAC-SHA2-384	KAT	CAST	Success or Failure Code	Counter mode KBKDF KAT. Inclusive of HMAC-SHA2-384 KAT.	At boot up
PBKDF (A5552)	HMAC SHA2-512/256	KAT	CAST	Success or Failure Code	Option 1a using HMAC SHA2-512/256	At boot up
RSA SigVer (FIPS186-5) (A5547)	3072 RSA PKCS#1_v1.5 Verification with SHA-384	KAT	CAST	Success or Failure Code	3072 RSA PKCS#1_v1.5 Verification with SHA-384 KAT the Module only supports the public key operation for RSA Signature Verification and KTS-RSA Wrap	At boot up before Pre-Operational firmware integrity test.
BootLoader Firmware Load test	RSA SigVer (FIPS186-5) (A5547)	KAT	SW/FW Load	Success or Failure Code	A 3072/ 4096-bit RSA or ECDSA P384 Signature Verification is executed on the bootloader copied into the Module	At boot up
Runtime Firmware Load test	RSA SigVer (FIPS186-5) (A5547)	KAT	SW/FW Load	Success or Failure Code	A 3072/ 4096-bit RSA or ECDSA P384 Signature Verification is executed on the SEE firmware copied into the Module	At boot up
XTS Duplicate Key		CT	Critical Function	Success or Failure Code	Duplicate Key Test	Upon generation of XTS key
Entropy 90B Start-up Repetition Count Test (RCT)	Repetition Count Test	Fault induction	CAST	Success or Failure Code	As specified in [90B] RCT startup health tests	At boot up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Entropy 90B Start-up Adaptive Proportion Test (APT)	Adaptive Proportion Test	Fault induction	CAST	Success or Failure Code	As specified in [90B] APT startup health tests	At boot up
Entropy 90B Continuous Repetition Count Test (RCT)	Repetition Count Test	Fault induction	CAST	Success or Failure Code	As specified in [90B] RCT continuous health tests	Continuous when entropy is requested
Entropy 90B Continuous Adaptive Proportion Test (APT)	Adaptive Proportion Test	Fault induction	CAST	Success or Failure Code	As specified in [90B] APT continuous health tests	Continuous when entropy is requested

Table 20: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Bootloader Firmware integrity test	KAT	SW/FW Integrity	On Demand	Device Reset
Module run time firmware integrity test	KAT	SW/FW Integrity	On Demand	Device Reset

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-KW (A5550) - Encrypt	KAT	CAST	On Demand	Device Reset
AES-KW (A5550) - Decrypt	KAT	CAST	On Demand	Device Reset
AES-XTS Testing Revision 2.0 - Encryption	Comparison	CAST	On Demand	Device Reset
AES-XTS Testing Revision 2.0 - Decryption	Comparison	CAST	On Demand	Device Reset
Conditioning Component Block Cipher Derivation Function SP800-90B (A2272)	KAT	CAST	On Demand	Device Reset
Counter DRBG (C1278)	KAT	CAST	On Demand	Device Reset
ECDSA KeyGen (FIPS186-5) (A5551)	PCT	PCT	N/A	N/A
ECDSA SigGen (FIPS186-5) (A5551)	KAT	CAST	On Demand	Device Reset
ECDSA SigVer (FIPS186-5) (A5551)	KAT	CAST	On Demand	Device Reset
HMAC-SHA2-384 (A5548)	KAT	CAST	On Demand	Device Reset
HMAC-SHA2-512 (A5548)	KAT	CAST	On Demand	Device Reset
KDF SP800-108 (A5546)	KAT	CAST	On Demand	Device Reset
PBKDF (A5552)	KAT	CAST	On Demand	Device Reset
RSA SigVer (FIPS186-5) (A5547)	KAT	CAST	On Demand	Device Reset
BootLoader Firmware Load test	KAT	SW/FW Load	On Demand	Device Reset
Runtime Firmware Load test	KAT	SW/FW Load	On Demand	Device Reset

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
XTS Duplicate Key	CT	Critical Function		
Entropy 90B Start-up Repetition Count Test (RCT)	Fault induction	CAST	On Demand	by power cycling the Module.
Entropy 90B Start-up Adaptive Proportion Test (APT)	Fault induction	CAST	On Demand	by power cycling the Module.
Entropy 90B Continuous Repetition Count Test (RCT)	Fault induction	CAST		
Entropy 90B Continuous Adaptive Proportion Test (APT)	Fault induction	CAST		

Table 22: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
ES1	The ROM fails a KAT	Triggered by cryptographic KAT failure.	Reboot/Power cycle the module	A Cryptographic Self-test Failure status is indicated in response to any service request.
ES2	The Module fails the firmware load test or the Firmware Integrity test	Firmware load and integrity check fails when the firmware fails to verify	Reboot/Power cycle the module	The Module enters the ES2 error state and outputs a verification failure status in response to the firmware service.
ES3	The Module fails conditional KAT self-test. Non-operational state. No services beside status services are allowed	Triggered by cryptographic KAT failure.	Reboot/Power cycle the module	The Module enters the ES3 error state and will output a self-test failure status to any service request

Table 23: Error States

10.5 Operator Initiation of Self-Tests

Self-tests can be initiated by the operator by resetting the module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Installation and 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.

Delivery:

On receipt of the Module, the CO should perform the following steps to ensure the integrity of the device before using the device.

1. Verify the product shipping packaging is intact and untampered.
2. Verify the product is FIPS validated as indicated in the product label.
3. Examine the module to ensure it has not been tampered with during shipping according to the procedures outlined in the module Security Policy.
4. Verify that the device indicates that it is a FIPS device and is in an Approved mode and state. This is accomplished by performing a Level 0 Discovery as defined by the TCG Core specification. The Level 0 Discovery Header Vendor specific bytes 22, 23 and 24 must contain:
 - a. FIPS Drive = 1,
 - b. FIPS Mode = 0x01,
 - c. FIPS State = 0x01.

Any other values indicate the Module is not operating in an Approved mode.

If physical or logical tampering with the device is detected or suspected the SSD should not be placed into use and returned to Micron for evaluation.

The SSD operates in an approved mode and contains the services necessary to support both NVMe and TCG concurrently. It is not necessary to activate Opal unless its features are desired.

11.2 Administrator Guidance

Micron Technology, Inc. provides the end user with the following documents:

1. Micron Technology Micron® MTC22-P4 based SSDs Drive Owner supplemental information

2. Micron Technical Note TN_FD-28: Installing Micron SEDs in Windows 8 and 10

11.3 Non-Administrator Guidance

N/A

11.4 Design and Rules

Rules of Operation

1. The Module provides one distinct operator role, the controller : (Cryptographic Officer).
2. The Module provides role-based authentication.
3. The Module clears previous authentications on power cycle.
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. All self-tests do not require any operator action.
7. Data output is inhibited during key generation, 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.
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 enter or output plaintext CSPs.
15. The Module does not output intermediate key values.
16. The Module does not provide bypass services for ports/interfaces.

12 Mitigation of Other Attacks

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

References and Definitions

The following standards are referred to in this Security Policy.

Abbreviation	Full Specification Name
[FIPS140-3]	<i>Security Requirements for Cryptographic Modules, March 22, 2019</i>
[ISO19790]	<i>International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017</i>
[ISO24759]	<i>International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015</i>
[IG]	<i>Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, October 23 2024</i>
[108]	<i>NIST Special Publication 800-108r1-upd1, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), August 2022</i>
[131A]	<i>Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 2, March 2019</i>
[132]	<i>NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, December 2010</i>
[133]	<i>NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020</i>
[186]	<i>National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-5, February 2023.</i>
[197]	<i>National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001, Updated May 9, 2023</i>

Abbreviation	Full Specification Name
[198]	<i>National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008</i>
[180]	<i>National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015</i>
[38A]	<i>National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001</i>
[38D]	<i>National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007</i>
[38E]	<i>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</i>
[38F]	<i>National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012</i>
[56Br2]	<i>NIST Special Publication 800-56B Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Finite Field Cryptography, March 2019</i>
[90A]	<i>National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.</i>
[90B]	<i>National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.</i>
[ACS-3]	<i>ACS-3 Reporting Security Compliance December 1,2009</i>
[TCG-SSC-Opal]	<i>TCG Storage Security Subsystem Class: Opal, Specification</i>
[TCG-SACS]	<i>TCG Storage Architecture Core Specification</i>

Table 24: References

Acronym	Definition
CCS	Command Completion Status
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
SSD	Solid State Drive
TCG	Trusted Computing Group

Table 25: Acronyms and Definitions