

Micron Technology, Inc.

Micron® MSA11-P5 Controller Sub Chip Security Subsystem

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 0.7

Date: 1/24/2025

Table of Contents

1 – General	4
1.1 Overview	4
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	13
2.7 Algorithm Specific Information	17
2.8 RBG and Entropy	17
2.9 Key Generation.....	17
2.10 Key Establishment.....	18
2.11 Industry Protocols.....	18
3 Cryptographic Module Interfaces.....	19
3.1 Ports and Interfaces	19
4 Roles, Services, and Authentication.....	20
4.1 Authentication Methods	20
4.2 Roles	20
4.3 Approved Services	22
4.4 Non-Approved Services.....	28
4.5 External Software/Firmware Loaded.....	29
5 Software/Firmware Security	30
5.1 Integrity Techniques	30
5.2 Initiate on Demand	30
6 Operational Environment.....	31
6.1 Operational Environment Type and Requirements	31
7 Physical Security.....	32
7.1 Mechanisms and Actions Required.....	32
8 Non-Invasive Security	33
8.1 Mitigation Techniques.....	33
9 Sensitive Security Parameters Management.....	34
9.1 Storage Areas	34

9.2 SSP Input-Output Methods	34
9.3 SSP Zeroization Methods	35
9.4 SSPs	36
10 Self-Tests	48
10.1 Pre-Operational Self-Tests	48
10.2 Conditional Self-Tests	48
10.3 Periodic Self-Test Information	52
10.4 Error States	54
10.5 Operator Initiation of Self-Tests	54
10.6 Additional Information	54
11 Life-Cycle Assurance	55
11.1 Installation, Initialization, and Startup Procedures	55
11.2 Administrator Guidance	56
11.3 Non-Administrator Guidance	56
11.4 Design and Rules	56
Rules of Operation	56
12 Mitigation of Other Attacks	58
References and Definitions	59

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.....	15
Table 7: Entropy Certificates	17
Table 8: Entropy Sources.....	17
Table 9: Ports and Interfaces	19
Table 10: Authentication Methods.....	20
Table 11: Roles.....	21
Table 12: Approved Services	28
Table 13: Mechanisms and Actions Required	32
Table 14: Storage Areas	34
Table 15: SSP Input-Output Methods.....	35
Table 16: SSP Zeroization Methods.....	35
Table 17: SSP Table 1	40
Table 18: SSP Table 2	47
Table 19: Pre-Operational Self-Tests	48
Table 20: Conditional Self-Tests	51
Table 21: Pre-Operational Periodic Information.....	52
Table 22: Conditional Periodic Information.....	53
Table 23: Error States	54
Table 24 – References.....	59
Table 25 – Acronyms and Definitions.....	61

List of Figures

Figure 1 – Cryptographic Boundary (red) and TOEPP	7
Figure 2 – Physical Perimeter / boundary (Top and Bottom View)	7
Figure 3 – – Tamper-Evident Example	32

1 – General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version MSA11-P5 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 the table below:

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® MSA11-P5 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 an 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 defined by the Security Subsystem and includes all cryptographic algorithm implementations. The physical cryptographic boundary (TOEPP) is the Micron® MSA11-P5 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® MSA11-P5 ASIC package.

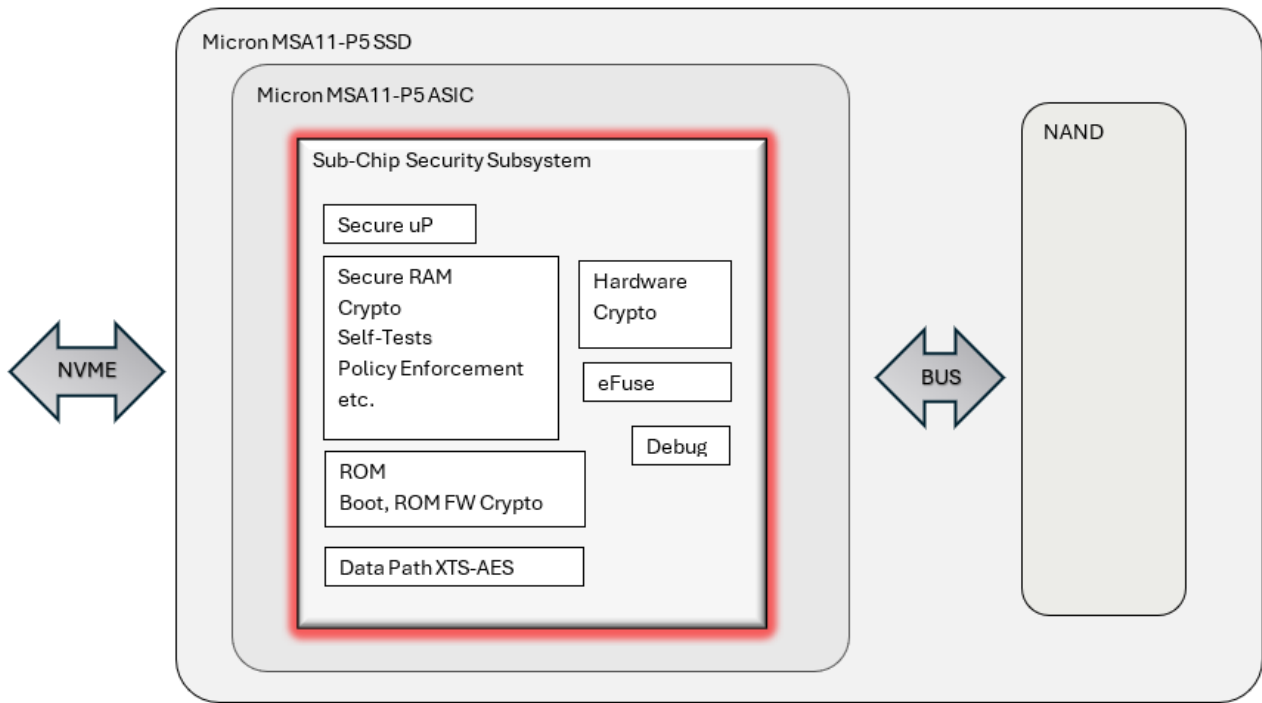


Figure 1 – Cryptographic Boundary (red) and TOEPP



Figure 2 – Physical Perimeter / boundary (Top and Bottom View)

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® MSA11-P5 Controller Sub Chip Security Subsystem	0x0C87E5	Function ROM v4.0, Bootloader V4.0, Runtime SCCS v4.2, 4.3, 4.4, 5.0	Micron® MSA11-P5	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	Type	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

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. A positive return status from the Get Status Service indicates the module is running in NMO mode.

The Module provides services to support NVME industry standard commands as well as TCG commands. The Module provides these services to support the deployment in 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 in the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	C1278	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A6144	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A6146	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	C1278	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	A6144	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 256-65536 Increment 128 AAD Length - AAD Length: 0	SP 800-38D
AES-KW	A6149	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	A6144	Direction - Decrypt, Encrypt Key Length - 256 Payload Length - Payload Length: 4096-32896 Increment 128 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
AES-XTS Testing Revision 2.0	A6146	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	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		Nonce - Nonce: 0 Personalization String Length - Personalization String Length: 0-256, Personalization String Length: 0-384 Returned Bits - 512	
ECDSA KeyGen (FIPS186-5)	A6142	Curve - P-384 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6142	Curve - P-384	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6142	Curve - P-384 Hash Algorithm - SHA2-384 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6142	Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
HMAC-SHA2-384	A6151	MAC - MAC: 384 Key Length - Key Length: 384	FIPS 198-1
HMAC-SHA2-512/256	A6151	MAC - MAC: 256 Key Length - Key Length: 256	FIPS 198-1
KDF SP800-108	A6148	KDF Mode - Counter MAC Mode - HMAC-SHA2-384, HMAC-SHA2-512/256 Supported Lengths - Supported Lengths: 256-384 Increment 128 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	A6150	IUT ID - 9550 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 - Associated Data Encoding - concatenation Key Length - 256	SP 800-56B Rev. 2
RSA SigVer (FIPS186-5)	A6147	Hash Pair - Hash Algorithm - SHA2-384 Modulo - 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
		Mask Function - mgf1 Fixed Public Exponent - 010001 Public Exponent Mode - fixed	
SHA2-384	A6143	Message Length - Message Length: 384, 8-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4
SHA2-384	A6145	Message Length - Message Length: 384, 8-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4
SHA2-512	A6145	Message Length - Message Length: 512, 8-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4
SHA2-512/256	A6145	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
CKG1	Key Type:Symmetric and Asymmetric	N/A	SP800-133rev2 Section 4 example 1 and IG D.H
CKG - XTS	AES 256:Symmetric Key Generation	N/A	SP 800-133rev2 Section 6.3 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: (A6149)
KTS2	KTS-Unwrap KTS-Wrap	Key Transport Wrapping	IG D.G:Approved Key Wrapping Caveat:Key establishment methodology provides 256 bits of encryption strength	AES-GCM: (A6144)
KTS3	KTS-Encap	Key Transport Encapsulation	IG D.G:Approved Key Encapsulation Key confirmation:No Caveat:Key transport methodology provides between 128 and 150 bits of encryption strength	KTS-IFC: (A6150)
GCME	BC-Auth	Authenticated message encryption		AES-GCM: (A6144) AES-ECB: (A6144)
GCMD	BC-Auth	Authenticated message decryption		AES-GCM: (A6144) AES-ECB: (A6144)
RNG	DRBG	DRBG		Counter DRBG: (C1278) AES-CTR: (C1278) AES-ECB: (C1278)

Name	Type	Description	Properties	Algorithms
ENT	ENT-Cond ENT-ESV	Entropy Source		Conditioning Component Block Cipher Derivation Function SP800-90B: (A2272)
SHS	SHA	Message hashing		SHA2-384: (A6143)
HMAC	MAC	Message authentication code generation		HMAC-SHA2-384: (A6151) HMAC-SHA2-512/256: (A6151) SHA2-384: (A6145) SHA2-512/256: (A6145)
DPE	BC-UnAuth	User Data encryption		AES-XTS Testing Revision 2.0: (A6146) AES-ECB: (A6146) CKG - XTS: () AES 256: Symmetric Key Generation
DPD	BC-UnAuth	User Data decryption		AES-XTS Testing Revision 2.0: (A6146) AES-ECB: (A6146) CKG - XTS: () AES 256: Symmetric Key Generation
AuxE	BC-UnAuth	User Data encryption		AES-XTS Testing Revision 2.0: (A6144) AES-ECB: (A6144) CKG - XTS: () AES 256: Symmetric Key Generation
AuxD	BC-UnAuth	User Data decryption		AES-XTS Testing Revision 2.0: (A6144) AES-ECB: (A6144) CKG - XTS: ()

Name	Type	Description	Properties	Algorithms
				AES 256: Symmetric Key Generation
KDF	KBKDF	Key-Based Key Derivation		KDF SP800-108: (A6148) HMAC-SHA2-384: (A6151) HMAC-SHA2-512/256: (A6151) SHA2-384: (A6145) SHA2-512/256: (A6145)
RSASigVer	DigSig-SigVer	Signature verification		RSA SigVer (FIPS186-5): (A6147) SHA2-384: (A6145) SHA2-512: (A6145)
ECDSASigVer	DigSig-SigVer	Signature verification		ECDSA SigVer (FIPS186-5): (A6142) SHA2-384: (A6143)
ECDSASigGen	DigSig-SigGen	Signature generation		ECDSA SigGen (FIPS186-5): (A6142) SHA2-384: (A6143)
ECDSA-KeyGen	AsymKeyPair-KeyGen AsymKeyPair-KeyVer	Key generation		ECDSA KeyVer (FIPS186-5): (A6142) ECDSA KeyGen (FIPS186-5): (A6142) CKG1: () Key Type: Symmetric and Asymmetric
CKG	CKG	AES-256 Symmetric Key Generation from the direct output of the DRBG		CKG1: () Key Type: Symmetric and Asymmetric Counter DRBG: (C1278)

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 $\neq$ 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.

AES GCM IV Uniqueness

IV uniqueness is guaranteed by use of the following mode deployed by the module:

FIPS140-3 IG C.H, Option 2

The IV is generated internally at its entirety randomly.

The generation uses an Approved DRBG (Cert. #[C1278](#)) that is internal to the module's boundary.

The IV length is fixed at 96 bits (per SP 800-38D).

2.8 RBG and Entropy

Cert Number	Vendor Name
E203	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® MSA11-P5 SSD Controller Sub Chip Security Subsystem ENT	Physical	MSA11-P5 SSD Controller	1 bit	Full entropy	A2272 (BlockCipher_DF)

Table 8: Entropy Sources

2.9 Key Generation

For Key Generation, see Section 2.5 and Section 2.6 above.

The output of the module's approved DRBGs may be used to generate symmetric and asymmetric keys per SP 800-133r2, as indicated in Security Policy Section 2.5.2 - Vendor-Affirmed Algorithms.

Symmetric keys are generated per SP 800-133r2 Section 6.1 using the UpdateDEK service; additionally, Section 6.3 is applicable for AES-XTS keys.

Asymmetric keys are generated for digital signatures per SP 800-133r2 sections 5.1 and per FIPS 186-5 using the Attestation service.

2.10 Key Establishment

Key Agreement Information

N/A: The module does not perform Key Agreement

Key Transport Information

For further details of Key Transport, see Section 2.5 and Section 2.6 above.

The module provides RSA key encapsulation that is conformant to SP 800-56Br2 via the SUP Generate service.

The module provides AES key wrapping/unwrapping (AES KW and AES-GCM) that is conformant to SP 800-38F via the CSP-Export and CSP-Import services.

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 (decryption engine)	Data Input Data Output Control Input Status Output	User Data
Data	Data Input Data Output	Module Service data
Mbox (Mailbox)	Data Input Data Output Control Input Status Output	Service info input/output
Service request notification interrupt	Control Input	None
Power	Power	None
Reset	Control Input	None

Table 9: Ports and Interfaces

The module does not provide control output

4 Roles, Services, and Authentication

4.1 Authentication Methods

Authentication occurs when a signed object is verified using the $K_{FWControllerVerify}$ public key. The public key variant (either RSA or ECDSA) is selected at build time. Images and key manifests are signed using the proper key. The manifest is loaded during pre-operational initialization and is verified using keys stored in ROM or eFuse. The $K_{FWControllerVerify}$ public key from the manifest will then be used to verify the signed authentication object.

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

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Controller authentication	This role is authenticated to the msg in interface with cryptographic signature generation	RSA SigVer and ECDSA SigVer	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 $1/2^{128}$. ECDSA P-384 has a key strength of 192 bits. The probability of a successful verification from a single random attempt is at least $1/2^{192}$. This effectively eliminates the possibility of determining the private key through exhaustive methods.	The strength per minute is $5/2^{128}$ for RSA and $5/2^{192}$ for ECDSA. This controls the number of unsuccessful attempts before authentication is blocked until a system restart occurs.

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 Authentication Methods table 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 require 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 KTS3 GCME GCMD RNG ENT SHS HMAC DPE DPD AuxE AuxD KDF RSASigVer ECDSASigVer ECDSASigGen CKG	Controller - DRBG-El and seed: E - DRBG-State: G Unauthenticated - DRBG-El and seed: E - DRBG-State: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get Status	Get information about the operational state of the drive This includes Module identifier, hardware and firmware revision values.	CCS	Command	Command response with module status information	None	Controller
KeyMgmt	Update and enforce authorization credential	CCS	Password and wrapped credentials	Status Indicator	KTS1 KDF CKG	Controller - AdminKey: G,R,W,E - AuthKDK: G,R,W,E - AuthKey: G,R,W,E - PrivateKey: G,R,W,E - RdsKey: R,W - TCGWrapKey: E
Load Range Attributes	Load DEK into DPE for indicated range	CCS	Range and Key Info	Status Indicator	KTS1	Controller - AuthKey: E - PrivateKey: W,E - AdminKey: W,E - TCGWrapKey: E - RdsKey: W,E - DEK: W
UpdateDEK	Generate Symmetric Module protected Key	CCS	Key Type	Status Indicator	KTS1 RNG CKG	Controller - AuthKey: E - AdminKey: W,E - PrivateKey: W,E - RdsKey: G,R,W,E - TCGWrapKey: E - DEK: G,R
CSP-Export	Export module protected CSPs	CCS	CSP List	CSP List	KTS1 RNG CKG KTS2	Controller - TCGWrapKey: R,E - TCGHMACKey: R - OpenHMACKey: R - AdminKey: R,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PrivateKey: R,W,E - RdsKey: R,W,E - DEK: R - AuthKDK: E - RootKeyWrapKey: R,E - RootMACKey: R,E - RootPublicMacKey: R - aworWrappingKey: E - KDeviceIDPrivate: R - KDKDK: R - fsaKey: G,R,E
CSP-Import	Import module protected CSPs	CCS	CSP List	CSP List	KTS1 KTS2	Controller - RootMACKey: W,E - RootKeyWrapKey: W,E - RootPublicMacKey: W - TCGWrapKey: W - TCGHMACKey: W - OpenHMACKey: W - KDeviceIDPrivate: W - aworWrappingKey: E - RdsKey: W - KDeviceIDPublic: W - fsaKey: W,E - KDKDK: W
User Write/Read	Encryption / Decryption of user data to / from a user data range	CCS	Data packet	Data Packet	DPE DPD	Controller - DEK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
SUP Generate	KTS-IFC wrap an internally generated random	CCS	None	Encrypted password context Status	KTS3 RNG KDF	Controller - AuthKDK: G,E - AuthKey: G,E - TCGWrapKey: E - KDeviceWrappingPub: E - SUP Seed: R
SUP Authenticate	Unwrap SUP blob using KBKDF derived key	CCS	Password	Authentication result	KDF	Controller - AuthKDK: E - AuthKey: E - TCGWrapKey: E
Random	Returns a 256-bit random number	CCS	Size	DRBG output	RNG	Controller - DRBG-State: G,E - DRBG-EI and seed: E
HMAC	Generate an HMAC over the prescribed content	CCS	Data location	Calculated HMAC	HMAC	Controller - OpenHMACKey: E - TCGHMACKey: E - RootPublicMacKey: E - aworHMACKey: E
Attestation	Device cryptographic identity and attestation	CCS	Index	Status Indicator	RNG SHS ECDSASigVer ECDSASigGen ECDSA- KeyGen	Controller - KDeviceIDPrivate: G,E - KDeviceIDPublic: G,R,E - KAliasPrivate: G,E - KAliasPublic: G,R,E - UDS: G,E,Z - DRBG-State: E
Zeroize	Destroys all keys. Must be performed	CCS	None	None	None	Controller - RootKDK: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	under the direct control of the operator					- RootMACKey: Z - RootPublicMacKey: Z - DRBG-El and seed: Z - DRBG-State: Z - TCGWrapKey: Z - TCGHMACKey: Z - OpenHMACKey: Z - Password: Z - AuthKDK: Z - AuthKey: Z - AdminKey: Z - PrivateKey: Z - RdsKey: Z - DEK: Z - SUP Seed: Z - CDI: Z - DeviceIDWrapKey: Z - KDeviceIDPrivate: Z - KAliasPrivate: Z - KDKDK: Z - KDataDecryption: Z - aworWrappingKey: Z - aworHMACKey: Z - KProduct: Z - KBootloader: Z - KFWModuleVerify: Z - KFWControllerVerify: Z - KAuthPub: Z - KDeviceWrappingPub:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - KManifestPub: Z - fsaKey: - RootKeyWrapKey: Z
Module Deprovision	Deprovision the device, zeroize all SSPs	CCS	None	None	None	Controller - RootKDK: Z - RootMACKey: Z - TCGWrapKey: Z - TCGHMACKey: Z - OpenHMACKey: Z - CDI: Z - DeviceIDWrapKey: Z - KDeviceIDPrivate: Z - KAliasPrivate: Z - KDeviceIDPublic: Z - KAliasPublic: Z - KDKDK: Z - KDataDecryption: Z - aworWrappingKey: Z - aworHMACKey: Z - KProduct: Z - KBootloader: Z - KFWModuleVerify: Z - KFWControllerVerify: Z Z - KAuthPub: Z - KDeviceWrappingPub: Z Z - KManifestPub: Z - RootKeyWrapKey: Z - RootPublicMacKey:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - UDS: Z
Factory Auth	Authentication for factory-restricted services	CCS	Authorization signature	Random Value	RNG RSAVer	Controller - KAuthPub: E
Firmware Signature Check	Verify firmware image signature	CCS	Firmware Image Location	Status Indicator	RSASigVer ECDSASigVer	Controller - KFWModuleVerify: E - KFWControllerVerify: E - KProduct: E - KBootloader: E
Image Decrypt	Decrypt image	CCS	Firmware Image Location	Status Indicator	GCMD	Controller - KDKDK: E - KDataDecryption: E
Image Encrypt	Encrypt image	CCS	Firmware Image Location	Status Indicator	GCME	Controller - KDKDK: E - KDataDecryption: E
Manifest Load	Verify and load trusted set of PKS	CCS	Manifest Location	Status	RSASigVer ECDSASigVer	Controller - KManifestPub: E - KManifestPub_ROM: E
RawCrypto	Raw cryptographic algorithm service with no assurance of security	CCS	Cryptographic algorithm and parameter	Status Indicator and result	None	Controller

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

External firmware is loading during the boot process. The firmware is validated using an RSA 3072 or 4096-bit or ECDSA P384 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.

5 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: non-modifiable bootloader - binary
- Component 3: non-modifiable run time firmware - binary

The firmware components are protected with one of the following authentication technique(s) described in the Pre-Operational Self-tests table.

- RSA 3072/4096 PKCS1_v1.5 (SHA2-384)
- RSA 3072/4096 PSS (SHA2-384)
- ECDSA P-384 (SHA384)

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 with a Physical Security at Level 2 therefore per the FIPS 140-3 Management Manual Section 7.5 Partial validations and non-applicable areas this section is not applicable.

7 Physical Security

The module is a production grade, single-chip cryptographic module with standard passivation over the modules circuitry as defined by FIPS 140-3 and is designed to meet Level 3 physical security requirements.

7.1 Mechanisms and Actions Required

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. The MACE does not contain any doors, removable covers, or ventilation holes or slits. No maintenance access interface is available. No special procedures are required to maintain physical security of the MACE while delivering to operators.

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-Evident Example

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	N/A	N/A	
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
Input using SP800-38D AES key Transport (IO3)	Outside the module boundary in ASIC Internal SRAM	Sub Chip security sub system RAM (S1)	Encrypted	Automated	Electronic	KTS2
Output using SP800-38F Key Transport (IO4)	Sub Chip security sub system RAM (S1)	Outside the module boundary in ASIC Internal SRAM	Encrypted	Automated	Electronic	KTS1

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Output using SP800-38D AES key Transport (IO5)	Sub Chip security sub system RAM (S1)	Outside the module boundary in ASIC Internal SRAM	Encrypted	Automated	Electronic	KTS2
Output encapsulated by RSA (IO6)	Sub Chip security sub system RAM (S1)	Outside the module boundary in ASIC Internal SRAM	Encrypted	Automated	Electronic	KTS3

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
RootKDK	Master key used to derive other keys	256 - 256	Key Derivation key - CSP	Input at Manufacturing		KDF
RootKeyWrapKey	Wrap key used for transport	256 - 256	Transport Key - CSP	CKG		KTS1
RootMACKey	HMAC Key used for integrity	256 - 256	HMAC Key - CSP	KDF		HMAC
RootPublicMacKey	HMAC Key used for integrity	256 - 256	HMAC Key - CSP	KDF		HMAC
DRBG-EI and seed	CTR_DRBG entropy input.	384 - N/A	N/A - CSP	ENT		RNG
DRBG-State	CTR_DRBG internal state: V (128 bits) and Key (AES 256)	256 - 256	N/A - CSP	RNG		HMAC ECDSA- KeyGen CKG
TCGWrapKey	CSP Transport	256 - 256	Transport Key - CSP	CKG		KTS1
TCGHMACKey	HMAC generation	256 - 256	HMAC Key - CSP	CKG		HMAC
OpenHMACKey	HMAC generation	256 - 256	HMAC Key - CSP	CKG		HMAC
Password	KM Authorization password is processed and used as the Label field in a counter based HMAC-SHA2-256 KBKDF	256 - 256	Plaintext password - CSP			KDF

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AuthKDK	AuthKey Key Derivation Key	256 - 256	Key Derivation Key - CSP	CKG		KDF
AuthKey	Credential transport Key	256 - 256	Transport Key - CSP	KDF		KTS1
AdminKey	CSP transport Key	256 - 256	Encryption Key - CSP	CKG		KTS1
PrivateKey	CSP transport Key	256 - 256	Transport Key - CSP	CKG		KTS1
RdsKey	CSP Transport Key	256 - 256	Transport Key - CSP	CKG		KTS1
DEK	User Data Encryption Key	512 - 256	Encryption Key - CSP	CKG		DPE DPD
SUP Seed	Random value used to generate an internal password	256 - 256	Random - CSP	CKG		KTS3
UDS	Unique Device Secret. Used to generate CDI	384 - 256	Key Derivation - CSP	CKG		KDF
CDI	Compound Device ID. Used to generate Device ID Wrap Key	384 - 256	Key Derivation - CSP	KDF		KTS1 KTS2
DeviceIDWrapKey	key used for -wrapping the DeviceIDPrivate ECDSA key	256 - 256	Transport Key - CSP	KDF		KTS1
KDeviceIDPrivate	Device Identity Key	384 - 192	Asymmetric Signature Key - CSP	ECDSA-KeyGen		ECDSASigVer ECDSASigGen
KAliasPrivate	Alias Key	384 - 192	Asymmetric Signature Key - CSP	ECDSA-KeyGen		ECDSASigGen ECDSA-KeyGen
KDeviceIDPublic	Device Identity Key	384 - 192	Asymmetric Signature	ECDSA-KeyGen		ECDSASigVer ECDSASigGen

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
			Verification - PSP			
KAliasPublic	Alias Key	384 - 192	Asymmetric Signature Verification - PSP	ECDSA-KeyGen		ECDSASigVer ECDSASigGen
KDKDK	Data Decryption KDK used to generate KDataDecryption	256 - 256	Key Derivation Key - CSP	Input at Manufacturing		KDF
KDataDecryption	Data decryption Key	256 - 256	Decryption Key - CSP	KDF		GCME GCMD
aworWrappingKey	Wrap key key used for transport	256 - 256	Transport Key - CSP			KTS2
aworHMACKey	HMAC Key used for integrity	256 - 256	HMAC Key - CSP			HMAC
KProduct	Product verification key	ECDSA Curve: 384, Modulus: 3072/4096 - ECDSA: 192, RSA: 128, 150	Signature verification - PSP			RSASigVer ECDSASigVer
KBootloader	Module firmware verification key	ECDSA Curve: 384, Modulus: 3072/4096 - ECDSA: 192, RSA: 128, 150	Signature verification - PSP			RSASigVer ECDSASigVer
KFWModuleVerify	Module firmware verification key	ECDSA Curve: 384, Modulus: 3072/4096 -	Signature verification - PSP			RSASigVer ECDSASigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		ECDSA: 192, RSA: 128, 150				
KFWControllerVerify	Controller signature verification Key	ECDSA Curve: 384, Modulus: 3072/4096 - ECDSA: 192, RSA: 128, 150	Signature verification - PSP			RSASigVer ECDSASigVer
KAuthPub	Key for Factory- restricted services signature verification	Modulus: 3072/4096 - RSA: 150,128, RSA-PKCS- 1.5, RSA- PSS	Signature verification - PSP			RSASigVer
KDeviceWrappingPub	Public Key for SUP Generate	Modulus: 3072/4096 - RSA: 128, 150	Signature verification - PSP			KTS3
KManifestPub	Public Key for manifest signature verification	ECDSA Curve: 384, Modulus: 3072/4096 - ECDSA: 192, RSA: 128, 150	Signature verification - PSP	Input at Manufacturing		RSASigVer ECDSASigVer
KManifestPub_ROM	Public Key for manifest signature verification	ECDSA Curve: 384, Modulus: 3072/4096 - ECDSA: 192,	Signature verification - PSP	Input at Manufacturing		RSASigVer ECDSASigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		RSA: 128, 150				
fsaKey	FSA Data Encryption Key	512 - 256	Encryption Key - CSP	CKG		AuxE AuxD

Table 17: SSP Table 1

Au

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
RootKDK		Sub Chip security sub system e-Fuse (S2):Plaintext		Z2	RootKeyWrapKey:Derives RootPublicMacKey:Derives RootHmacKey:Derives
RootKeyWrapKey	Input using SP800-38D AES key Transport (IO3) Output using SP800-38D AES key Transport (IO5)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	RootKDK:Derived From
RootMACKey	Input using SP800-38D AES key Transport (IO3) Output using SP800-38D AES key Transport (IO5)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	RootKDK:Derived From
RootPublicMacKey	Input using SP800-38D AES key Transport	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	RootKDK:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	(IO3) Output using SP800-38D AES key Transport (IO5)				
DRBG-EI and seed		Sub Chip security sub system register (S3):Plaintext	Until reboot	Z1	DRBG-State:Used With
DRBG-State		Sub Chip security sub system RAM (S1):Plaintext	Until reboot or reseed	Z1	DRBG-EI and seed:Derived From TCGWrapKey:directly generated from Drbg-State TCGHMACKey:directly generated from DrbgState OpenHMACKey:directly generated from DrbgState RdsKey:directly generated from DrbgState AdminKey:directly generated from DrbgState PrivateKey:directly generated from DrbgState DEK:directly generated from DrbgState SUP Seed:directly generated from DrbgState UDS:directly generated from DrbgState aworWrappingKey:directly generated from DrbgState aworHMACKey:directly generated from DrbgState

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TCGWrapKey	Input using SP800-38F AES key Transport (IO2) Input using SP800-38D AES key Transport (IO3) Output using SP800-38F Key Transport (IO4) Output using SP800-38D AES key Transport (IO5)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	RootKeyWrapKey:Wrapped by aworWrappingKey:Wrapped by DEK:Wraps
TCGHMACKey	Input using SP800-38F AES key Transport (IO2) Input using SP800-38D AES key Transport (IO3) Output using SP800-38F Key Transport (IO4) Output using SP800-38D AES key Transport (IO5)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	RootKeyWrapKey:Wrapped by aworWrappingKey:Wrapped by
OpenHMACKey	Input using SP800-38F AES key Transport	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	RootKeyWrapKey:Wrapped by aworWrappingKey:Wrapped by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	(IO2) Input using SP800-38D AES key Transport (IO3) Output using SP800-38F Key Transport (IO4) Output using SP800-38D AES key Transport (IO5)				
Password	Input in Plaintext(IO1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	AuthKDK:Used With AuthKey:Derives
AuthKDK	Input using SP800-38F AES key Transport (IO2) Output using SP800-38F Key Transport (IO4)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	Password:Used With AuthKey:Derives
AuthKey	Input using SP800-38F AES key Transport (IO2) Output using SP800-38F Key Transport (IO4)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	Password:Derived From AuthKDK:Derived From PrivateKey:Wraps
AdminKey	Input using SP800-38F AES key Transport (IO2)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	PrivateKey:Wraps and Wrapped by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Output using SP800-38F Key Transport (IO4)				
PrivateKey	Input using SP800-38F AES key Transport (IO2) Output using SP800-38F Key Transport (IO4)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	AuthKey:Wrapped by AdminKey:Wrapped by RdsKey:Wraps
RdsKey	Input using SP800-38F AES key Transport (IO2) Input using SP800-38D AES key Transport (IO3) Output using SP800-38F Key Transport (IO4) Output using SP800-38D AES key Transport (IO5)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	PrivateKey:Wrapped by DEK:Wraps
DEK	Input using SP800-38F AES key Transport (IO2) Output using SP800-38F Key Transport (IO4)	Sub Chip security sub system register (S3):Plaintext		Z1	TCGWrapKey:Wrapped by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SUP Seed	Output encapsulated by RSA (IO6)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	Password:Generates
UDS		Sub Chip security sub system e-Fuse (S2):Plaintext		Z2	CDI:Derives
CDI		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	UDS:Derived From DeviceIDWrapKey:Derives
DeviceIDWrapKey		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	CDI:Derived From KDeviceIDPrivate:After KDF, the key wraps the KDeviceIDPrivate
KDeviceIDPrivate		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KDeviceIDPublic:Used With DeviceIDWrapKey:Wrapped by
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
KDKDK		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	DRBG-State:directly generated by the DRBG
KDataDecryption	Input using SP800-38D AES key Transport (IO3)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KDKDK:Derived from

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
aworWrappingKey		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	DRBG-State:Generated by
aworHMACKey		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	DRBG-State:directly generated by the DRBG
KProduct	Input in Plaintext(IO1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	
KBootloader	Input in Plaintext(IO1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	
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_ROM:Used to establish trust by checking signature on Key Manifest
KDeviceWrappingPub	Input in Plaintext(IO1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	SUP Seed:Encrypts
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 KDeviceWrapping:Verified as trusted by using MVK to verify signature of a Key Manifest
KManifestPub_ROM	Input in Plaintext(IO1)	Sub Chip security sub system e-	Until reboot		

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
		Fuse (S2):Plaintext			
fsaKey	Input using SP800-38F AES key Transport (IO2) Output using SP800-38F Key Transport (IO4)	Sub Chip security sub system register (S3):Plaintext	Until reboot	Z1	TCGWrapKey:Wrapped by DRBG-State:Generated by

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.

The Module performs the following pre-operational self-tests in the 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) (A6147) or ECDSA SigVer (FIPS186-5) (A6142)	KAT	SW/FW Integrity	Success or Failure Code	Executed on the whole firmware stored in the Module - See 10.6 - Additional Information
Module run time firmware integrity test	RSA SigVer PKCS1_v1.5 or PSS (FIPS186-5) (A6147) or ECDSA SigVer (FIPS186-5) (A6142)	KAT	SW/FW Integrity	Success or Failure Code	Executed on the whole firmware stored in the Module - See 10.6 - Additional Information

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-GCM Encrypt	AES-256 Encrypt	KAT	CAST	Success or Failure Code	(Auxiliary) AES-256 GCM Encrypt KAT	At boot up
AES-GCM Decrypt	AES-256 Decrypt	KAT	CAST	Success or Failure Code	(Auxiliary) AES-256 GCM Decrypt KAT	At boot up
AES-KW Encryption	AES-256 Encrypt	KAT	CAST	Success or Failure Code	(Auxiliary) AES-256 KW Encrypt KAT	At boot up
AES-KW Decryption	AES-256 Decrypt	KAT	CAST	Success or Failure Code	(Auxiliary) AES-256 KW Decrypt KAT	At boot up
AES-XTS DPE Encryption	AES-256 Encrypt	KAT	CAST	Success or Failure Code	DPE 256-bit AES-XTS encryption KAT	At boot up
AES-XTS DPE Decryption	AES-256 Decrypt	KAT	CAST	Success or Failure Code	DPE 256-bit AES-XTS decryption KAT	At boot up
AES-XTS Aux Encryption	AES-256 Encrypt	KAT	CAST	Success or Failure Code	(Auxiliary) 256-bit AES-XTS encryption KAT	At boot up
AES-XTS Aux Decryption	AES-256 Decrypt	KAT	CAST	Success or Failure Code	(Auxiliary) 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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA KeyGen (FIPS186-5) (A6142)	ECDSA P-384	PCT	PCT	Success or Failure Code	A pairwise consistency check is performed on ECDSA private/public key on generation	When a new ECDSA key pair is generated
ECDSA SigGen (FIPS186-5)	ECDSA P-384 Signature Generation	KAT	CAST	Success or Failure Code	P-384 Signature Generation KAT with SHA-384	At boot up
ECDSA SigVer (FIPS186-5)	ECDSA P-384 Signature Verification KAT	KAT	CAST	Success or Failure Code	P-384 Signature Verification KAT with SHA-384	At boot up before Pre-Operational firmware integrity test.
HMAC-SHA2 ROM	HMAC SHA2-384	KAT	CAST	Success or Failure Code	HMAC SHA2-384 KAT	At boot up
KDF SP800-108	with HMAC-SHA2-384	KAT	CAST	Success or Failure Code	Counter mode KBKDF KAT. Inclusive of HMAC-SHA2-384 KAT.	At boot up
SHA2-384 FW	SHA2-384 Performed during boot before the pre-operational integrity checks (ROM)	KAT	CAST	Success or Failure Code	SHA2-384 KAT for the Firmware SHA	At boot up
SHA2 ROM	SHA2-512	KAT	CAST	Success or Failure Code	SHA2-512 for the SHA engine	At boot up
RSA SigVer (FIPS186-5) (A6147)	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.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
BootLoader Firmware Load test	RSA SigVer (FIPS186-5) (A6147), ECDSA SigVer (FIPS186-5) (A6142)	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. See 10.6 - Additional Information	At boot up
Runtime Firmware Load test	RSA SigVer (FIPS186-5) (A6147), ECDSA SigVer (FIPS186-5) (A6142)	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. See 10.6 - Additional Information	At boot up
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
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-GCM Encrypt	KAT	CAST	On Demand	Device Reset
AES-GCM Decrypt	KAT	CAST	On Demand	Device Reset
AES-KW Encryption	KAT	CAST	On Demand	Device Reset
AES-KW Decryption	KAT	CAST	On Demand	Device Reset
AES-XTS DPE Encryption	KAT	CAST	On Demand	Device Reset
AES-XTS DPE Decryption	KAT	CAST	On Demand	Device Reset
AES-XTS Aux Encryption	KAT	CAST	On Demand	Device Reset
AES-XTS Aux Decryption	KAT	CAST	On Demand	Device Reset
Conditioning Component Block	KAT	CAST	On Demand	Device Reset

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Cipher Derivation Function SP800-90B (A2272)				
Counter DRBG (C1278)	KAT	CAST	On Demand	Device Reset
ECDSA KeyGen (FIPS186-5) (A6142)	PCT	PCT	N/A	N/A
ECDSA SigGen (FIPS186-5)	KAT	CAST	On Demand	Device Reset
ECDSA SigVer (FIPS186-5)	KAT	CAST	On Demand	Device Reset
HMAC-SHA2 ROM	KAT	CAST	On Demand	Device Reset
KDF SP800-108	KAT	CAST	On Demand	Device Reset
SHA2-384 FW	KAT	CAST	On Demand	Device Reset
SHA2 ROM	KAT	CAST	On Demand	Device Reset
RSA SigVer (FIPS186-5) (A6147)	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
Entropy 90B Start-up Repetition Count Test (RCT)	Fault induction	CAST	On Demand	Device Reset
Entropy 90B Start-up Adaptive Proportion Test (APT)	Fault induction	CAST	On Demand	Device Reset
Entropy 90B Continuous Repetition Count Test (RCT)	Fault induction	CAST	N/A	N/A
Entropy 90B Continuous Adaptive Proportion Test (APT)	Fault induction	CAST	N/A	N/A

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 self-test. Non-operational state. No services beside status services are allowed	Triggered by cryptographic self-test 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.

10.6 Additional Information

For the Firmware Integrity and Load tests, based on client needs, either RSA or ECDSA is selected, and the proper signature verification is used.

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 Complete 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 outline 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 under either NVMe, TCG Opal or both 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. Drive Owner supplementary Info9550_nvme_ssd_ES_2024_05_13.pdf
2. Micron Technical Note TN_FD-28: Installing Micron SEDs in Windows 8 and 10
3. TCG Level 0 Discovery Values

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 or 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.

Table 24 – References

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, December 20, 2024</i>
[108]	<i>NIST Special Publication 800-108r1, 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>
[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>
[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>

Abbreviation	Full Specification Name
[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]	ACS-3 Reporting Security Compliance December 1,2009
[TCG-SSC-Opal]	<i>TCG Storage Security Subsystem Class: Opal, Specification</i>
[TCG-SACS]	<i>TCG Storage Architecture Core Specification</i>
[185]	<i>National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-5, February 2023.</i>

Table 25 – Acronyms and Definitions

Acronym	Definition
KAT	Known Answer Test
SSP	Sensitive Security Parameter
AK	Authentication key
DEK	Data Encryption Key
LBA	Logical Block Address
CCS	Command Completion Status