Micron Technology, Inc.

Micron® MSA12-P5 Controller Sub Chip Security Subsystem

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 0.3
Date: 8-5-2025

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 10
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 15
3 Cryptographic Module Interfaces 16
3.1 Ports and Interfaces 16
4 Roles, Services, and Authentication 17
4.1 Authentication Methods 17
4.2 Roles 17
4.3 Approved Services 18
4.4 Non-Approved Services 25
4.5 External Software/Firmware Loaded 25
5 Software/Firmware Security 26
5.1 Integrity Techniques 26
5.2 Initiate on Demand 26
6 Operational Environment 27
6.1 Operational Environment Type and Requirements 27
7 Physical Security 28
7.1 Mechanisms and Actions Required 28
8 Non-Invasive Security 29
8.1 Mitigation Techniques 29
9 Sensitive Security Parameters Management 30
9.1 Storage Areas 30
9.2 SSP Input-Output Methods 30

9.3 SSP Zeroization Methods 31
9.4 SSPs 31
10 Self-Tests 42
10.1 Pre-Operational Self-Tests 42
10.2 Conditional Self-Tests 42
10.3 Periodic Self-Test Information 46
10.4 Error States 48
10.5 Operator Initiation of Self-Tests 48
10.6 Additional Information 48
11 Life-Cycle Assurance 49
11.1 Installation, Initialization, and Startup Procedures 49
11.2 Administrator Guidance 49
11.3 Non-Administrator Guidance 49
11.4 Design and Rules 49
Rules of Operation 49
12 Mitigation of Other Attacks 50
References and Definitions 50

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 10
Table 5: Vendor-Affirmed Algorithms 10
Table 6: Security Function Implementations 13
Table 7: Entropy Certificates 14
Table 8: Entropy Sources 15
Table 9: Ports and Interfaces 16
Table 10: Authentication Methods 17
Table 11: Roles 17
Table 12: Approved Services 24
Table 13: Mechanisms and Actions Required 28
Table 14 – Tamper-Evident Seal Locations Guidance 28
Table 15: Storage Areas 30
Table 16: SSP Input-Output Methods 31
Table 17: SSP Zeroization Methods 31
Table 18: SSP Table 1 35
Table 19: SSP Table 2 41
Table 20: Pre-Operational Self-Tests 42
Table 21: Conditional Self-Tests 45
Table 22: Pre-Operational Periodic Information 46
Table 23: Conditional Periodic Information 47
Table 24: Error States 48
Table 25 References 50
Table 26 Acronyms and Definitions 51

List of Figures

Figure 1 – Cryptographic Boundary (red) and TOEPP 7
Figure 2 – Physical Perimeter / boundary (Top and Bottom View) 7

1 – General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version MSA12-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:

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® MSA12-P5 Controller Sub Chip Security Subsystem module is hereafter denoted as the Module. The Module is a Single-Chip Hardware sub-chip cryptographic subsystem, as defined in FIPS 140-3 Implementation Guidance 2.3.B.

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 1. The Module is a single chip embodiment. The cryptographic boundary is the logical cryptographic boundary of the module is defined by the Security Subsystem and includes all cryptographic algorithm implementations. The physical cryptographic boundary is the Micron® MSA12-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® MSA12-P5 ASIC package.

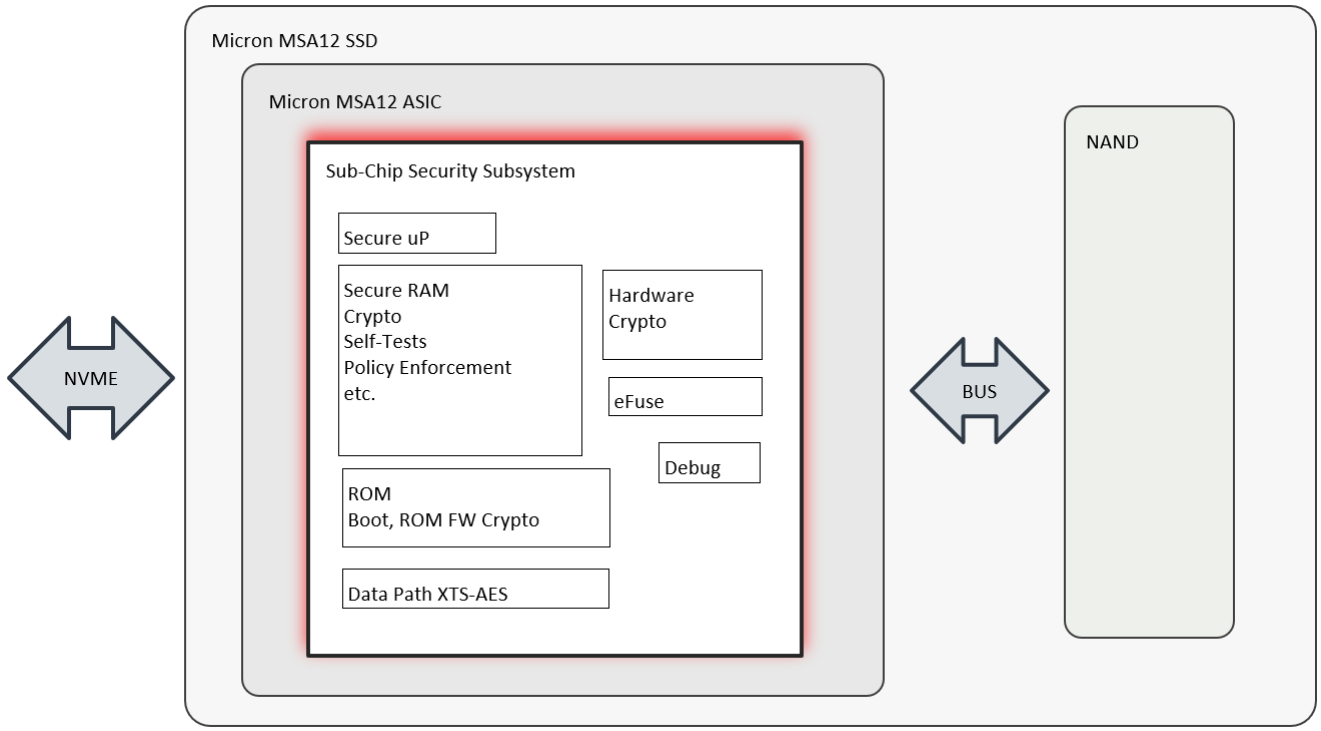


Figure 1 – Cryptographic Boundary (red) and TOEPP



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® MSA12-P5 Controller Sub Chip Security Subsystem	0x0C87E5	Function ROM v4.0, Bootloader V4.1, Runtime SCCS v6.0	Micron® MSA12-P5	NVMe interface at the physical boundary

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

The module does not have any excluded components.

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

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 FIPS Approved cryptographic algorithms listed the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	C1278	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A7661, A7668	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	C1278	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	A7668	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 256	SP 800-38D
AES-KW	A7663	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38F
AES-XTS Testing Revision 2.0	A7661, A7668	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
Conditioning Component Block Cipher Derivation Function SP800-90B	A2272	Key Length - 128	SP 800-90B
Counter DRBG	C1278	Prediction Resistance - No, Yes Mode - AES-128, AES-256 Derivation Function Enabled - No	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A7666	Curve - P-384 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A7666	Curve - P-384	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7666	Curve - P-384 Hash Algorithm - SHA2-384 Component - Yes	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A7666	Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
HMAC-SHA2-384	A7535	Key Length - Key Length: 384	FIPS 198-1
HMAC-SHA2-512/256	A7535	Key Length - Key Length: 256	FIPS 198-1
KDF SP800-108	A7667	KDF Mode - Counter Supported Lengths - Supported Lengths: 384	SP 800-108 Rev. 1
KTS-IFC	A7662	Modulo - 3072, 4096 Key Generation Methods - rsakpg1-basic Scheme - KTS-OAEP-basic - KAS Role - initiator Key Transport Method - Key Length - 256	SP 800-56B Rev. 2
RSA SigVer (FIPS186-5)	A7534	Hash Pair - Hash Algorithm - SHA2-384 Modulo - 3072, 4096	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
		Signature Type - pkcs1v1.5, pss	
SHA2-384	A7664, A7665	Message Length - Message Length: 384, 8-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4
SHA2-512	A7665	Message Length - Message Length: 512, 8-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4
SHA2-512/256	A7665	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 below.

Name	Properties	Implementation	Reference
CKG1	Key Type:Symmetric and Asymmetric	N/A	SP800-133rev2 Section 4 example 1 and IG D.H
CKG - XTS	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

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

Name	Type	Description	Properties	Algorithms
KTS1	KTS-Unwrap KTS-Wrap	Key Transport Wrapping	Caveat:Key establishment methodology provides 256 bits of encryption strength IG:D.G	AES-KW: (A7663)
KTS2	KTS-Unwrap KTS-Wrap	Key Transport Wrapping	Caveat:Key establishment methodology provides 256 bits of encryption strength I.G.:D.G	AES-GCM: (A7668)
KTS3	KTS-Encap	Key Transport Encapsulation	Caveat:Key transport methodology provides between 128 and 150 bits of encryption strength IG:D.G Key confirmation:No	KTS-IFC: (A7662) SHA2-384: (A7664)
GCME	BC-AuthEncrypt	Authenticated message encryption		AES-GCM: (A7668) AES-ECB: (A7668)
GCMD	BC-AuthDecrypt	Authenticated message decryption		AES-GCM: (A7668) AES-ECB: (A7668)
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)
SHS1	SHA	Message hashing		SHA2-384: (A7665)
SHS2	SHA	Message hashing		SHA2-512: (A7665)

Name	Type	Description	Properties	Algorithms
HMAC	MAC	Message authentication code generation		HMAC-SHA2-384: (A7535) HMAC-SHA2-512/256: (A7535) SHA2-384: (A7665) SHA2-512/256: (A7665) : ()
DPE	BC-UnAuthEncrypt	User Data encryption		AES-ECB: (A7661) AES-XTS Testing Revision 2.0: (A7661) CKG - XTS: () AES 256: Symmetric Key Generation
DPD	BC-UnAuthDecrypt	User Data decryption		AES-ECB: (A7661) AES-XTS Testing Revision 2.0: (A7661) CKG - XTS: () AES 256: Symmetric Key Generation
AuxE	BC-UnAuthEncrypt	User Data encryption		AES-ECB: (A7668) AES-XTS Testing Revision 2.0: (A7668) CKG - XTS: () AES 256: Symmetric Key Generation
AuxD	BC-UnAuthDecrypt	User Data decryption		AES-ECB: (A7668) AES-XTS Testing Revision 2.0: (A7668) CKG - XTS: () AES 256:

Name	Type	Description	Properties	Algorithms
				Symmetric Key Generation
KDF	KBKDF	Key-Based Key Derivation		KDF SP800-108: (A7667) HMAC-SHA2-384: (A7535) HMAC-SHA2-512/256: (A7535) SHA2-384: (A7665) SHA2-512/256: (A7665)
RSAVer	DigSig-SigVer	Signature verification		RSA SigVer (FIPS186-5): (A7534) SHA2-384: (A7665) SHA2-512: (A7665)
ECDSASigVer	DigSig-SigVer	Signature verification		ECDSA SigVer (FIPS186-5): (A7666) SHA2-384: (A7665)
ECDSASigGen	DigSig-SigGen	Signature generation		ECDSA SigGen (FIPS186-5): (A7666) SHA2-384: (A7665)
ECDSA-KeyGen	AsymKeyPair-KeyGen AsymKeyPair-KeyVer	Key generation		ECDSA KeyGen (FIPS186-5): (A7666) ECDSA KeyVer (FIPS186-5): (A7666) 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 ≠ 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 2 modes 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).

FIPS140-3 IG C.H, Option 4

Image encryption uses a key derived from the KDK and a random (DRBG) value used as the fixed input string.

The IV (96 bits) is entirely generated using an approved DRBG (Cert. #C1278).

The key (256 bits) is generated using a KDF. The inputs for the KDF are:
1. The key – It is the KDK (256 bits). It is a fixed random value per device (established at time of manufacture).
2. The String (aka Label & Context - 256 bits) – This entire field is generated using an approved DRBG.

The possibility of key/IV collision over the life of the device is very small. The key and IV are both generated with new random numbers on each encryption operation.

2.8 RBG and Entropy

Cert Number	Vendor Name
E304	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 ® MSA12-P5 SSD Controller	Physical	MSA12-P5 SSD Controller	128 bit	Full entropy	A2272 (BlockCipher_DF)

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Sub Chip Security Subsystem ENT					

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 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 Protocol.

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

Note: The module does not support Control Output.

4 Roles, Services, and Authentication

4.1 Authentication Methods

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	RSAVer and ECDSASigVer	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 roles, the Controller (Cryptographic Officer). One authentication is allowed per Module reset.

The module does not support a maintenance role

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

The Module does not support concurrent operators.

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:

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 SHS1 SHS2 HMAC DPE DPD AuxE AuxD KDF RSAVer ECDSASigVer ECDSASigGen CKG	Controller - DRBG-EI and seed: G,E - DRBG-State: G Unauthenticated - DRBG-EI and seed: G,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 and module status.	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 - Password: W,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 KTS2 RNG AuxE	Controller - TCGWrapKey: G,R,E - TCGHMACKey: G,R - OpenHMACKey: R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					AuxD CKG	- AdminKey: R,W - PrivateKey: R,W,E - RdsKey: R,W,E - DEK: R - AuthKDK: E - RootKeyWrapKey: G,R,E - RootMACKey: G,R,E - RootPublicMacKey: G,R - aworWrappingKey: G,E - KDeviceIDPrivate: R - KDKDK: R - fsaKey: G,R,E - RootKDK: E
CSP-Import	Import module protected CSPs	CCS	CSP List	CSP List	KTS1	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	CCS	Data packet	Data Packet	DPE DPD	Controller - DEK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	data to / from a user data range					
SUP Generate	KTS-IFC wrap an internally generated random	CCS	None	Encrypted password context Status	KTS3 RNG KDF CKG	Controller - AuthKDK: G,E - AuthKey: G,E - TCGWrapKey: E - KDeviceWrappingPub: W,E - Password: E - SUP Seed: G,R
SUP Authenticate	Unwrap SUP blob using KBKDF derived key	CCS	Password	Authentication result	KDF	Controller - AuthKDK: E - AuthKey: E - TCGWrapKey: E - Password: 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: G,E
Attestation	Device cryptographic identity and attestation	CCS	Index	Status Indicator	RNG SHS1 SHS2 KDF ECDSASigVer ECDSASigGen ECDSA-KeyGen	Controller - KDeviceIDPrivate: G,E - KDeviceIDPublic: G,R,E - KAliasPrivate: G,E - KAliasPublic: G,R,E - UDS: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG-State: E - CDI: G,E - DeviceIDWrapKey: G,E
Zeroize	Destroys all keys. Must be performed under the direct control of the operator	CCS	None	None	None	Controller - RootKDK: Z - RootMACKey: Z - RootPublicMacKey: Z - DRBG-EI 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:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - KAuthPub: Z - KDeviceWrappingPub: Z - KManifestPub: Z - fsaKey: - RootKeyWrapKey: Z - UDS: Z - KAliasPublic: 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 - KAuthPub: Z - KDeviceWrappingPub:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - KManifestPub: Z - RootKeyWrapKey: Z - RootPublicMacKey: Z - UDS: Z
Factory Auth	Authentication for factory-restricted services	CCS	Authorization signature	Random Value	RSAVer	Controller - KAuthPub: W,E
Firmware Signature Check	Verify firmware image signature	CCS	Firmware Image Location	Status Indicator	RSAVer ECDSASigVer	Controller - KFWModuleVerify: W,E - KFWControllerVerify: W,E - KProduct: W,E - KBootloader: W,E
Image Decrypt	Decrypt image	CCS	Firmware Image Location	Status Indicator	GCMD KDF	Controller - KDKDK: E - KDataDecryption: G,E
Image Encrypt	Encrypt image	CCS	Firmware Image Location	Status Indicator	GCME KDF	Controller - KDKDK: E - KDataDecryption: G,E
Manifest Load	Verify and load trusted set of PKS	CCS	Manifest Location	Status	RSAVer 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

NOTE: 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.
Data output is inhibited during software or firmware loading and load test.

5 Software/Firmware Security

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 PKCS1_PSS (SHA2-384)
- ECDSA P-384 (SHA384)

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

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.

5.2 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

The Module has a non-modifiable/limited operational environment at Level <# > under the FIPS 140-3 definitions therefore per the FIPS 140-3 Management Manual Section 7.5 Partial validations and non-applicable areas this section is not applicable.

Type of Operational Environment: Limited

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

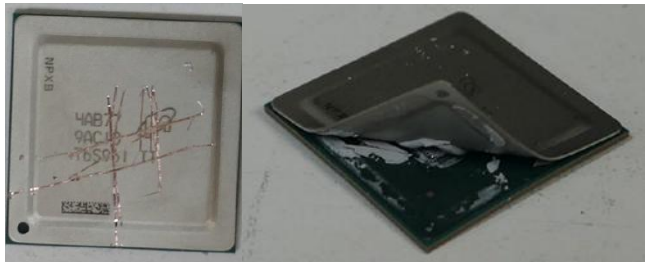


Table 14 – Tamper-Evident Seal Locations Guidance

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 15: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input in Plaintext (I1)	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 (I2)	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 (I3)	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 (O1)	Sub Chip security sub system RAM (S1)	Outside the module boundary in ASIC Internal SRAM	Encrypted	Automated	Electronic	KTS1
Output using SP800-38D AES key Transport (O2)	Sub Chip security sub system RAM (S1)	Outside the module boundary in ASIC Internal SRAM	Encrypted	Automated	Electronic	KTS2
Output encapsulated by RSA (O3)	Sub Chip security sub system RAM (S1)	Outside the module boundary in ASIC Internal SRAM	Encrypted	Automated	Electronic	KTS3

Table 16: 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 17: 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

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
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
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

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
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		KDF
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 Verification - PSP	ECDSA-KeyGen		ECDSASigVer ECDSASigGen
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	CKG		KTS2
aworHMACKey	HMAC Key used for integrity	256 - 256	HMAC Key - CSP	CKG		HMAC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
KProduct	Product verification key	ECDSA Curve: 384, Modulus: 3072/4096 - ECDSA: 192, RSA: 128, 150	Signature verification - PSP			RSAVer ECDSASigVer
KBootloader	Module firmware verification key	ECDSA Curve: 384, Modulus: 3072/4096 - ECDSA: 192, RSA: 128, 150	Signature verification - PSP			RSAVer ECDSASigVer
KFWModuleVerify	Module firmware verification key	ECDSA Curve: 384, Modulus: 3072/4096 - ECDSA: 192, RSA: 128, 150	Signature verification - PSP			RSAVer ECDSASigVer
KFWControllerVerify	Controller signature verification Key	ECDSA Curve: 384, Modulus: 3072/4096 - ECDSA: 192, RSA: 128, 150	Signature verification - PSP			RSAVer ECDSASigVer
KAuthPub	Key for Factory-restricted services signature verification	Modulus: 3072/4096 - RSA: 150,128, RSA-PKCS-1.5, RSA-PSS	Signature verification - PSP			RSAVer
KDeviceWrappingPub	Public Key for SUP Generate	Modulus: 3072/4096 - RSA: 128, 150	Signature verification - PSP			KTS3

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
KManifestPub	Public Key for manifest signature verification	ECDSA Curve: 384, Modulus: 3072/4096 - ECDSA: 192, RSA: 128, 150	Signature verification - PSP	Input at Manufacturing		RSAVer ECDSASigVer
KManifestPub_ROM	Public Key for manifest signature verification	ECDSA Curve: 384, Modulus: 3072/4096 - ECDSA: 192, RSA: 128, 150	Signature verification - PSP	Input at Manufacturing		RSAVer ECDSASigVer
fsaKey	FSA Data Encryption Key	512 - 256	Encryption Key - CSP	CKG		AuxE AuxD

Table 18: SSP Table 1

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 (I3) Output using SP800-38D AES key Transport (O2)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	RootKDK:Derived From
RootMACKey	Input using SP800-38D AES key Transport (I3) Output using SP800-38D AES	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	RootKDK:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	key Transport (O2)				
RootPublicMacKey	Input using SP800-38D AES key Transport (I3) Output using SP800-38D AES key Transport (O2)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	RootKDK:Derived From
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

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					aworHMACKey:directly generated from DrbgState
TCGWrapKey	Input using SP800-38F AES key Transport (I2) Input using SP800-38D AES key Transport (I3) Output using SP800-38F Key Transport (O1) Output using SP800-38D AES key Transport (O2)	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 (I2) Input using SP800-38D AES key Transport (I3) Output using SP800-38F Key Transport (O1) Output using SP800-38D AES key Transport (O2)	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 (I2) Input using SP800-38D AES key Transport (I3)	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
	Output using SP800-38F Key Transport (O1) Output using SP800-38D AES key Transport (O2)				
Password	Input in Plaintext (I1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	AuthKDK:Used With AuthKey:Derives
AuthKDK	Input using SP800-38F AES key Transport (I2) Output using SP800-38F Key Transport (O1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	Password:Used With AuthKey:Derives
AuthKey	Input using SP800-38F AES key Transport (I2) Output using SP800-38F Key Transport (O1)	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 (I2) Output using SP800-38F Key Transport (O1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	PrivateKey:Wraps and Wrapped by
PrivateKey	Input using SP800-38F AES key Transport (I2) Output using SP800-38F Key Transport (O1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	AuthKey:Wrapped by AdminKey:Wrapped by RdsKey:Wraps

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
RdsKey	Input using SP800-38F AES key Transport (I2) Input using SP800-38D AES key Transport (I3) Output using SP800-38F Key Transport (O1) Output using SP800-38D AES key Transport (O2)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1	PrivateKey:Wrapped by DEK:Wraps
DEK	Input using SP800-38F AES key Transport (I2) Output using SP800-38F Key Transport (O1)	Sub Chip security sub system register (S3):Plaintext		Z1	TCGWrapKey:Wrapped by
SUP Seed	Output encapsulated by RSA (O3)	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

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
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 (I3)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	KDKDK:Derived from
aworWrappingKey		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	DRBG-State:Generated by aworHMACKey:Used With
aworHMACKey		Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	DRBG-State:directly generated by the DRBG aworWrappingKey:Used With
KProduct	Input in Plaintext (I1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	
KBootloader	Input in Plaintext (I1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	
KFWModuleVerify	Input in Plaintext (I1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	
KFWControllerVerify	Input in Plaintext (I1)	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
KAuthPub	Input in Plaintext (I1)	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 (I1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	SUP Seed:Encrypts
KManifestPub	Input in Plaintext (I1)	Sub Chip security sub system RAM (S1):Plaintext	Until reboot	Z1 Z2	
KManifestPub_ROM	Input in Plaintext (I1)	Sub Chip security sub system e-Fuse (S2):Plaintext	Until reboot		
fsaKey	Input using SP800-38F AES key Transport (I2) Output using SP800-38F Key Transport (O1)	Sub Chip security sub system register (S3):Plaintext	Until reboot	Z1	TCGWrapKey:Wrapped by DRBG-State:Generated by

Table 19: 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 (A7534 or ECDSA SigVer (FIPS186-5) (A7666)	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 (A7534 or ECDSA SigVer (FIPS186-5) (A7666)	KAT	SW/FW Integrity	Success or Failure Code	Executed on the whole firmware stored in the Module - See 10.6 - Additional Information

Table 20: 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	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)	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)	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) (A7534, ECDSA SigVer (FIPS186-5) (A7666)	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) (A7534, ECDSA SigVer (FIPS186-5) (A7666)	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	RCT	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	APT	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	RCT	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	APT	CAST	Success or Failure Code	As specified in [90B] APT continuous health tests	Continuous when entropy is requested

Table 21: 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 22: 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 Cipher Derivation Function SP800-90B (A2272)	KAT	CAST	On Demand	Device Reset

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG	KAT	CAST	On Demand	Device Reset
ECDSA KeyGen (FIPS186-5)	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)	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)	RCT	CAST	On Demand	Device Reset
Entropy 90B Start-up Adaptive Proportion Test (APT)	APT	CAST	On Demand	Device Reset
Entropy 90B Continuous Repetition Count Test (RCT)	RCT	CAST	N/A	N/A
Entropy 90B Continuous Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A

Table 23: 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 24: 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 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 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: 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, sw/fw loading and error states.
8. Cryptographic operations are inhibited in all error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
10. There are no restrictions on which keys or SSPs are zeroized by the zeroization service.
11. The Module does not support concurrent operators.
12. The Module does not support a maintenance interface or role.
13. The Module does not support manual SSP establishment method.
14. The Module does not have any proprietary external input/output devices used for entry/output of data.
15. The Module does not enter or output plaintext CSPs.
16. The Module does not output intermediate key values.
17. 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 25 References

Abbreviation	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, March 22, 2019
[ISO19790]	*International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017*
[ISO24759]	*International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015*

Abbreviation	Full Specification Name
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, September 2, 2025*
[108]	*NIST Special Publication 800-108rev1, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), February 2024*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 2, March 2019*
[133]	*NIST Special Publication 800-133rev2, Recommendation for Cryptographic Key Generation, Revision 2, June 2020*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38D]	*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*
[38E]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, Special Publication 800-38E, January 2010*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56Br2]	*NIST Special Publication 800-56B Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Finite Field Cryptography, March 2019*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*
[ACS-3]	ACS-3 Reporting Security Compliance December 1,2009
[TCG-SSC-Opal]	*TCG Storage Security Subsystem Class: Opal, Specification*
[TCG-SACS]	*TCG Storage Architecture Core Specification*
[185]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-5, February 2023.*

Table 26 Acronyms and Definitions

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