Micron Technology, Inc.

MICRON 1100 SSD

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 1.35

Date: 04/24/17

CHANGE RECORD

Revision	***Date***	***Author***	***Description of Change***
1.17	7/12/16	Dale McNamara	Change to multi-chip embedded from standalone
1.18	7/16/16	Dale McNamara	Restore the FWD and VSA roles
1.19	7/18/16	Dale McNamara	Add RSA justification
1.20	7/19/16	Dale McNamara	Add configurations and H/W part numbers
1.21	7/21/16	Dale McNamara	Update Module name
1.22	7/24/16	Dale McNamara	Change CRC from 16 to 32 to match code, update to minimum 10 byte password
1.23	7/24/16	Dale McNamara	Add this change record
1.24	7/25/16	Dharmalingam Nagarajan	Updated Revert and RevertSp method
1.25	7/27/16	Dale McNamara	Update module numbers, remove default password for ATA security
1.26	8/01/16	Dale McNamara	Update Module numbers, add firmware load check service
1.27	8/05/16	Dale McNamara	Add Micron Generic Module numbers
1.28	8/10/16	Dale McNamara	Add F/W Versions, Update Password Justification
1.29	8/11/16	Dale McNamara	Update Password Justification
1.30	8/24/16	Dale McNamara	Incorporate InfoGard markups (some formatting, Micron Name update, Cert numbers)
1.31	9/27/16	Dale McNamara	Update Figure 1, respond to InfoGard comments
1.32	10/4/16	Dale McNamara	Certificate numbers were updated
1.33	12/21/16	Dale McNamara	Minor changes based on NIST report comments
1.34	1/23/17	Dale McNamara	Updates after review with InfoGard
1.35	4/24/17	Dale McNamara	Correction made to firmware version

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Micron Technology, Inc. (Micron) MICRON 1100 SSD module, hereafter denoted as the “MICRON 1100 SSD” or the “cryptographic module”. The MICRON 1100 SSD is a multi-chip embedded device which provides AES 256 encryption/decryption of data that is stored in NAND flash. The Module supports the SATA interface and is compliant with the Trusted Computing Group (TCG) SSC specification Opal. The Module meets FIPS 140-2 overall security level 2.

Table 1 – Cryptographic Module Configurations

	Module	Capacity	HW P/N and Version	FW Version
1	1100 2.5-Inch SATA NAND Flash SSD	256GB	MTFDDAK256TBN-1AR15FCHA	HPC0F10
		512GB	MTFDDAK512TBN-1AR15FCHA	
		256GB	MTFDDAK256TBN-1AR15FCYY	M0MF000
		512GB	MTFDDAK512TBN-1AR15FCYY	
2	1100 M.2 SATA NAND Flash SSD	256GB	MTFDDAV256TBN-1AR15FCHA	HPC0F10
		512GB	MTFDDAV512TBN-1AR15FCHA	
		256GB	MTFDDAV256TBN-1AR15FCYY	M0MF000
		512GB	MTFDDAV512TBN-1AR15FCYY	

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated storage devices. The Module is a multi-chip embedded embodiment; the cryptographic boundary is encapsulated in a tamper evident enclosure for the 2.5” form factor and is packaged with an opaque material for the M.2 form factor.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2

Security Requirement	Security Level
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

1.1 Hardware and Physical Cryptographic Boundary

The MICRON 1100 SSD is provided in two physical form factors, 2.5" and M.2. These are depicted in Figures 1 and 2 below. In both figures the red outline in the figure depicts the physical cryptographic boundary. For the 2.5" form factor the drive enclosure is the physical boundary. The module is protected by a tamper evident enclosure and tamper evident labels. To ensure evidence of tampering, two labels are used as indicated in Figure 1. The only components exposed are the SATA Data and Power ports. The module does not support a maintenance access interface. For the MICRON 1100 M.2 format, the boundary encompasses the entire PCB. This boundary includes all components (processor and memory) that implement cryptography and process the CSPs. Both modules rely on the SATA IO module as input/output devices.

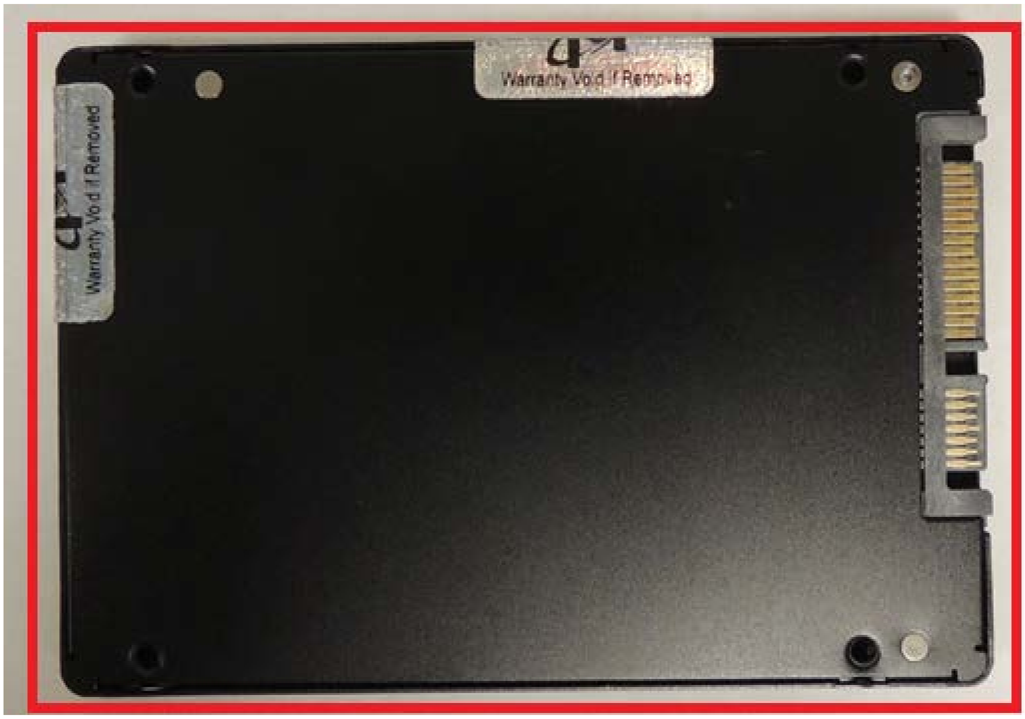

Figure 1 – MICRON 1100 2.5" Form Factor

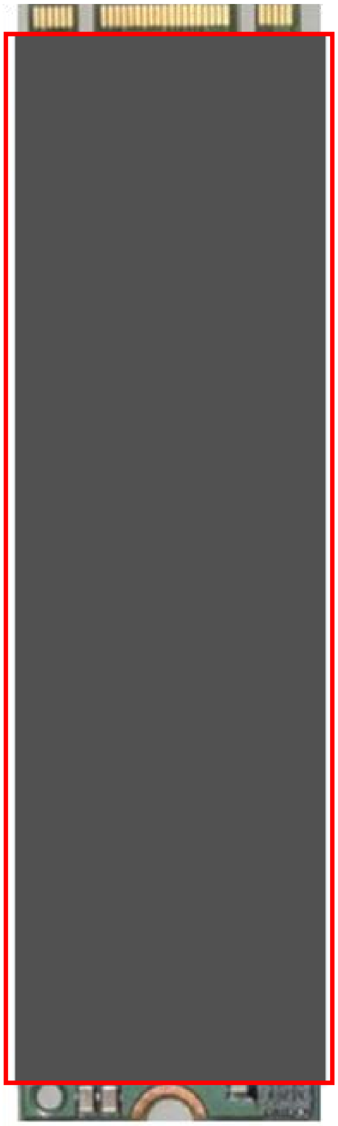

Figure 2 – MICRON 1100 M.2 Form Factor

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
SATA Power	SATA power	Power In
SATA Data	SATA Data IO	Control In, Data In, Data Out, and Status Out

1.2 Firmware and Logical Cryptographic Boundary

The MICRON 1100 SSD module uses a single chip controller with a SATA interface on the system side and Micron NAND flash internally. The following figure depicts the Module operational environment. The red outline in the figure depicts the logical cryptographic boundary which is within the enclosure of the device. All firmware runs on the controller within this logical boundary.

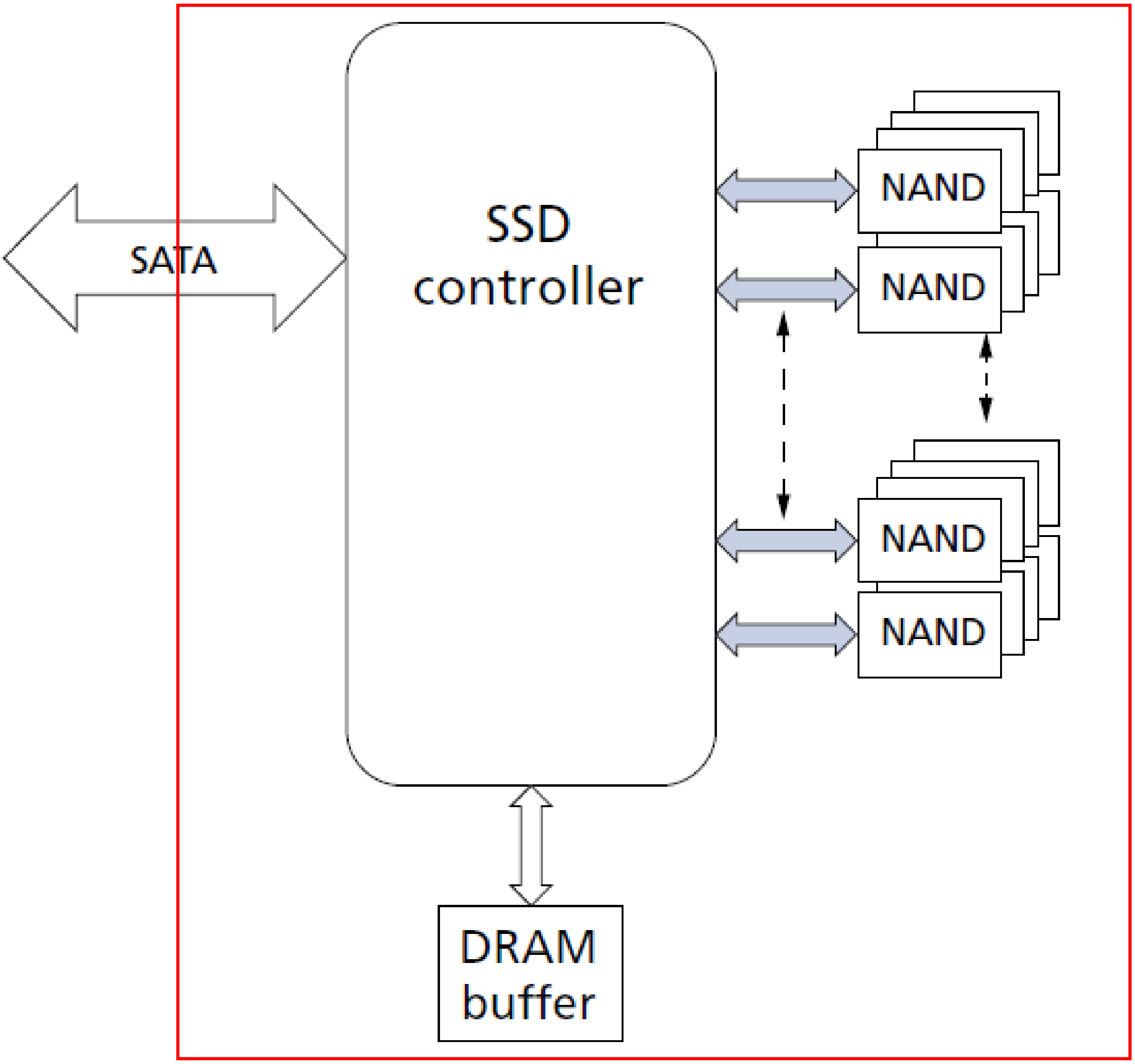

Figure 3 – Module Block Diagram

- All firmware executes on the SSD controller which provides:
  - SATA Host interface – providing control status and data paths.
  - Cryptographic functionality
    - AES bulk encrypt/decrypt functionality
    - RSA 2048 for firmware signature verification
    - SHA256/HMAC integrity checking
    - DRBG - Random number generation
- DRAM provides variable storage, instruction memory, data mapping tables and buffer for user data going into and out of the device.

- NAND flash is the storage medium where user data, system data, mapping tables, and main firmware are stored.

1.3 Modes of Operation

The MICRON 1100 SSD drive supports two distinct FIPS approved modes of operation. These are defined as Security mode 0 and Security mode 1. The device can transition from Security mode 0 to Security mode 1 but the transition from Security mode 1 to Security mode 0 can only be effected by resetting the device. The characteristics of the approved modes of operation are described below.

- **Security Mode 0 -** This is the default operating mode of the module. The device will always boot in this mode. The following states this mode are defined.
    - **Uninitialized State –** In this operating state, ownership of the drive has not been taken and the operating security characteristics have not been initialized. Once initialized the module will operate in one of the following two operating sub-states.
    - **Opal Security State -** In this state the module provides services through ATA industry standard commands as well as TCG Opal commands addressed to both the TCG Admin SP and the TCG locking SP. In addition extra features are provided through the TCG opal commands. All ATA security State services are unsupported. To initialize in this mode the module owner must take ownership of the device by invoking the activate method on the locking SP from the uninitialized state. This State has the capability to have multiple Users with independent access control to read, write or erase the data areas (LBA ranges). Note that by default there is a single “Global Range” that encompasses the whole user data area.
    - **ATA Security State** – In this state the module provides services through ATA industry standard commands as well as specific TCG Opal commands. Both master and user roles are implemented as defined in the ATA specification [ATA-8 ACS]. To transition to this state of operation, the ATA user must perform a set PIN from the uninitialized state. TCG Admin SP commands are allowed in this state which do not require any cryptographic services.
- **Security Mode 1 –** This mode is effectively a superset of Security Mode 0. The operating security characteristics of Security mode 0 will be inherited when a transition to mode 1 occurs. The module transitions directly from Security modes 0 to Security mode 1 upon receipt of a host command requiring the RSA Authentication (i.e. FW download request or VS authentication command request). All initialization self-tests, see Self Tests, will also be automatically performed by the module when Security mode 1 is entered. Once entered this mode will persist until the next reboot. The module will run the above defined states
    - **Uninitialized State**
    - **Opal Security State**
    - **ATA Security State**

The MICRON 1100 SSD does not support an unapproved mode of operation.

2 Cryptographic Functionality

The Module implements FIPS Approved cryptographic functions listed in the table(s) below.

Table 4 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption, Modes: ECB and CBC Key sizes: 256 bits Note: ECB and CBC were tested but is not used by the module	4111
DRBG	[SP 800-90A] Functions: CTR DRBG Security Strengths: 256 bits	1236
HMAC	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-256	2685
RSA*	[FIPS 186-4, PKCS #1 v2.1 (PKCS1.5) Functions: Signature Verification Key sizes: 2048	2224
SHA	[FIPS 180-4] Functions: Digital Signature Verification, Public Key validation, HMAC SHA sizes: SHA-256	3383
AES	[FIPS 197, SP 800-38A, SP 800-38E] Functions: Encryption, Decryption Modes: ECB, CBC, and XTS Key sizes: 256 bits Main Data path ME – Media Encryption/Decryption Engine Note: CBC was tested but is not used by the module	4051
AES	[FIPS 197, SP 800-38A, SP 800-38E] Functions: Encryption, Decryption Modes: ECB, CBC, and XTS Key sizes: 256 bits Auxiliary MRE – Media Re-Encryption/Decryption Engine Note: CBC was tested but is not used by the module	4052
Key Wrapping	[SP 800-38F] Modes: KW; Authenticated-Encryption & Authenticated-Decryption Functions: Key wrap, unwrap using AES 256 bit	4111

* Only used in Security Mode 1

Table 5 – Approved Cryptographic and Vendor Affirmed Functions

Algorithm	Description	IG Ref.
KDF, Password-Based	[SP 800-132] Options: PBKDF with Option 2B. Functions: HMAC-based KDF using, SHA-256 (CAVP Certified) Password length minimum is 10 bytes to 32 bytes. Salt 32 bytes DRBG Generated. Iteration Count – 100 Used to derive AK 0-27, which are only used in a storage application.	Vendor Affirmed IG D.6

Table 6 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
NDRNG	[Annex C] Hardware Non-Deterministic RNG; minimum of 16 bits per access. The NDRNG output is used to seed the FIPS Approved DRBG.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 3

Table 7 – Critical Security Parameters (used in all Security Modes)

CSP	Description / Usage
RKEK	Root Key Encryption Key (256 bits) 1. Data Integrity checking for PSPs and CSPs stored in nonvolatile memory. 2. Obfuscation of multiple DEKs when the associated range locking is not enabled. 3. Obfuscation of C-Blob (Credential Blob)
RDSKEY	Range data structure key. Key Wrap/Unwrap – AES 256 bit key used for maintaining the confidentiality and integrity of multiple DEKs by wrapping.
DEK 0	Data Encryption Keys for user ranges - AES-XTS 256 bit key, one unique key per range used to encrypt/decrypt user data
DEK 1-15	Data Encryption Keys for user ranges - AES-XTS 256 bit key, one unique key per range used to encrypt/decrypt user data
AK 0-27	Authentication Key – 256 bit key generated by a PBKDF. Used to verify the authentication.
Internal State	The V and Key values of the internal state of the DRBG.
Authority Password	Used to authenticate. This is an input to the PBKDF algorithm

2.2 Public Security Parameters

This section contains information on non-confidential security parameters such as public cryptographic keys

Table 8 – Public Keys (only used in Security Mode 1)

Key	Description / Usage
$K_{Firmware\_Verification}$	RSA 2048-bit Public Key used to verify download firmware images
$K_{vs\_Authentication}$	RSA 2048-bit Public Key used to authorize for MFG diagnostic capabilities (VS authentication)

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module supports two distinct operator roles, User and Crypto Officer (CO). The cryptographic Module enforces the separation of roles using password based authentication.

The table below lists all operator roles supported by the Module. The Module does not support a maintenance role and/or bypass capability. The roles supported by the Module are defined in the following table.

Table 9 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Crypto Officer – These roles relate only to the Opal Security State. **Drive owner** This role corresponds to the SID authority on the Admin SP. The [TCG-SSC-Opal] specification defines this authority. This role is responsible for transitioning from the uninitialized state to the Opal Security State of operation. 1. Locks/unlocks the Firmware Download port 2. Locks/unlocks the Diagnostics port **Admins 1-4** in Admin SP. This is equivalent to the named authority on the Admin SP as defined in the [TCG-SSC-Opal]. This role is disabled by default but can be enabled via SID. When enabled it can transition from the initialized to the uninitialized state **Admins 1-4** in locking SP (OPAL Security State. This is equivalent to the named authority on the locking SP as defined in the [TCG-SSC-Opal]. This role is used to enable and disable users, create and delete user data ranges, set the data range attributes, lock and unlock data ranges and erase data ranges with cryptographic erase service.	Role-based	PIN

Role ID	Role Description	Authentication Type	Authentication Data
User	**Users 1-16** – Opal Security State This role can unlock and lock the drive to allow the operator to read and write data to the drive. This user can also call the Cryptographic Erase service. In the Opal Security State there can be up to 16 different users (User IDs). This role corresponds to the same named TCG Authority on the Locking SP. They are defined in [TCG-SSC-Opal] specification. The Locking SP Admin role as defined above enables and disables users and assigns them read, write and erase access to user data ranges. **ATA-User** - ATA Security State This role can unlock and lock the drive to allow the operator to read and write data to the drive. This user can also call the Cryptographic Erase service **ATA-Master** - ATA Security State This role corresponds to the same named role as defined in the ATA specification [ATA-8 ACS]. This role only provides a backup authentication to the ATA User and does not have access to administration services beyond those of the ATA User role.	Role based	PIN
FWD	Firmware Download: This is an assumed role based on the Firmware download operation. The role is assumed when the FW download operation is invoked and is active for the lifetime of the operation. The signature of the image is used as the authentication data.	Role based	RSA 2048 bit RSA Signature

Role ID	Role Description	Authentication Type	Authentication Data
VSA	VS Authentication: This is an assumed role which enables the module to accept Micron manufacturing specific commands This role can only be assumed by Micron	Role based	RSA 2048bit Signature
Unauthenticated	This is a role which does not require authentication. Limited services are provided, show status, reset etc.	Unauthenticated	N/A

3.2 Authentication Methods

All operator authentication is role and password based. Each authority has their unique password.

3.2.1 Authentication Data Personalization in Opal Security State

All Crypto Officer & User passwords are delivered from Micron with a default password. The initial value of SID is created during manufacturing and is called MSID. This is a 32byte public value. All other authority passwords are set to NULL (32 bytes zeros). To personalize the password, the authority must open a TCG session, authenticate with default password, and then modify (TCG Set) the new password.

3.2.2 Authentication Data Personalization in ATA Security State

To personalize the passwords, the user sets the password for ATA user and master authorities [ATA-8 ACS]. Depending on a parameter of the ATA Set Password service for the User password, the User services may or may not be fully extended to the Master role. If the Master Password Capability is set to “High”, then either role can access the same services. Otherwise the Master role only has access to the erase service.

3.2.3 Operator Authentication Description

Authentication method description and strength is illustrated in the following table. Operator PINS are converted to an internal representation of the PIN using PBKDF.

3.2.4 FWD and VSA Authentication in all states.

The FWD and VSA roles are assumed when the relevant operation (FW download or enable enhanced VS commands) is initiated.

For the firmware download process, the FWD role is assumed when the operation is initiated. This role is authenticated verifying the signature image. Signature images are verified by the device using RSA2048 signature verification. FW image signatures can only be generated by Micron.

To enable enhanced VS command mode, the VSA role is assumed when the commands are required. This role is authenticated verifying the signature image. Signature images are verified by the device using RSA2048 signature verification. This role can only be authenticated by Micron and is restricted.

Table 10 – Operator Authentication Description

Authentication Method	Probability	Justification
Password (PIN) based authentication for CO and User roles.	Minimum PIN length is 10 bytes with a maximum length of 32 bytes.	The probability of guessing a PIN in a single attempt with a 10 character password is 1/2^80 in a single random attempt. This easily meets the FIPS 140 authentication strength requirements of less than 1/1,000,000. Each authentication attempt takes greater than 31ms on average to complete. This means that about ((60*1000)/31) = 1936 attempts can be made in one minute. This is about 1936/2^80. This is significantly lower than the FIPS requirement of 1/100,000. Each PIN has associated retry limit of 5. This controls the number of unsuccessful attempts before authentication is blocked until a module reset occurs. **Opal Security State** In this state TCG Start Session or Authenticate Methods are provided by TCG for authentication by the Operator. The operator ID and associated PIN will be provided in the Start Session or Authenticate methods. The authentication will persist for that session as long as it is active. TCG also provides for the "Anybody" Authority. This authority does not have a private credential and can perform unauthenticated services **ATA Security State** In this state Master and User authentication is provided through a password provided as a parameter to the ATA Security Unlock Command [ATA-8 ACS].
FIPS 140-2 CMVP (RSA2048). Authenticates firmware download, and MFG VS authentication.	Key Length is 2048 bit, Key strength is equal to 112 bits.	RSA 2048 has a key strength of 112 bits, which is the minimum approved by CMVP. This effectively eliminates the possibility of determining the private key through exhaustive methods. Each verification takes 172ms. Limiting it to less than 6 attempts per second.

3.3 Services

All services implemented by the Module are listed in the table(s) in this section which describes the modes within which they can be used. Each service description also describes the operator roles involved along with the interface command associated with the service. Services are only valid when operating in those modes which they are defined. The Module provides a mechanism to clear CSPs by allowing the user to revert to the uninitialized state of operation through the revert service. All of these services are provided in Security mode 0 and Security mode 1.

Table 11 – Authenticated Services For All Operating State (Uninitialized, Opal, ATA)

Service	Description	CO	U	FWD	VSA	Mechanism
Firmware Download port lock/unlock	Disallows/Allows firmware Download (Default unlocked)	X				TCG Set Method
Firmware Download	Download to new version of firmware			X		DOWNLOAD MICROCODE*
Diagnostics port lock/unlock	Disallows/Allows MFG VS commands (Default unlocked)	X				TCG Set Method
Zeroize	Manufacturing can zerioze all CSP. RKEK is programmed to all 1's.				X	MFG VS command**
Enhanced VS mode enable	Enable enhanced VS Commands				X	MFG VS command**

* Firmware download port must be unlocked. Transition to Security Mode 1.

** Diagnostics port must be unlocked and VS command authentication completed successfully. Transition to Security Mode 1.

3.3.1 Uninitialized State services

Table 12 – Authenticated Services for Uninitialized State

Service	Description	CO	U	Mechanism
Take Ownership	See Security initialization	X		TCG Activate Method MSID is used to authenticate the 1st time

Table 13 – Unauthenticated Services for Uninitialized State

Service	Description	Mechanism
ATA Set Password	Enter the ATA Security state of operation	ATA SECURITY SET PASSWORD

Service	Description	Mechanism
User Data Write / Read	Encryption / Decryption of user data to / from the drive	ATA Write and Read
Sanitize operation*	ATA sanitize operation as specified in ATA Spec.	ATA SANITIZE Operation

*The Sanitize Device feature set allows hosts to request that devices modify the content of all user data areas in the device in a way that results in previously existing data in these areas becoming unreadable. Sanitize operations [ATA-8 ACS] are initiated using one of the sanitize operation commands.

3.3.2 Opal Security State Services

Table 14 – Authenticated Services for OPAL Security State

Service	Description	CO	U	Mechanism
Crypto Erase	Erase user data in an LBA range by cryptographic means: Changing the encryption key	X	X	TCG GenKey Method
Set PIN	Set Password which changes the operator authentication credential. Note: Locking SP admins can set PINs for any User or Locking SP Admin	X	X	TCG Set Method
Enable/Disable an Admin or User Authority	Enable/Disable an Admin for Admin SP or Admin for Locking SP or a User Authority	X		TCG Set Method
Update a Range	Set start LBA, end LBA, Locking and User access rights of the range	X		TCG Set Method
Lock/Unlock a Range	Block or allow read (decrypt) / write (encrypt) of user data in a range	X	X	TCG Set Method
User Data Write / Read	Encryption / Decryption of user data to / from a user data range	*	*	ATA Read/Write Commands
Return to uninitialized state	Disable Admin and locking Authorities and Erase user data in an LBA range by cryptographic means: zeroizing and changing the encryption key.	X		TCG AdminSPObj.Revert TCG LockingSPObj. RevertSP

* Range must be unlocked

3.3.3 Unauthenticated Services for Opal Security State

The following unauthenticated roles are defined as Initialized for Opal Security State of operation:

Table 15 – Unauthenticated Services for Opal Security State

Service	Description	Mechanism
Show Status	Get information about the operational state of the drive	TCG Level 0 discovery
Reset	Causes power on self-tests	Power cycle
FIPS 140 Compliance Descriptor	Reports overall FIPS 140 Revision, Security Level, Hardware and Firmware versions and Module Name	Trusted Receive Protocol ID 0, ComID: 2
Generate random number	Returns a SP800-90 DRBG Random number of 256 bits	TCG_Random Method
Return to uninitialized state	Use public PSID to return drive to manufactured uninitialized state. All DEK's zeroized and regenerated. PINs set to default	AdminSPObj.Revert()

3.3.4 Authenticated services for ATA Security State

Table 16 – Authenticated Services for ATA Security State

Service	Description	CO	U	Mechanism
Crypto Erase (Return to uninitialized state)	Erase user data by cryptographic means: Changing the encryption key.		X	ATA SECURITY ERASE PREARE + ATA SECURITY ERASE UNIT
Set PIN	Set Password which changes the operator authentication credential. Setting User PIN also sets Drive Owner PIN		X	ATA SECURITY SET PASSWORD
User Data Encrypt/Decrypt	Encryption / Decryption of user data		X	ATA READ/WRITE
Unlock ATA Security	Enable user data Write / Read and set PIN services		X	ATA SECURITY UNLOCK
Return to uninitialized state	Exit ATA Security State		X	ATA SECURITY DISABLE PASSWORD

3.3.5 Unauthenticated services for ATA Security State

Table 17 – Unauthenticated Services for ATA Security State

Service	Description	Mechanism
Status	Get information about the operational state of the drive	ATA IDENTIFY DEVICE (WORD 128 BIT 1==1)

Service	Description	Mechanism
Reset	Causes power on self-tests	Power cycle
Disable ATA Security Services	Disable ATA Security commands until Reset. Security has to be unlocked.	ATA SECURITY FREEZE LOCK*
FIPS 140 Compliance Descriptor	Reports overall FIPS 140 Revision, Security Level, Hardware and Firmware versions and Module Name	Trusted Receive Protocol ID 0, ComID: 2

*The SECURITY FREEZE LOCK command sets the device to frozen mode. Frozen mode is disabled by a power-off or a hardware reset.

Table 18 table below defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The Module generates the CSP.
- R = Read: The Module reads the CSP. The read access is typically performed before the module uses the CSP.
- E = Execute: The Module executes using the CSP.
- W = Write: The Module writes the CSP. The write access is typically performed after a CSP is imported into the Module, when the Module generates a CSP, or when the Module overwrites an existing CSP.
- Z = Zeroize: The Module zeroizes the CSP.

Table 18 – CSP Access Rights within Services

Service	CSPs						
	RKEK	DEK 0	DEK 1-15	RDSKEY	Internal State[4]	AK 0-27	Password[4]
Take Ownership (OPAL)	R,E						
Firmware Download port lock/unlock	R,E						
Firmware Download	R,E						
Diagnostics port lock/unlock	R,E						
Zeroize	Z,G	Z,G	Z	Z,G	R,E	Z,G	E
Enhanced VS mode enable	R,E						

Service	CSPs						
	RKEK	DEK 0	DEK 1-15	RDSKEY	Internal State[4]	AK 0-27	Password[4]
Crypto Erase	R,E	Z,G	Z,G	R,E	R, E		E
Set PIN	R,E			R		G, E	E
Enable/Disable an Admin or User Authority	R,E						
Update a Range	R, E	G[1], Z[2]	G[1], Z[2]				
Lock/Unlock a Range	R, E	R	R	R,E			
User Data Write / Read		R,E[3]	R,E[3]				
Return to uninitialized state	R, E	Z,G	Z,G	Z,G	R,E	G,E	E
ATA Set Password	R,E			R		G, E	E
Unlock ATA Security	R,E	R		R,E		G,E	E
Sanitize operation**	R,E	Z,G					
Status							
Reset	R, E	R[3]	R[3]				
Generate random number					R,E		
Disable ATA Security Services **							
FIPS 140 Compliance Descriptor							

[1] Create a Range

[2] Delete a Range

[3] Range has to be unlocked (OPAL, ATA)

** Drive has to be unlocked (ATA)

[4] Stored in volatile memory and zeroized with removal of power.

4 Self-Tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self–tests are available on demand by power cycling the module. They are performed without user interruption when the device is power-cycled. In addition they are also executed when the module transitions from Security mode 0 to Security mode 1.

On power up or reset, the Module performs self-tests described in Table 19 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the self-test error state.

Table 19 – Self-Tests

Test Target	When Executed	Description	Failure Behavior
Firmware Integrity	Power-On	32 bit CRC performed over ROM code in the ASIC 32 bit CRC performed over Bootloader Firmware 32 bit CRC performed over Main firmware	Firmware Integrity Failure State
ASIC AES MRE	Power-On/ Entering Security Mode 1	KATs: Encryption, Decryption Modes: ECB, XTS Key sizes: 256bits	Enter Self-Test Error state
ASIC AES ME	Power-On/ Entering Security Mode 1	KATs: Encryption, Decryption Modes: ECB Key sizes: 128bits	Enter Self-Test Error state
DRBG	Power-On/ Entering Security Mode 1/When DRBG reseeded	KATs: Per NIST Special Publication 800-90A Revision 1 SP 800-90A Section 11.3 Health Checks	Enter Self-Test Error state
HMAC- SHA-256	Power-On/ Entering Security Mode 1	KATs: HMAC Verification Mode: HMAC-SHA256 SHA sizes:, SHA-256,	Enter Self-Test Error state
RSA 2048bit	Entering Security Mode 1	RSA 2048 signature verification KAT performed when Security Mode 1 is entered.	Firmware Download aborts or VS authentication aborts Enter Self-Test Error state
RNG	Conditional: When a random number is generated	New random number is compared to the previously generated random number, test fails if they are equal.	Enter Self-Test Error state
Firmware Load Check	Conditional: When a Microcode download command is received	RSA 2048 signature verification (PKCS#1) of new firmware image before loading it.	Reject the firmware download command and discard the new image

5 Physical Security

5.1 MICRON 1100 2.5" form factor physical security

The MICRON 1100 2.5" form factor module is a multi-chip embedded device. The Module includes the following physical security mechanisms:

1. Opaque two piece enclosure. The physical enclosure functions as the security boundary of the module. The only components exposed are the SATA Data and Power ports. The module does not support a maintenance access interface.
2. Two (2) tamper evident labels positioned as indicated in the following image.

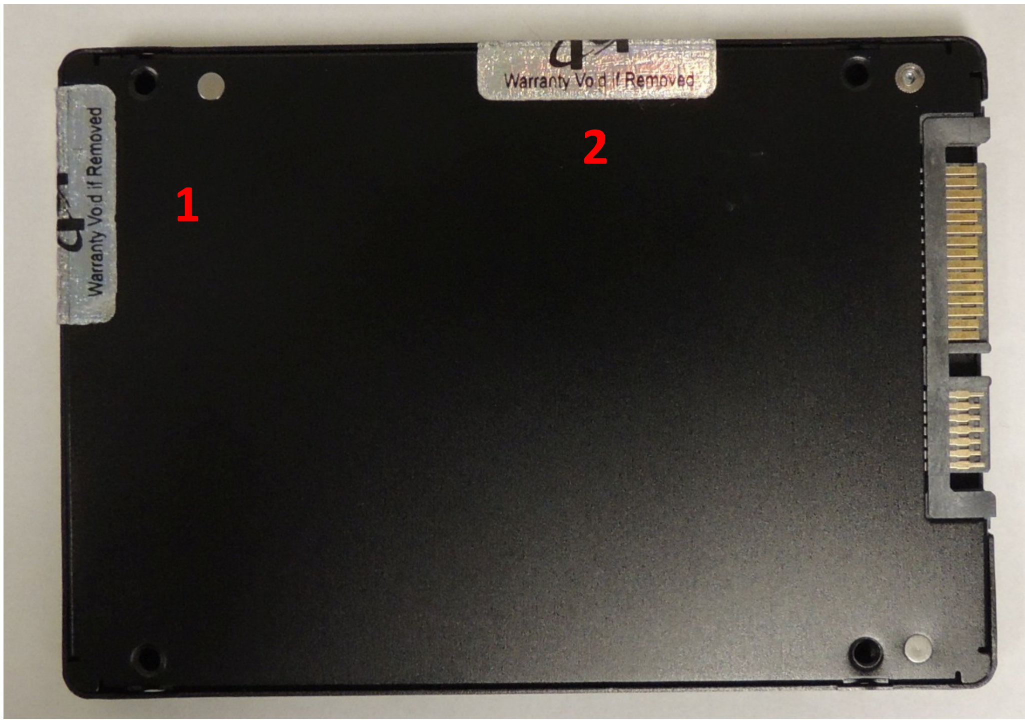

Figure 4 – MICRON 1100 2.5 inch Form Factor Physical Security Tamper-Evident Label Placement

The two (2) labels are required to ensure the detection tamper attempt. They are applied by Micron during the manufacturing process. These labels cannot be removed and/or reapplied without tamper evidence. The labels are pictured in the following figure.

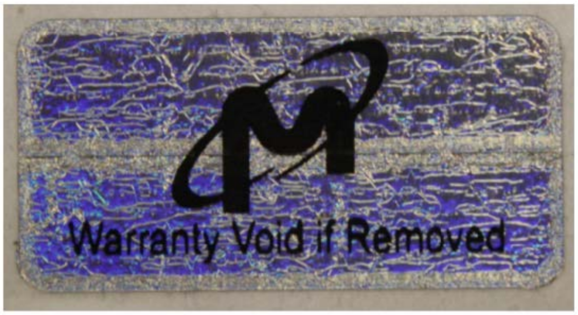

Figure 5 – MICRON 1100 2.5" Tamper-Evident Label

The Module should be examined at regular intervals for evidence according to the following guidance. In all cases of evidence of tampering being detected, the device should be removed from service.

Table 20 – MICRON 1100 2.5" Form factor Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Physical enclosure	On initial receipt of the device and periodically afterwards.	Inspect for evidence of prying or removal • Bending of enclosure • Removal of TE label
Tamper Evident Seals	On initial receipt of the device and when feasible afterwards.	Inspect labels for evidence of a removal attempt. In all cases the label will not be able to be reapplied. • Peeling – will result in a residue on the enclosure and/or an inability to reapply the label • Solvent – will result in the TE label being physically disfigured • Temperature based will result in the TS label being disfigured

Examples of tamper evidence are provided in the following diagrams

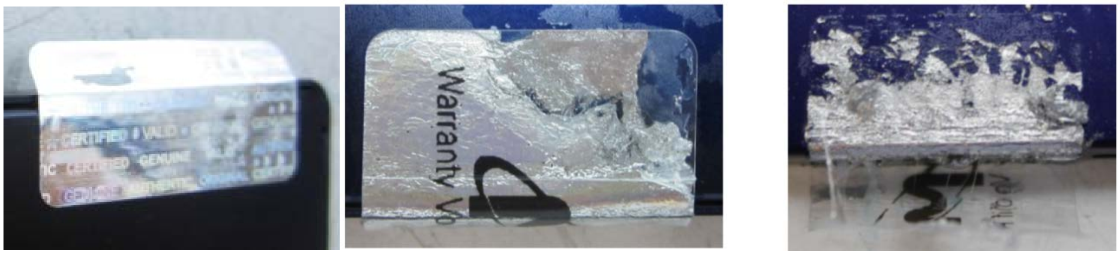

Figure 6 – MICRON 1100 2.5" Tamper Evidence

5.2 MICRON 1100 M.2 form factor physical security

The MICRON 1100 M.2 form factor module is a multi-chip embedded device. The Module includes the following physical security mechanisms:

1. The Module is surrounded by an opaque epoxy which is applied by Micron during the manufacturing process. This coating functions as the physical security boundary of the device. The only components exposed are the SATA Data and Power ports. The module does not support a maintenance access interface.   This is illustrated in the following figure:

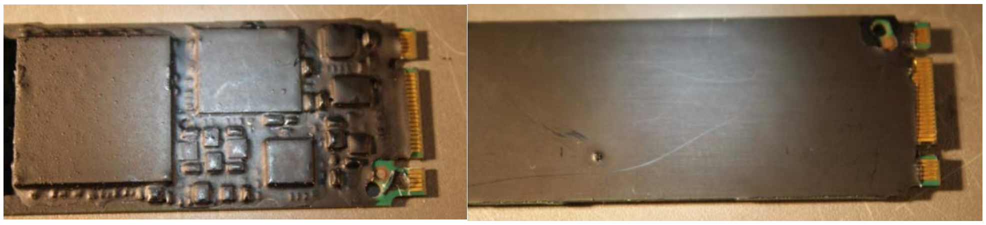

Figure 7 – MICRON 1100 M.2 Form Factor Epoxy Coating-Top and Bottom

The Module should be examined at regular intervals for evidence according to the following guidance:

Table 21 – MICRON 1100 M.2   Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Opaque packaging	On initial receipt of the device and when feasible afterwards.	Check packaging for attempts to remove the epoxy coating. • Inspect for cuts, gouges etc.

In all cases of evidence of tampering being detected, the device should be removed from service.

Evidence of tampering is provided in the following diagrams.

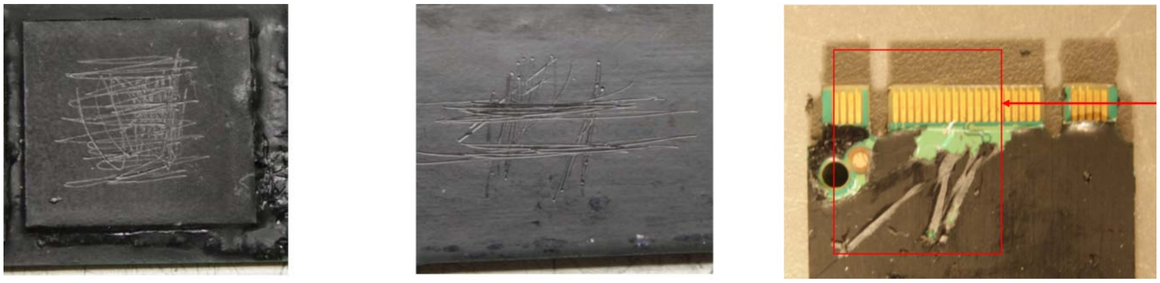

Figure 8 – MICRON 1100 M.2 Tamper Evidence

6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes an authenticated firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP.

7 Mitigation of Other Attacks Policy

The Module has not been designed to mitigate attacks outside of the scope of FIPS 140-2. This area is noted as not being applicable.

8 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

8.1 Operational Rules for the User/Operator

1. The Module does not support concurrent operators.
2. In OPAL Security State a security rule is that the host must not authenticate to more than one operator (TCG authority) in a session. To clear the authentication the session must close or the Module must be power cycled.
3. In OPAL Security State set all ReadLockEnabled and WriteLockEnabled to “TRUE” for all created ranges. The default state is “FALSE”.

8.2 Operational Guidance for the Device

1. Requires the operator to be authenticated before having access to any cryptographic service other than those outlined in Roles, Authentication and Services
2. The operator is capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.

3. At installation set all operator PINs applicable for the Security State to private values of at least 10 bytes in length.
4. All module owner generated keys or CSPs are zeroized by the zeroization service.
    a. RKEK zeroization requires return to MFG and VS Authentication
5. The Module enforces a maximum authentication attempt before a reset is required to continue. After 5 consecutive unsuccessful Password validation attempts have occurred, the module shall require a power cycle before any more authentication attempts are allowed.

8.3 Operational Behavior of the Device

1. The Module provides two distinct operator roles: User and Cryptographic Officer.
2. The Module clears previous authentications on power cycle.
3. Data output is inhibited during key generation, self-tests, zeroization, and error states.
4. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
5. The Module does not support a maintenance interface or role.
6. The Module does not support manual key entry.
7. The Module does not output plaintext CSPs
8. The Module does not output intermediate key values.
9. The Module does not support the update of the logical serial number or vendor ID.
10. The Module does not provide access to internal data structures while plaintext CSPs are present.
11. The Module supports a maximum of 16 individual users.
12. In an OPAL Security State TCG Session, if the Module remains inactive in any valid role for a maximum period of 4 minutes, the Module automatically logs out the session.

8.4 Security initialization

The device is shipped from the factory in an approved mode of operation (Security mode 0 – uninitialized state). The keys generated during manufacturing are used to encrypt/decrypt data. On receipt of the module the CO should examine the product to ensure it has not been tampered with during shipping according to the procedures outline in the module Physical Security Policy section. Upon verification that the module has not been tampered, the user should initialize the drive into either the OPAL Security State or the ATA Security State. No direct transition is allowed between the Opal and ATA security states. In order to transition from one state to another the Module must revert to the original uninitialized state. The operations to initialize the Module and transition between states is summarized below

1. Verifying the Module is in an approved mode of operation

To verify that a module is in the Approved mode of operation the operator will perform the following tasks

1. Perform get FIPS security compliance descriptor by issuing a TCG Trusted Receive.
    a. See [ACS-3] in the Reference section

2. **Initializing the device to Opal Security State**
    a. Issue activate method on locking SP
    b. Set PINs for all operators to private values of at least 10 bytes in length but recommended length is 32 bytes. These operators include admins, Drive owners and users.
    c. Set range locking values.
    d. Perform a power cycle.
3. **Returning to uninitialized state from the Opal Security State**
    a. The TCG revert or Revert SP methods may be invoked by an authenticated role to effect a transition into the uninitialized state of operation. This is analogous to restoring the MICRON 1100 SSD Module to a factory default state.
4. **Initializing the device to ATA Security State**
    a. Set PINs for master and user to private values of at least 10 bytes in length.
    b. Perform a power cycle.
5. **Returning to uninitialized state from the ATA Security State**
    a. Issue the ATA security Disable Password or ATA security Erase command.

The Master password can be changed at this time if required.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 22 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[TCG-SSC-Opal]	TCG Storage Security Subsystem Class: Opal, Specification v2.00 Revision 1.00
[TCG-SACS]	TCG Storage Architecture Core Specification Version 2.00 Revision 2.00
[TCG-SIIS]	TCG Storage Interface Interactions Specification v1.0
[ATA-8 ACS]	STA=8 ACS-3
[SATA]	Serial ATA Rev 2.6
[ACS-3]	ACS-3 Reporting Security Compliance December 1,2009

Table 23 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
AK	Authentication Key
CO	Cryptographic Officer
CSP	Critical Security Parameter
DEK	Data Encryption Key
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book mode of AES encryption/decryption
CBC	Cipher Block Chaining mode of AES encryption/decryption
KAT	Known Answer Test
KDF	Key Derivation Function
LBA	Logical Block Address
MSID	Manufactured SID, Public value that is used as default PIN
PBKDF	Password Based Key Derivation Function
PSID	Physical SID, a public unique value for each drive
PSP	Public Security Parameter
RDSKEY	Range Data Structure Key
RSA	Rivest Shamir Adleman
SATA	Serial Advanced Technology Attachment
SED	Self-Encrypting Drive
SHA	Secure Hashing Algorithm

Acronym	Definition
SID	Security ID, PIN for Drive Owner CO Role - TCG OPAL
TCG	Trusted Computing Group
XTS	A mode of AES