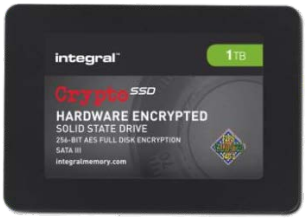
Integral AES 256 Bit Crypto SSD Underlying PCB



Integral Memory PLC.

FIPS 140-2 non-Proprietary Security Policy

Module Document Version: 1.4

Table of Contents

Table of Contents

Figures & Tables

1. Introduction

1.1. Purpose

This is a non-proprietary FIPS 140-2 Security Policy for the Integral AES 256 Bit Crypto SSD Underlying PCB Cryptographic Modules. It describes how these modules meet all requirements as specified for FIPS 140-2, Security Level 3. This policy forms a part of the submission package to the security testing (Lightship Security) Testing Laboratory.

FIPS 140-2 (Federal Information Processing Standard Publication, 140-2) specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections. For more information about the standard, visit:

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

1.2. References

This Security Policy describes how this module complies with the eleven sections of FIPS 140-2:

- For more information on the FIPS 140-2 standard and CMVP please refer to the NIST website at http://csrc.nist.gov/groups/STM/cmvp/index.html
- For more information about Integral Memory Solutions please visit www.integralmemory.com/crypto/

1.3. Document History

Author(s)	Version	Date	Comment
Patrick Warley	1.4	26/06/2020	Draft Copy

2. Cryptographic Module Description

2.1. The Integral AES 256 Bit Crypto SSD Underlying PCB

The Integral AES 256 Bit Crypto SSD Underlying PCB is an internal storage device which has mandatory encryption for all data including the operating system. The Integral 256 Bit Crypto SSD Underlying PCB comes in, 128GB, 256GB, 512GB 1TB 2TB 4TB versions SATA 2.5" SATA M.2 2280 NVMe M.2280. The devices feature many security enhancements including an epoxy resin coating around both the circuit components and the printed circuit board (PCB).

The devices require an operating system to be installed to operate the encryption program which must be in a desktop or laptop computer with Microsoft Windows® or Linux operating system. The encryption program SSDLock can be run from the Desktop or from the USB Drive that is supplied with the Crypto SSD. With this you will be able to run a software package (called SSDLock) directly. The software GUI has a people friendly interface that makes using the drive simple and easy but does not compromise security.

The encryption is carried out using AES (256 bit in XTS and CBC mode). It also supports identity based authentication with a strong user password containing a minimum of 8 and a maximum of 16 characters. The password must contain both upper and lower case letters, and include at least one numeric and special character. For further protection the Integral 256 Bit Crypto SSD allows minimum of 8 a maximum of 20 incorrect password attempts depending on how the drive is configured in setup in both user and Admin Mode before destroying all data on the device. This protects against brute force attacks on the drive.

The Integral 256 Bit Crypto SSD Underlying PCB has a Multi-Lingual interface in 13 languages.

2.2. Cryptographic Module Specification

The modules are multi-chip embedded cryptographic hardware module as defined by FIPS PUB 140-2, and meet the overall requirements applicable to Level 3. The cryptographic boundary for the modules (demonstrated by the red line in ***Figure 1***) which contains all integrated circuits. All components of the module are production grade and the module is opaque within the visible spectrum. The modules execute proprietary non-modifiable firmware.

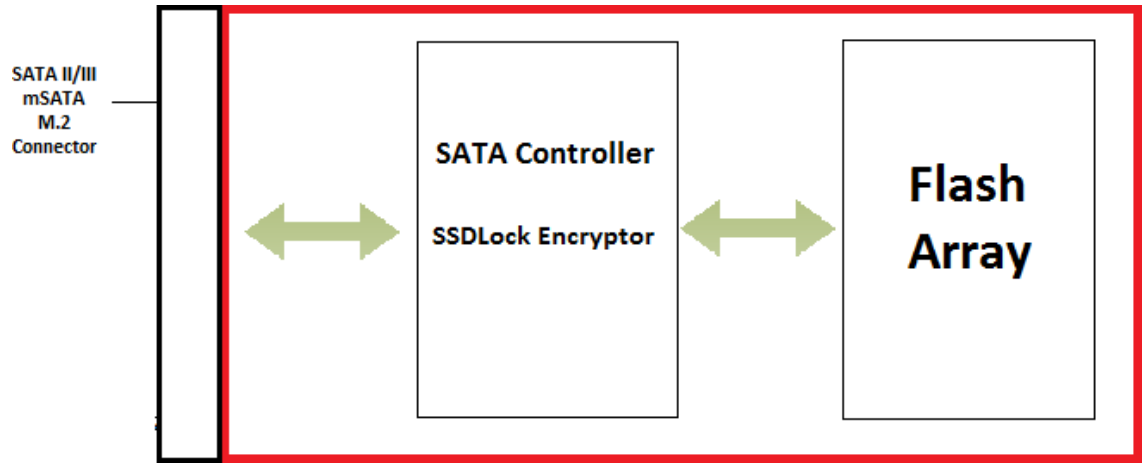


Figure 1 – Cryptographic Module Block Diagram

2.3. Module Compliance to FIPS 140-2 Sections

The Integral AES 256 Bit Crypto SSD Underlying PCB modules conform to the following Sections of FIPS 140-2:

Section	***Level***
1. Cryptographic Module Specification	3
2. Cryptographic Module Ports and Interfaces	3
3. Roles, Services, and Authentication	3
4. Finite State Model	3
5. Physical Security	3
6. Operational Environment	N/A
7. Cryptographic Key Management	3
8. EMI/EMC	3
9. Self-Tests	3
10. Design Assurance	3
11. Mitigation of Other Attacks	N/A
Overall Level	3

Table 1 - FIPS 140-2 Sections

2.4. Tested Modules

The modules which have been tested are listed in ***Table 2***. The Integral AES 256 Bit Crypto SSD Underlying PCB executes in a non-modifiable proprietary operational environment. Every module specified in the following table can contain either an E12 or S12 processor. Modules that have the same interfaces are visually indistinguishable from each other as they only differ in memory size.

Model	***Hardware Version***	***Firmware Version***	***Memory Option***	***Visual Representation***
2.5” SATA III	INSSD128GS625C140	SCPJ13.0	128GB	See Figure 2
2.5” SATA III	INSSD256GS625C140	SCPJ13.0	256\GB	
2.5” SATA III	INSSD512GS625C140	SCPJ13.0	512GB	
2.5” SATA III	INSSD1TS625C140	SCPJ13.0	1TB	
2.5” SATA III	INSSD2TS625C140	SCPJ13.0	2TB	
2.5” SATA III	INSSD4TS625C140	SCPJ13.0	4TB	
M.2 2280 SATA III	INSSD128GM280C140	SCPJ13.0	128GB	See Figure 3
M.2 2280 SATA III	INSSD256GM280C140	SCPJ13.0	256GB	
M.2 2280 SATA III	INSSD512GM280C140	SCPJ13.0	512GB	

Model	Hardware Version	Firmware Version	Memory Option	Visual Representation
M.2 2280 SATA III	INSSD1TM280C140	SCPJ13.0	2TB	
M.2 2280 SATA III	INSSD2TM280C140	SCPJ13.0	2TB	
M.2 2280 SATA III	INSSD4TM280C140	SCPJ13.0	4TB	
M.2 2280 MVMe	INSSD128GM280NC140	SCPJ13.0	128GB	
M.2 2280 MVMe	INSSD256GM280NC140	SCPJ13.0	256GB	
M.2 2280 MVMe	INSSD512GM280NC140	SCPJ13.0	512GB	
M.2 2280 MVMe	INSSD1TM280NC140	SCPJ13.0	1TB	See Figure 4
M.2 2280 MVMe	INSSD2TM280NC140	SCPJ13.0	2TB	
M.2 2280 MVMe	INSSD4TM280NC140	SCPJ13.0	4TB	

Table 2 - Tested modules

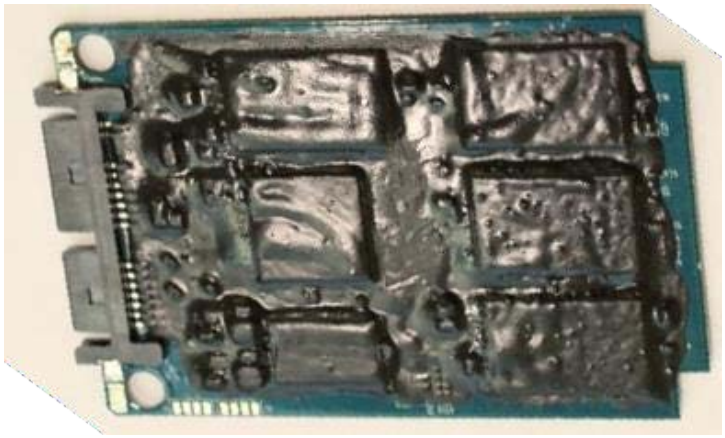


Figure 2 – 2.5" SATA Models

Pin	Signal Name	Signal Description	FIPS 140-2 Logical Interface
1	GND	Ground	
2	A+	A+ (Differential Signal Pair A)	Data Output, Data Input, Control Input Status Output
3	A-	A- (Differential Signal Pair A)	Data Output, Data Input, Control Input Status Output
4	GND	Ground	
5	B-	B- (Differential Signal Pair B)	Data Output, Data Input, Control Input Status Output
6	B+	B+ (Differential Signal Pair B)	Data Output, Data Input, Control Input Status Output
7	GND		

Pin	Signal Names	Signal Description	FIPS 140-2 Logical Interface
8	V33	3.3v Power	Power Pin
9	V33	3.3v Power	Power Pin
10		Status Output Data Input	
11	Ground	1st Mate	
12	Ground	2nd Mate	
13	Ground	3rd Mate	
14	V5	5v pre-charge	Power Pin
15	V5	5v Power	Power Pin
16	V5	5v Power	Power Pin
17	Ground		
18	DAS1	Tolerated input Voltage (max)3.3V	
19	Ground		
20	V12	12v Power, Pre-charge	
21	V12	12v Not Used	
22	V12	12v Not Used	

Table 3 Pin out SATA 2.5

Figure 3 – M.2 2280 SATA Models

Pin	Signal Names	Signal Description	FIPS 140-2 Logical Interface
1	CONFIG_3	Ground	
2	3.3V	Supply pin	Power Pin Input
3	GND	Ground	
4	3.3V	Supply pin	Power Pin Input
5	N/C	No Connect	
6	N/C	No Connect	
7	N/C	No Connect	
8	N/C	No Connect	
9	N/C or GND Note	No Connect or Ground	
10	DAS/DSS# (O) (OD)	Status indicators via LED devices that will be provided by the system Active Low. A pulled-up LED with series current limiting resistor should allow for 9mA when On.	
11	N/C	No Connect	
12	Module Key		

13	Module Key		
14	Module Key		
15	Module Key		
16	Module Key		
17	Module Key		
18	Module Key		
19	Module Key		
20	N/C	No Connect	
21	CONFIG_0	Ground	
22	N/C	No Connect	
23	N/C	No Connect	
24	N/C	No Connect	
25	N/C	No Connect	
26	N/C	No Connect	
27	GND	Ground	
28	N/C	No Connect	
29	N/C	No Connect	
30	N/C	No Connect	
31	N/C	No Connect	
32	N/C	No Connect	
33	GND	Ground	
34	N/C	No Connect	
35	N/C	No Connect	
36	N/C	No Connect	
37	N/C	No Connect	
38	DEVSLP (I)	Device Sleep, Input. When driven high the host is informing the SSD to enter a low power state	
39	GND	Ground	
40	N/C	No Connect	
41	SATA-B+	SATA differential signals in the SATA specification	Data Input, Data Output, Control Input, Status Output
42	N/C	No Connect	
43	SATA-B-	SATA differential signals in the SATA specification	Data Input, Data Output, Control Input, Status Output
44	N/C	No Connect	

45	GND	Ground	
46	N/C	No Connect	
47	SATA-A-	SATA differential signals in the SATA specification	Data Input, Data Output, Control Input, Status Output
48	N/C	No Connect	
49	SATA-A+	SATA differential signals in the SATA specification	Data Input, Data Output, Control Input, Status Output
50	N/C	No Connect	
51	GND	Ground	
52	N/C	No Connect	
53	N/C	No Connect	
54	N/C	No Connect	
55	N/C	No Connect	
56	Reserved for MFG Data	No Connect	
57	GND	Ground	
58	Reserved for MFG Clock	No Connect	
59	Module Key		
60	Module Key		
61	Module Key		
62	Module Key		
63	Module Key		
64	Module Key		
65	Module Key		
66	Module Key		
67	N/C	No Connect	
68	SUSCLK (I) (0/3.3V)	No Connect	
69	CONFIG_1	Ground	
70	3.3V	Supply pin	Power Pin Input
71	GND	Ground	
72	3.3V	Supply pin	Power Pin Input
73	GND	Ground	
74	3.3V	Supply pin	Power Pin Input
75	CONFIG_2	Ground	

Table 4 - Pin out SATA M.2 2280

Figure 4 – M.2 2280 MVMe Models

Pin No.	PCIe Pin	Description	FIPS 140-2 Logical Interface
1	GND	CONFIG_3 = GND	
2	3.3V	3.3V source	Power Pin Input
3	GND	Ground	
4	3.3V	3.3V source	Power Pin Input
5	PETn3	PCIe TX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
6	N/C	No connect	
7	PETp3	PCIe TX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
8	N/C	No connect	
9	GND	Ground	
10	LED1#	Open drain, active low signal. These signals are used to allow the add-in card to provide status indicators via LED devices that will be provided by the system.	
11	PERn3	PCIe RX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
12	3.3V	3.3V source	
13	PERp3	PCIe RX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
14	3.3V	3.3V source	Power Pin

15	GND	Ground	
16	3.3V	3.3V source	Power Pin
17	PETn2	PCIe TX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
18	3.3V	3.3V source	
19	PETp2	PCIe TX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
20	N/C	No connect	
21	GND	Ground	
22	N/C	No connect	
23	PERn2	PCIe RX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
24	N/C	No connect	
25	PERp2	PCIe RX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
26	N/C	No connect	
27	GND	Ground	
28	N/C	No connect	
29	PETn1	PCIe TX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
30	N/C	No connect	
31	PETp1	PCIe TX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
32	N/C	No connect	
33	GND	Ground	
34	N/C	No connect	
35	PERn1	PCIe RX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
36	N/C	No connect	
37	PERp1	PCIe RX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output

38	N/C	No connect	
39	GND	Ground	
40	SMB_CLK (I/O)(0/1.8V)	SMBus Clock; Open Drain with pull-up on platform	
41	PETn0	PCIe TX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
42	SMB_DATA (I/O)(0/1.8V)	SMBus Data; Open Drain with pull-up on platform.	
43	PETp0	PCIe TX Differential signal defined by the PCI Express M.2 spec	
44	ALERT#(O) (0/1.8V)	Alert notification to master; Open Drain with pull-up on platform; Active low.	
45	GND	Ground	
46	N/C	No connect	
47	PERn0	PCIe RX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
48	N/C	No connect	
49	PERp0	PCIe RX Differential signal defined by the PCI Express M.2 spec	Data Input, Data Output, Control Input, Status Output
50	PERST#(I)(0/3.3V)	PE-Reset is a functional reset to the card as defined by the PCIe Mini CEM specification.	
51	GND	Ground	
52	CLKREQ#(I/O)(0/3.3V)	Clock Request is a reference clock request signal as defined by the PCIe Mini CEM specification; Also used by L1 PM Sub-states.	
53	REFCLKn	PCIe Reference Clock signals (100 MHz) defined by the PCI Express M.2 spec.	
54	PEWAKE#(I/O)(0/3.3V)	PCIe PME Wake. Open Drain with pull up on platform; Active Low.	
55	REFCLKp	PCIe Reference Clock signals (100 MHz) defined by the PCI Express M.2 spec.	
56	Reserved for MFG DATA	Manufacturing Data line. Used for SSD manufacturing only. Not used in normal operation. Pins should be left N/C in platform Socket.	

57	GND	Ground	
58	Reserved for MFG CLOCK	Manufacturing Clock line. Used for SSD manufacturing only. Not used in normal operation. Pins should be left N/C in platform Socket.	
59	Module Key M	Module Key	
60	Module Key M		
61	Module Key M		
62	Module Key M		
63	Module Key M		
64	Module Key M		
65	Module Key M		
66	Module Key M		
67	N/C	No connect	
68	SUSCLK(32KHz) (I)(0/3.3V)	32.768 kHz clock supply input that is provided by the platform chipset to reduce power and cost for the module.	
69	N/C	PEDET (NC-PCIe)	
70	3.3V	3.3V source	Power Pin Input
71	GND	Ground	
72	3.3V	3.3V source	Power Pin Input
73	GND	Ground	
74	3.3V	3.3V source	Power Pin Input
75	GND	Ground	

Table 5 - Pin Out M.2 2280 NVMe

3. Approved Mode of Operation

3.1. FIPS Approved Mode

The modules only operate in the Approved mode of operation, meaning no configuration exists whereby the modules can operate in a non-Approved mode. The instructions to securely configure and initialize the modules into the Approved mode are as follows:

1. Install the Integral AES 256 Bit Crypto SSD into the host computer or laptop.

2. Install the Windows 10 or Linux Operating System.

3. Run the SSDLock software.

4. Enter language.

5. Create a password 8-16 Characters long for the master.

6. Create a password 8-16 characters long for the user.

7. Choose how many login attempts allowed up to 20.

8. Re start the Computer or Laptop run and if completed.

9. Crypto Runs Self Tests this happens each time the drive is powered up now running in FIPS approved Mode.

10. Enter Password for the User or Master Account.

11. The module will confirm that the Approved mode has been entered by presenting the operator with the login prompt and that the menu is visible when drive is unlocked.

3.2. Crypto Officer and User Guidance

In order to ensure compliance with best security practices, the following rules ***shall*** be observed when operating the module in the Approved mode unless otherwise indicated:

- The Crypto Officer ***shall*** inspect the packaging after taking delivery of the module for any signs of tampering. The module ***shall*** be sent back if there is any evidence the module may have been tampered with during shipping.
- Usernames and passwords ***shall*** be uniquely assigned and not shared between operators.
- The Crypto-Officer ***shall*** periodically inspect the module as instructed in Section Physical Security of this document.
- The Crypto-Officer ***shall*** retain the correct password. If the password is not successful up to a maximum after 20 attempts, all keys, CSPs and user data will be zeroized.
- It is recommended that Crypto Officers and users meet the maximum password length of 16 characters rather than the minimum 8 character password length when configuring passwords.

4. Module Ports & Interfaces

This section maps the FIPS 140-2 logical interfaces to the module's physical interface as follows:

- Data Input logical Interface maps to the physical SATA and NVMe data cable interface of the module.
- Data Output logical interface maps to the physical SATA and NVMe data cable interface of the module.
- Control Input logical interface maps to the physical SATA and NVMe data cable interface of the

module.

- Status output logical interface maps to the physical SATA and NVMe data cable interface of the module.
- The module contains a power interface which maps to the physical SATA and NVMe power cable interface of the module. This interface requires power from the host hardware platform.

***NOTE:** All four FIPS 140-2 logical interfaces map to the SATA 2.5" SATA M.2 2280 and NVMe M.2 2280 interface of each module listed in Table 3, 4, and 5.

5. Roles, Services & Authentication

The modules support the following two roles:

1) Crypto Officer role:
   This role is also referred to as the 'Master' role. This is the role assumed by an operator to perform cryptographic initialization, management functions, and cryptographic operations.

2) User role:
   This is the role assumed by an operator to perform general security services, including cryptographic operations.

The modules implement identity-based authentication comprised of a username and password combination. The Crypto Officer role and the User role are explicitly assumed by the operator by successfully authenticating to the module using the correct username and password combination.

5.1. Identification & Authentication

The authentication methods employed by the module are described here in **Table** . After 20 unsuccessful authentication attempts the module zeroizes all Keys, CSPs and data.

Role	Authentication (User name and Password combination)	Auth. Strength	Multi-Attempt in 60 sec. Strength
Crypto Officer (Master)	Passwords must meet each of the following requirements: • 8 to 16 characters in length • 1 upper case alphabetical character • 1 lower case alphabetical character • 1 numeric character • 1 special character	Probability of a random attempt succeeding is: 1 in (94^8) = 1 in 6,095,689,385,410,816	Probability of random attempts during a one minute period succeeding are: : 1 in (94^8)/20 = 1 in 304,784,469,270,540

User	Passwords must meet each of the following requirements: • 8 to 16 characters in length • 1 upper case alphabetical character • 1 lower case alphabetical character • 1 numeric character • 1 special character	Probability of a random attempt succeeding is: 1 in (94^8) = 1 in 6,095,689,385,410,816	Probability of random attempts during a one minute period succeeding are: : 1 in (94^8)/20 = 1 in 304,784,469,270,540

Table 6 - Roles & Authentication Methods

5.2. Roles & Services

The services that are available to operators are listed in **Table**. The table specifies the authorized services by the operator roles and identifies the Cryptographic Keys and CSPs associated with the services. The modes of access are also identified per the explanation.

Legend

N/A – The service is not associated with a key or CSP
DEK – Data Encryption Key
Password – Operator Password
Seed – Random seed consumed by NIST SP 800-90A DRBG

R - The item is **read** or referenced by the service.
W - The item is **written** or updated by the service.
E - The item is **executed** by the service. (The item is used as part of a cryptographic function.)

	Service	Roles	Keys & CSPs	RWE
1	**Self-Test**	Crypto-Officer & User	N/A	E
2	**Authenticate**	Crypto-Officer & User	Password	W, E
3	**Create & Change Password**	Crypto-Officer	Password	W, E
4	**Password Reset**	Crypto-Officer	Password	W, E
5	**Delete User**	Crypto-Officer	Password	
6	**Lock**	Crypto-Officer User	N/A	E
7	**Show Status**	Crypto-Officer User	N/A	R
8	**Key Generation**	Crypto-Officer User	DEK, DRBG V, DRBG Key	W, E
9	**Encrypt/Decrypt**	Crypto-Officer User	DEK	W, E

10	**Hash**	Crypto-Officer User	N/A	W
11	**Reset (Zeroize)**	Crypto-Officer User	DEK, DRBG V, DRBG Key, Password	W, E
12	**Logout**	Crypto-Officer User	N/A	E
13	**AES Key Wrap**	Crypto-Officer User	DEK, KEK	E

Table 7 - Roles & Services

NOTE : In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133 (vendor affirmed) Section 4, scenario 1 for symmetric key . The approved random number generator is located within the physical boundary of the cryptographic module. The DRBG is executed in the controller (S12 and E12), which is inside of the physical boundary.

6. Physical Security

6.1. Physical Security Mechanisms

The modules are contained within a removable metal chassis for the 2.5" SATA Drive however; the cryptographic boundary for the modules is defined as the outer surface of the epoxy resin which covers the module's PCB board, electronic components, and circuitry. The modules' physical boundaries do not include the steel chassis for the M.2 2280 SATA and the M.2 2280 NVMe. The modules are comprised of off-the-shelf production grade components that include standard passivation. The modules are opaque within the visible spectrum and do not have any removable covers, openings, or doors. In the event that the hard coating protecting the PCB is breached to the depth of the underlying circuitry, the module will cease to function completely. The module should be replaced immediately if any type of damage is witnessed.

It is the responsibility of the Crypto-Officer to periodically inspect the module for tamper evidence. This requires the removal of the outer metal chassis to be able to inspect the epoxy resin to ensure that it has not been breached and does not show and signs of attempted tampering.

To inspect the module, the Crypto Officer shall perform the following at a frequency of at least once every six months:

- Remove the (4) standard Phillips screws from the metal casing on the 2.5' SATA SSD in which the module ships, With the M.2 2280 SATA and MVME drives the outer shell of epoxy coating.

- Closely inspect the epoxy resin coating for any evidence of tamper (evidence includes chipping, and/or scraping, and/or drilling of the epoxy resin coating)

If the Crypto Officer discovers tamper evidence during a physical inspection of the module the following action ***shall*** be taken:

- Zeroize all keys and CSPs
- Return the module to Integral Memory. The module must be replaced.

The module hardness testing was only performed at room temperature and no assurance is provided for Level 3 hardness conformance at any other temperature.

7. Operational Environment

The Integral AES 256 Bit Crypto SSD Underlying PCBs S5FDM018 firmware provides a limited a proprietary, non-modifiable operational environment.

8. Key Management & Cryptographic Algorithms

8.1. Cryptographic Keys and CSPs

The module does not allow for the input or output of any keys, key components, or CSPs. The table below outlines the cryptographic keys, Key components, and CSPs used by the modules.

Key/CSP	Type	Service	Generation	Zeroization	Storage
Data Encryption/Decryption Key	XTS-AES-256	7, 9, and 10	SP800-90A HMAC-DRBG	Reset command or exceeding password attempt threshold	Encrypted by Key Encryption Key and stored in NAND. Plaintext in DRAM
AES CBC Key	AES CBC-256	7,9, and 10	Generated during manufacturing baked into firmware	Reset command or exceeding password attempts threshold	Plaintext in DRAM
User Key Encryption Key	AES Key Wrap 256	9	SP800-90A HMAC-DRBG	Reset command or exceeding password attempts threshold	Encrypted by user password based key with AES key Wrap 256 and Stored in NAND Plaintext
KEK	AES Key Wrap 256	9 and 10	SP800-132 PBKDF2	Reset command or exceeding password attempts threshold	Plaintext in DRAM
Admin/User Password	16 bytes – 32 bytes	9 and 10	Default Password Configuration	Reset command or exceeding password attempts threshold	Hashed (SHA-512) and stored in NAND
RSA Code Sign Public Key	RSA-2048	8 and 11	N/A (HSM)	Reset command or exceeding password attempts threshold	Public Key Stored With FW code
Seed Material (Entropy input and Nonce of SP800-90A	SP800-90A DRBG Entropy Input is 32 bytes Nonce is 16 Bytes	8 and 11	HW RNG (TRNG)	Reset command or exceeding password attempts threshold	Plaintext in DRAM
HMAC DRBG Seed	DRBG Seed	8 and 11	Initialized with DRBG	Reset command or exceeding password attempts threshold	Plaintext in Dram
Internal State (V and Key) of SP800 90A	SP800-90A DRBG Entropy Input is 32 Bytes	8 and 11	Initialized with DRBG instantiation	Reset command or exceeding password attempts threshold	Plaintext in Dram
HMAC SHA-256 Key	HMAC SHA 256 Key	8	Generated internally	Reset command or exceeding password attempts threshold	Plaintext in Dram

Table 8 - Keys and CSP's

NOTE: PBKDF (NIST SP 800-132) Option 2a (vendor affirmed) Section 4 scenario 1 Password/passphrase length used in key derivation: 8 bytes ~ 136 bytes. The PRF used is HMAC-SHA-256 with its hash digest size being 256bits. The Iteration count uses 1024 Bits and the Salt Length uses 256 Bits.

8.2. Cryptographic Algorithms

Algorithm	CAVP Algorithm Certificate	Implemented In	Key Length	Algorithm Usage
Advanced Encryption Standard (AES) 256-bit in CBC mode	C1688	Hardware	256 bits	Prerequisite
Advanced Encryption Standard (AES) 256-bit in XTS mode	C1688	Hardware	256 bits	Encryption/Decryption
AES Key Wrap	C1688	Hardware	256 bits	Key Wrapping
HMAC-SHA-256	C1687	Firmware	256 bits	Deriving Keys for Storage Application
SHA-256	C1688	Hardware	N/A	Prerequisite
SHA-512	C1688	Hardware	N/A	Password Protection
NIST SP 800-90A HMAC_DRBG	C1687	Firmware	N/A	Deterministic Random Bit Generation
RSA PKCSPSS SigVer 2048 with SHA2-256	C1688	Hardware	2048 bits	Digital Signature Verification
PBKDF	Vendor Affirmed	Firmware	256 bits	Deriving Keys for Storage Application
CKG	Vendor Affirmed	Firmware	N/A	Cryptographic Key Generation

Table 9 - Approved Algorithm Certificates

Algorithm	CAVP Algorithm Certificate	Implemented In	Key Length	Algorithm Usage
NDRNG	N/A	Hardware	N/A	Seed of DRBG (256bit)

Table 10 – Non-Approved but allowed Algorithms

9. Self Tests

9.1. Power Up Self-Tests

The modules perform the following power-up self-tests after power has been applied to the module. Once power has been applied the power-up self-tests will execute automatically without any intervention from the operator:

- Firmware Integrity Test using 2048-bit RSA Signature Verification
- AES CBC Encrypt KAT
- AES CBC Decrypt KAT
- SHA-256 KAT
- SHA-512 KAT
- DRBG KAT
- HMAC SHA-256 KAT
- AES XTS Encrypt KAT
- AES XTS Decrypt KAT
- AES Wrap KAT
- AES Unwrap KAT

9.2. Conditional Tests

The modules perform the following conditional tests as required:

- DRBG continuous Test
- NDRNG continuous Test
- RSA Signature Verification Test

9.3. Critical Function Tests

- DRBG Instantiate KAT
- DRBG Generate KAT
- DRBG reseed KAT

9.4. Self-Test Failure

If *any* self-test fails the module will transition into the error state and an error message will output via the status output interface (message will be displayed on-screen). While in the error state the modules' data input, data output, and control input interfaces are disabled and as a result data output is inhibited while the module is in the error state. Additionally all cryptographic operations are Inhibited from taking place while the module in the error state. The operator can attempt to clear the error by power cycling the host PC with the module connected. Should the module encounter another error during the subsequent power-up self-tests then the error is considered to be unrecoverable. The module should be replaced in this circumstance.

10. Design Assurance

10.1. Secure Delivery

When the module is shipped to the customer, a bonded courier is used. The Crypto-Officer is advised to check the packaging when accepting delivery of the module and to send it back if there is any evidence of tampering. All boxes have warranty Seals and are also sealed with a Tamper proof stickers on all box's and internal packaging. Shipments from the factory to the warehouse and made by Secure Bonded transport. Once delivered shipments are placed in a safe witch is locked and entry controlled Storage.

10.2. Configuration Management

Each version of each configuration item for both the cryptographic module and associated documentation is assigned and labeled with a unique identification number by Integral Memory and placed in secure document management.

11. Mitigation of Other Attacks

The modules do not claim mitigation of other attacks.