Integral Memory PLC.

Integral AES 256 Bit Crypto SSD
Underlying PCB
FIPS 140-2 Security Policy

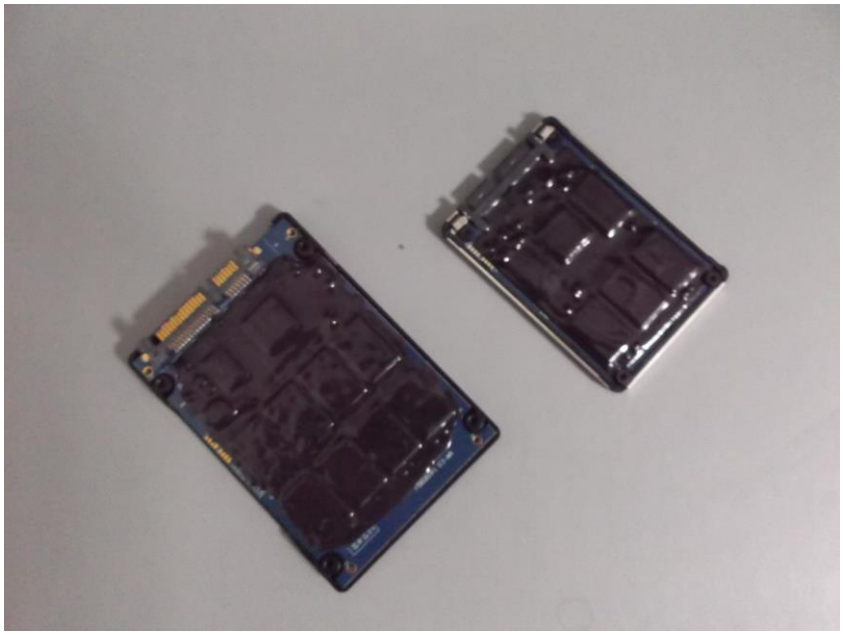


Table of Contents

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 module. It describes how this module meets all the requirements as specified in the FIPS 140-2 Level 2 requirements. This Policy forms a part of the submission package to the testing lab.

FIPS 140-2 (Federal Information Processing Standards 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 the Standard:

- For more information on the FIPS 140-2 standard and validation program 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 http://www.integralmemory.com/industrial-storage/encrypted-ssd/25-sata-encrypted-ssd-0

1.3 Document History

Author(s)	Date	Version	Comment
Patrick Warley	February 11th 2014	1.0	FIPS Submission Draft

2. PRODUCT DESCRIPTION

The Integral AES 256 Bit Crypto SSD Underlying PCB is an internal storage device which has mandatory encryption for all data, which includes the operating system. The Integral 256 Bit Crypto SSD Underlying PCB comes in 32 GB, 64 GB, 128 GB, 256 GB, 512 GB and 1 TB versions. The devices feature many security enhancements, a steel outer shell and an epoxy resin coating around both the circuit components and the printed circuit board (PCB). The module implements AES, XTS, in FIPS Approved Mode.

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® 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 & AES 128 bit in XTS Mode). It also supports identity based authentication with a strong user password of at least 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 a maximum of 20 incorrect password attempts in user or 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.

2.1 Cryptographic Module Specification

The Integral AES 256 Bit Crypto SSD Underlying PCB module is a multi-chip standalone implementation of a cryptographic module as defined by FIPS PUB 140-2. The product meets the overall requirements applicable to Level 2 security for FIPS 140-2, Physical security meeting level 2, with roles services and authentication, EMI/EMC and Design Assurance meeting the Level 3 requirements. The Integral AES Crypto SSD Underlying PCB comes in two options: 2.5” and 1.8” SATA II & SATA III.

The Cryptographic Boundary for the Integral AES 256 Bit Crypto SSD Underlying PCB (the red line in Figure 1) is defined as all components within the epoxy resin. All components are coated in epoxy and encased in a SSD enclosure. The epoxy resin contains integrated circuit packaging that is production grade and opaque within the visible spectrum. No hardware or firmware components of the module are excluded from the requirements of FIPS 140-2, however the casing around the module is outside the cryptographic boundary.

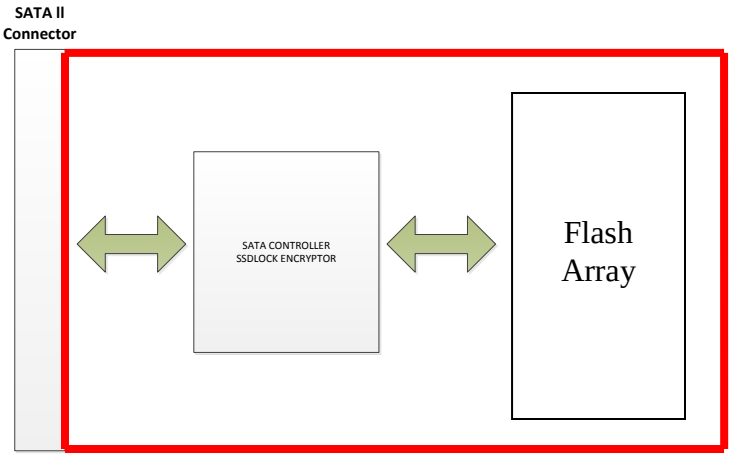


Figure 1 - Module Block Diagram

The Integral AES 256 Bit Crypto SSD Underlying PCB which are being submitted for validation include:

Model	*Hardware Versions*	*Crypto Processor*	*Memory Option*	*Firmware Version*
2.5″ SATAII & III	INSSD32GS25MCR140-2(R)	PS3105 or PS3108	32GB	S5FDM018
2.5″ SATAII & III	INSSD64GS25MCR140-2(R)	PS3105 or PS3108	64GB	S5FDM018
2.5″ SATAII & III	INSSD128GS25MCR140-2(R)	PS3105 or PS3108	128GB	S5FDM018
2.5″ SATAII & III	INSSD256GS25MCR140-2(R)	PS3105 or PS3108	256GB	S5FDM018
2.5″ SATAII & III	INSSD512GS25MCR140-2(R)	PS3105 or PS3108	512GB	S5FDM018
2.5″ SATAII & III	INSSD1TS25MCR140-2(R)	PS3105 or PS3108	1T	S5FDM018
1.8″ SATA II & III	INSSD32GS18MCR140-2(R)	PS3105 or PS3108	32GB	S5FDM018
1.8″ SATA II & III	INSSD64GS18MCR140-2(R)	PS3105 or PS3108	64GB	S5FDM018
1.8″ SATA II & III	INSSD128GS18MCR140-2(R)	PS3105 or PS3108	128GB	S5FDM018
1.8″ SATA II & III	INSSD256GS18MCR140-2(R)	PS3105 or PS3108	256GB	S5FDM018
1.8″ SATA II & III	INSSD512GS18MCR140-2(R)	PS3105 or PS3108	512GB	S5FDM018
1.8″ SATA II & III	INSSD1TGS18MCR140-2(R)	PS3105 or PS3108	1T	S5FDM018

Table 1 - Module Validation Table

Security Requirements Section	*Level*
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles and Services and Authentication	3
Finite State Machine Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	2
Overall Level of Certification	2

Table 2 - Module Compliance Table

3 MODULE PORTS AND INTERFACES

3.1 Physical Interface Description

The Integral AES 256 Bit Crypto SSD Underlying PCB 2.5” SATA II & III Interface.

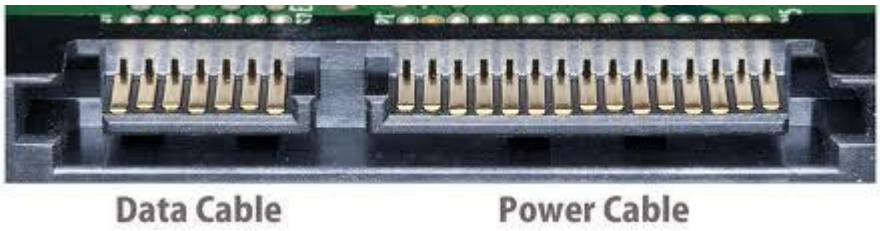
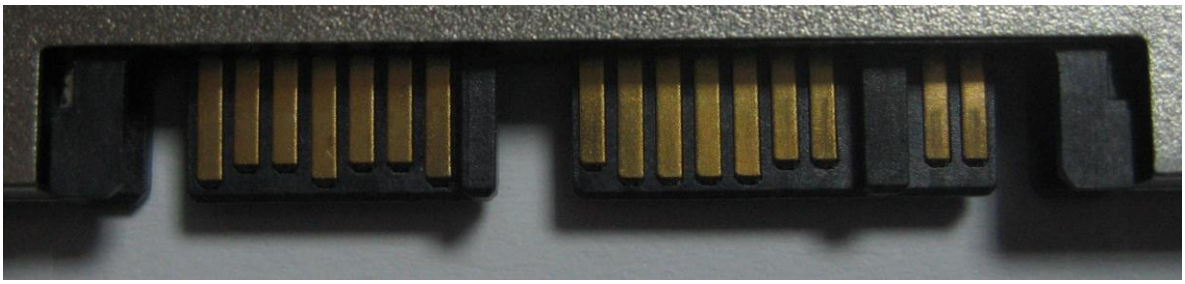


Figure 2 - Functional Specifications of PIN

SATA PinOut, Data			**Logical Mapping**
Pin #	**Signal Name**	**Signal Description**	
1	GND	Ground	N/A
2	A+	Transmit +	Plaintext Data, Ciphertext, Control Input, Status Output
3	A-	Transmit -	
4	GND	Ground	N/A
5	B-	Receive -	Plaintext Data, Ciphertext, Control Input, Status Output
6	B+	Receive +	
7	GND	Ground	N/A

SATA PinOut, Power		
Pin #	**Signal Name**	**Signal Description**
1	V33	3.3v Power
2	V33	3.3v Power
3	V33	3.3v Power, Pre-charge, 2nd mate
4	Ground	1st Mate
5	Ground	2nd Mate
6	Ground	3rd Mate
7	V5	5v Power, pre-charge, 2nd mate
8	V5	5v Power
9	V5	5v Power
10	Ground	2nd Mate
11	Reserved	-
12	Ground	1st Mate
13	V12	12v Power, Pre-charge, 2nd mate
14	V12	12v Power
15	V12	12v Power

The Integral AES 256 Bit Crypto SSD Underlying PCB 1.8” SATA II & III Interface.



Data

SATA PinOut, Data			**Logical Mapping**
Pin #	**Signal Name**	**Signal Description**	
1	GND	Ground	N/A
2	A+	Transmit +	Plaintext Data, Ciphertext, Control Input, Status Output
3	A-	Transmit -	
4	GND	Ground	N/A
5	B-	Receive -	Plaintext Data, Ciphertext, Control Input, Status Output
6	B+	Receive +	
7	GND	Ground	N/A

Power

SATA PinOut, Power		
Pin #	**Signal Name**	**Signal Description**
1	V33	3.3v Power
2	V33	3.3v Power
3	GND	1st mate
4		1st mate
5	V5	5v Power, pre-charge, 2nd mate
6	V5	5V power
7	Reserved	
8	Reserved	Activity indicator (3.3V, active low)
9	Reserved	

4. ROLES AND SERVICES

AUTHENTICATION

The Integral 256 Bit Crypto SSD supports a Crypto-Officer (Master), and a User role that are explicitly assumed by the Crypto-Officer. The module implements Identity-based authentication using a unique user ID and password. The module doesn’t support a maintenance role.

4.1 Identification and Authentication

Describe here the type of authentication mechanisms implemented.

Role	*Type of Authentication*	*Authentication Data*	*Strength of Authentication*
User	Identity Based	Minimum 8 to 16 alpha/numeric & Special Character password	Passwords are required to be at least 8 to 16 characters long. With a minimum password of 8 alpha/numeric characters, the probability of guessing this is 1 in 8!x52x10x32x94[5]
Crypto Officer	Identity Based	Minimum 8 to 16 alpha/numeric & special character password	Passwords are required to be at least 8 to 16 characters long. With a minimum password of 8 alpha/numeric characters, the probability of guessing this is 1 in 8!x52x10x32x94[5]

Table 3 - Authentication Type Table

4.2 Roles and Services

The Integral AES 256 Bit Crypto SSD supports the services listed in the following table. The table groups 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.

- **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.)

The two following tables show the services available to each of the two roles:

Role	*Authorized Services*	*Key/CSP*	*Access Type*
Crypto-Officer	Self-Test	N/A	Execute
	Authenticate	Password	Write, Execute
	Create & Change Password	Password	Write Execute
	Password Reset	Password	Write Execute
	Delete user	Password	Execute
	Lock	N/A	Execute
	Show Status	N/A	Read
	Key Generation	DEK, (Data Encryption Key) DRBG V DRBG C	Write, Execute
	Encrypt/Decrypt	DEK	Write/Execute
	Hash	N/A	Write
	Reset (Zeroize)	DEK, DRBG V DRBG C, Password	Write, Execute
	Logout	N/A	Execute

Table 5 - Cryptographic Officer (Master) – Roles and Services

Role	*Authorized Services*	*Key/CSP*	*Access Type*
User	Self-Test	N/A	Execute
	Authenticate	Password	Write, Execute
	Lock	N/A	Execute
	Show Status	N/A	Read
	Key Generation	DEK, DRBG V DRBG C	Write, Execute
	Encrypt/Decrypt	DEK	Write/Execute
	Hash	N/A	Write
	Reset (Zeroize)	DEK, DRBG V DRBG C Password	Write, Execute
	Logout	N/A	Execute

Table 6 - User – Roles and Services

5 PHYSICAL SECURITY

The cryptographic boundary for the Integral AES 256 Bit Crypto SSD Underlying PCB is defined as all components beneath and including epoxy resin coating. All components are coated in epoxy resin. The Integral AES 256 Bit Crypto SSD Underlying PCB does not have any removable doors or covers. The epoxy resin contains components with integrated circuit packaging that is production grade using standard passivation and is opaque within the visible spectrum. No hardware or firmware components of the module are excluded from the requirements of FIPS 140-2. The Crypto officer will have to devise a schedule to inspect the epoxy coating for damage or tampering using a standard phillips head screwdriver.

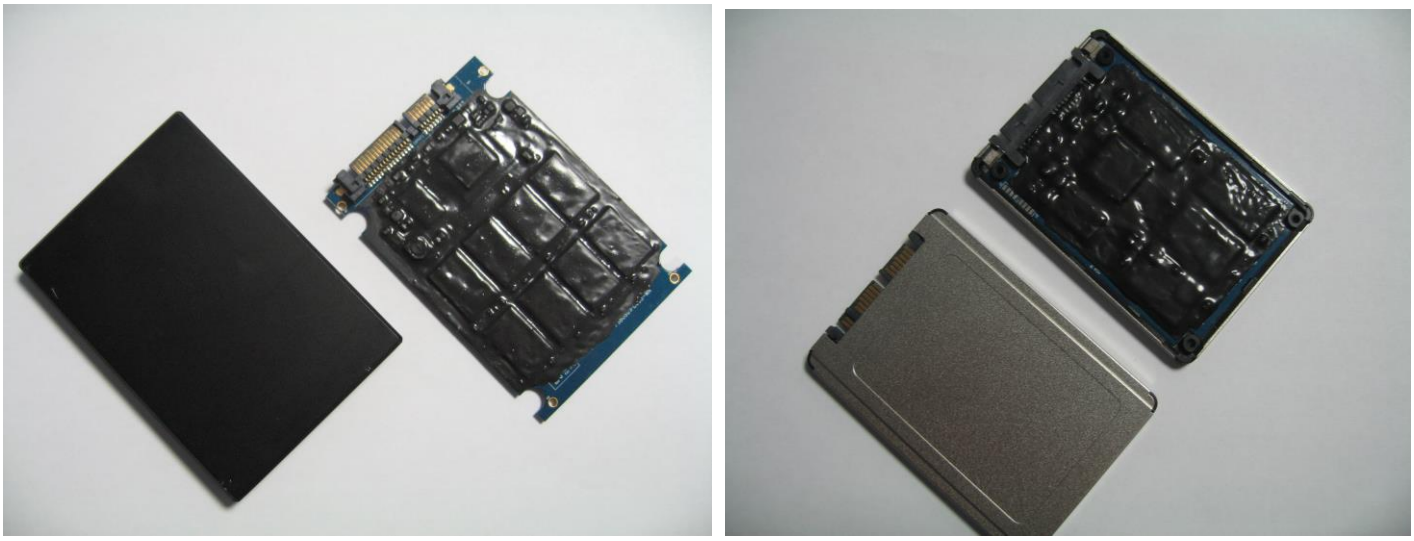


Figure-3

2.5” SATA 1.8” SATA

Figure 3 – Integral AES 256 bit Crypto SSD Underlying PCB (outside of its case)

5.1 EMI/EMC

The base cryptographic module has been tested by International Standards Labs, and found in compliance with the requirement of the following standards:

- FCC Part 15 : 2005 Subpart B, Class B.(Section 15.31,15.107 and 15.109;) and
- CISPR 22: 1997,Class B.(Section 5,6,9 and 10)

6 CRYPTOGRAPHIC KEY MANAGEMENT

The following table summaries the module's keys and CSPs:

Key/CSP	Generation	Storage	Zeroization	Use
Data Encryption Key (AES)	Generated internally using a PRNG & HMAC compliant to DRBG	Stored in Flash in plaintext	Reset Command Excessive Attempts	AES Data Encryption Key (DEK) used for data encryption and decryption.
Password	N/A	Stored in Flash, hashed	Reset Command Excessive Attempts	Authentication
Seed	H/W RNG	Stored in Volatile RAM	Reset Command Excessive Attempts	DRBG random number generation

Table 7 - Cryptographic Keys and CSPs

6.1 Key Entry / Key Output

The module does not input / output keys or CSPs.

6.2 Key Destruction

The Integral AES 256 Bit Crypto SSD Underlying PCB zeroize all keys and CSPs with the reset command or by failing a maximum of 20 password attempts in user or master accounts.

6.3 Algorithm Implementations

The module keys map to the following algorithms certificates:

Approved Security Function	*Certificate*
AES (H/W implementation) CBC (enc/dec; 256)	2175
XTS 128, XTS 256	2175
HMAC 256	1335
DRBG	254
SHA 256	1887

Table 8 - FIPS Approved Algorithms Table

7 SELF-TEST

The module performs the following self tests at power on:

Cryptographic Algorithm KATs:
Known Answer Tests (KATs) are run at power-up for:

- AES (XTS, CBC mode for Encrypt/Decrypt);
- SHA-256; and SHA-512
- DRBG
- HMAC SHA-256 and HMAC SHA-512

Firmware Integrity Tests:
The module checks the integrity of its components using SHA-512 at power up.

The module performs the following conditional self-tests:

- Continuous RNG Test for the DRBG RNG; and

If the Self test fails on the Integral AES 256 Bit Crypto SSD Underlying PCB it will not authenticate to the Host computer and will display an error. No operations are possible at this time as the interfaces are disabled. If this happens the only way to recover from the is to power down the Computer.

8 CRYPTO-OFFICER AND USER GUIDANCE

This section shall describe the configuration, maintenance, and administration of the cryptographic module.

8.1 Secure Setup and Initialization

The procedures to securely setup and initialize the Integral AES 256 bit Crypto SSD Underlying PCB include:

1. Install the Integral AES 256 Bit Crypto SSD into the host computer or laptop;
2. Install the Windows 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;
8. Re start the Computer or Laptop;
9. Enter Password for the User or Master Account.

8.2 Module Security Policy Rules

Security rules enforced by the cryptographic module to implement the security requirements of FIPS 140-2 Level 2 module includes:

1. Encrypting data using AES 256 (default setting).
2. Will include the setting of a minimum of 8 to 16 character password (this is default value and the operator cannot select any less than 8 characters.
3. The crypto officer must periodically inspect the Integral AES 256 Bit Crypto SSD Underlying PCB for signs of physical tampering to the epoxy resin coating.
4. The crypto officer MUST remember their password as there are only a maximum of 20 attempts. If the password is incorrect after 20 attempts the Integral AES 256 Bit SSD Underlying PCB will zeroize all keys, CSPs and user data including the operating system.
5. If the User forgets there password and uses up all of the set login attempts the User account will be locked and then user must go to the crypto office to have his password reset so allow access to the drive.

9 MITIGATION OF OTHER ATTACKS

The module does not mitigate against any specific attacks