Just Rams PLC.

Integral 256 bit AES Drive &
Integral 256 bit AES MAC Drive
FIPS 140-2 Security Policy

Table of Contents

INTRODUCTION

1.1 Purpose

This is a non-proprietary FIPS 140-2 Security Policy for the Integral 256 bit AES Drive & Integral 256 bit AES MAC Drive 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 validating 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/cavp/index.html
- For more information about Justrams/Integral Solutions please visit http://www.integralmemory.com/crypto/ .

1.3 Document History

Author(s)	Date	Version	Comment
Patrick Warley	March 31, 2010	1.0	FIPS Submission Draft
Patrick Warley	September 15, 2010	2.0	FIPS Submission Draft
Patrick Warley	October 4, 2010	3.0	FIPS Submission Draft

2 PRODUCT DESCRIPTION

The Integral AES 256 bit Drive & Integral 256 bit AES MAC Drive are removable storage devices which encrypt documents transferred onto them. The AES 256 bit Drive comes in 1GB, 2GB, 4GB, 8GB, 16GB and 32GB versions whereas the Integral 256 bit AES MAC Drive comes in 2GB, 4GB, 8GB, 16GB and 32GB versions. These devices feature many security enchantments, like a waterproof outer coating, steel inner coating, and an epoxy resin coating around the PCB. The module implements AES, SHS, and ANSI X9.31 RNG in FIPS Approved Mode.

The devices require no software installation and works by creating two partitions when attached to a PC. The first partition appears as a CD drive which runs a software package (called Total Lock) directly from the device. The second partition is the password protected data drive onto which files can be transferred. Data can only be accessed on this drive once the correct password is entered via the Total Lock software package. The CD drive is read only and no files can be transferred to this partition. It has a zero footprint that requires no software installation and a people friendly interface that makes using the drive simple and easy but does not compromise security.

The Integral 256 bit AES Drive & Integral 256 bit AES MAC Drive also has an optional function to add un-encrypted contact information to the device whilst keeping all other data secure. This allows lost devices to be returned to the correct owner. The contact information can only be changed during the setup or factory reset of the device; at which point any sensitive data being stored will automatically be destroyed.

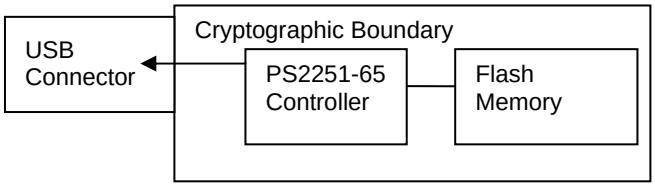
The Integral 256 bit AES Drive & Integral 256 bit AES MAC Drive has mandatory encryption for any data transferred onto it. The encryption is carried out using the AES-256 in CBC mode. It also supports identity based authentication with a strong user password of at least 8 and a maximum of 16 characters. The password must contain both upper and lower case letters, and include at least one numeric. For further protection the Integral 256 bit AES Drive & Integral 256 bit AES MAC Drive allows only 6 incorrect password attempts before destroying all data on the device. This protects against brute force attacks on the drive.

The Integral 256 bit AES USB Flash drive has a Multi-Lingual interface in 22 languages.

2.1 Cryptographic Module Specification

The Integral 256 bit AES Drive & Integral 256 bit AES MAC Drive 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 cryptographic boundary for the Integral 256 bit AES & Integral 256 bit AES MAC Drive is defined as all components within the steel enclosure. All components are coated in epoxy and encased in a steel enclosure with a rubber sleeve that provides waterproof protection only. The steel enclosure 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.



Cryptographic Boundary

The Integral 256 bit AES Drive & Integral 256 bit AES MAC Drives that are being submitted for validation include:

Module Name	*Memory Option*	Hardware Version	*Software Version*	*Firmware Version*
Integral 256bit AES Drive	1 GB	YFD1GBSPLCRYATV1INTL	4.00	PS2251-65
Integral 256bit AES Drive	2 GB	YFD2GBSPLCRYATV1INTL	4.00	PS2251-65
Integral 256bit AES Drive	4 GB	YFD4GBSPLCRYATV1INTL	4.00	PS2251-65
Integral 256bit AES Drive	8 GB	YFD8GBSPLCRYATV1INTL	4.00	PS2251-65
Integral 256bit AES Drive	16 GB	YFD16GSPLCRYATV1INTL	4.00	PS2251-65
Integral 256bit AES Drive	32 GB	YFD32GBCRYPTOINTL	4.00	PS2251-65
Integral 256bit AES MAC Drive	2 GB	YFD2GBCRYPTOMACINTL	4.00	PS2251-65
Integral 256bit AES MAC Drive	4 GB	YFD4GBCRYPTOMACINTL	4.00	PS2251-65
Integral 256bit AES MAC Drive	8 GB	YFD8GBCRYPTOMACINTL	4.00	PS2251-65
Integral 256bit AES MAC Drive	16 GB	YFD16GBCRYPTOMACINTL	4.00	PS2251-65
Integral 256bit AES MAC Drive	32 GB	YFD32GBCRYPTOMACINTL	4.00	PS2251-65

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 256 bit AES Drive supports four pins that lead to the PCB board.

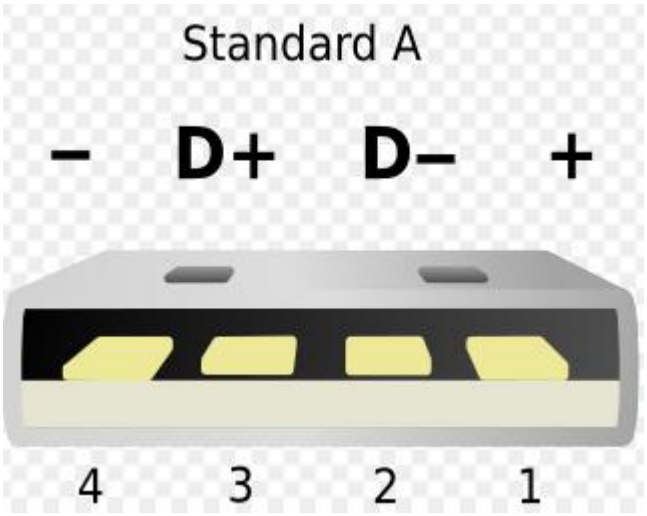


Figure 3 Functional Specifications of PIN

SPECIFIC FUNCTIONS OF USB CONTACTS

PIN	*Function*	*FIPS 140-2 Logical Interface*
USB 1	V^{BUS} supply voltage 4.75V – 5.25V	Power Interface
USB 2	Data +	Data Input, Data Output, Control Input, Status Output
USB 3	Data -	Data Input, Data Output, Control Input, Status Output
USB 4	Ground	N/A

Table 3 Functional Specifications of PIN.

LOGICAL INTERFACE DESCRIPTION

The I/O PIN (USB PIN 2 and 3) of the token (refer to Table 4) provides the following logical interfaces:

- Data In (I/O bidirectional line)
- Data Out (I/O bidirectional line)
- Control In (I/O bidirectional line)
- Status Out (I/O bidirectional line) and LED

4 ROLES, SERVICES AND AUTHENTICATION

The Integral 256 bit AES Drive and Integral 256 bit AES MAC Drive supports a Crypto-Officer 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 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 62^8 which is far greater than 1: 1,000,000 required for this standard.
Crypto Officer	Identity Based	Minimum 8 to 16 alpha/numeric 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 62^8 which is far greater than 1: 1,000,000 required for this standard.

Table 5 Authentication Type Table

4.2 Roles and Services

The Integral 256 bit AES Drive and Integral 256 bit AES MAC Drive 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 below table shows the services available to each role:

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

Table 6. Cryptographic Officer – Roles and Services

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

Table 7 User – Roles and Services

5 PHYSICAL SECURITY

The cryptographic boundary for the Integral 256 bit AES Drive and Integral 256 bit AES MAC Drive is defined as all components within the steel enclosure. All components are coated in epoxy and encased in a steel enclosure with a rubber sleeve that provides waterproof protection. The rubber sleeve is not part of the cryptographic boundary. Neither the Integral 256 bit AES Drive nor the Integral 256 bit AES MAC Drive has any removable doors or covers. The steel enclosure 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.

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 CSP's:

Key	Generation	Storage	Zeroization	Use
Data Encryption Key (AES)	Generated internally using a PRNG compliant to ANSI X9.31.	Stored in Flash in plaintext	Reset Command	AES Data Encryption Key (DEK) used for data encryption and decryption.
Password	N/A	Stored in Flash, hashed	Reset Command	Authentication
Seed Key	H/W RNG	Stored in Volatile RAM	Reset Command	ANSI X9.31 random number generation
Seed	H/W RNG	Stored in Volatile RAM	Reset Command	ANSI X9.31 random number generation

Table 8: Cryptographic Keys and CSPs

6.1 Key entry /Key Output

The module does not input / output keys or CSP's.

6.2 Key Destruction

The Integral 256 bit AES Drive & Integral 256 bit AES MAC Drive zeroizes all keys and CSP's with the reset command or by failing 6 password attempts.

6.3 Algorithm Implementations

The module keys map to the following algorithms certificates:

Approved Security Function	*Certificate*
AES (H/W implementation) CBC and ECB (enc/dec; 128 and 256)	1205
SHA-1 and SHA-256, byte-oriented	1108
ANSI X9.31 RNG (256 AES)	666

Table 9 FIPS Approved Algorithms Table

Non-Approved Security Function
RSA (512 bit modulus size)
H/W RNG for Seeding

Table 10 Non Approved Security Function

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 (CBC mode for Encrypt/Decrypt);
- SHA-1;
- SHA-256; and
- ANSI X9.31 RNG

Firmware Integrity Tests:
The module checks the integrity of its components using 16 bit CRC at power up.

The module performs the following conditional self-tests:

- Conditional RNG Test for the ANSI X9.31 RNG; and
- Conditional RNG test for the H/W RNG.

If the Self test fails on the Integral 256 bit AES Drive & Integral 256 bit AES MAC Drive 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 or pull the Integral 256 bit AES Drive & Integral 256 bit AES MAC Drive out of the host computer and reinsert.

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 256 bit AES Drive & Integral 256 bit AES MAC Drive include:

1. Plug the Integral AES 256 USB Flash drive to the host computer;
2. Run the Total lock software ;
3. Enter language;
4. Create a personal ID;
5. Create a password 8-16 characters; and
6. Enter the secure partition as a data encryption key is automatically generated when an operator is created

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 256 bit AES Drive & Integral 256 bit AES MAC Drive for signs of physical tampering to the enclosure

4. The crypto officer MUST remember there password as there are only 6 attempts. If the password is incorrect after 6 attempts the Integral 256 bit AES Drive and Integral AES 256 bit AES MAC Drive will zeroize all keys, CSP's and user data.

9 Mitigation of Other Attacks

The module does not mitigate against any specific attacks.