

# Integral Crypto AES 256 Bit USB 3.0



Integral Memory Plc  
FIPS 140-2 non-Proprietary Security Policy



# Table Of Contents

1. Introduction .....	4
1.1 Purpose .....	4
1.2 References .....	4
1.3 Document History .....	4
2. Cryptographic Module Description .....	5
2.1 The Integral Crypto AES 254 Bit USB 3.0 .....	5
2.2 Cryptographic Module Specification .....	5
2.3 Module Compliance to FIPS 140-2 Sections .....	6
2.4 Tested Module Configurations .....	7
3. Mode of Operation .....	8
3.1 FIPS Approved Mode .....	8
3.2 Rules & Recommendations .....	9
4. Module Ports & Interfaces .....	9
4.1 Physical Interface Description .....	9
4.2 Logical Interface Description .....	10
5. Roles Services & Authentication .....	10
5.1 Identification & Authentication .....	10
5.2 Roles & Services .....	11
6. Physical Security .....	12
6.1 Physical Security Mechanisms .....	12
7. Operational Environment .....	12
8. Key Management .....	13
8.1 Cryptographic Keys and CSPs .....	13
9. Power Up Self Tests .....	14
9.1 Power Up Self-Tests .....	14
9.2 Conditional Self- Tests .....	15
9.3 Critical Function Tests .....	15
9.4 Cryptographic Algorithms .....	15
9.5 Self-Test Failure .....	15
9.6 On Demand Self-Test .....	15
10. Design Assurance .....	16
10.1 Secure Delivery .....	16
10.2 Configuration Management .....	16
11. Mitigation Of Other Attacks .....	16

## Figures & Tables

Figure 1 Cryptographic Module Block Diagram

Table 1 Level of Compliance .....	6
Table 2 Module Information .....	8
Table 3 USB Pin Out .....	9
Table 4 Logical Interfaces .....	10
Table 5 Roles & Authentication .....	10
Table 6 Roles & Services .....	11
Table 7 Inspection/Testing of Physical Security Mechanisms.....	12
Table 8 Cryptographic Keys and CSPs.....	13
Table 9 Algorithm Certificates .....	15

## 1. Introduction

## 1.1 Purpose

This is a non-proprietary FIPS 140-2 Security Policy for the Integral Crypto AES 256 Bit USB 3.0 Hardware Cryptographic Modules. It describes how these modules meet all requirements as specified for FIPS 140-2, Level 3. This policy forms a part of the submission package to the security testing (Lightship Security) 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/](http://www.integralmemory.com/crypto/)

## 1.3 Document History

Author(s)	Version	Date	Comment
Patrick Warley	1.0	27/06/2020	Initial Draft

## 2. Cryptographic Module Description

### 2.1 The Integral Crypto AES 256 Bit USB 3.0

The Integral Crypto AES 256 Bit USB 3.0 Hardware Cryptographic Modules are removable storage devices which encrypt the content transferred onto them. The modules come in **2GB, 4GB, 8GB, 16GB, 32GB, 64GB, 128GB, 256GB, 512GB** and **1TB** sizes. The modules feature a steel outer chassis and an epoxy resin coating around the circuit components and the printed circuit board (PCB). The modules implement AES in FIPS Approved Mode.

The modules require no software installation and work by creating two partitions, when attached to either a Microsoft Windows® based PC or to an Apple Mac® Computer. The first partition appears as a CD drive which runs a software package (called Dual Lock or 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 Dual Lock or Total Lock software package running on the host computer. The CD drive is read only and no files can be transferred to this partition. The module has a zero footprint that requires no software installation on the host computer with a people friendly interface, making the drive simple and easy to use without compromising security.

The modules also have 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 modules have mandatory encryption for any data transferred onto it. The encryption is carried out using AES (256 bit in XTS mode). They also support identity-based authentication with a strong user password of a minimum 8 characters and a maximum of 16 characters. The password must contain both upper- and lower-case letters and must include at least one numeric and one special character. For further protection, the modules allow only 6 incorrect password attempts in either User or Admin mode, before destroying all data on the device. This measure protects against brute force attacks on the drive.

The modules have been tested by International Standards Labs, and found to be in compliance with the requirement of the following:

- ✓ FCC Part 15: 2005 Subpart B, Class B; and
- ✓ CISPR 22: 1997, Class B.

The modules have a multi-lingual interface supporting 26 languages.

### 2.2 Cryptographic Module Specification

The modules are multi-chip standalone hardware cryptographic modules 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) is defined as all components inside and including the steel chassis which contains integrated circuit packaging that is production grade and opaque within the visible spectrum.

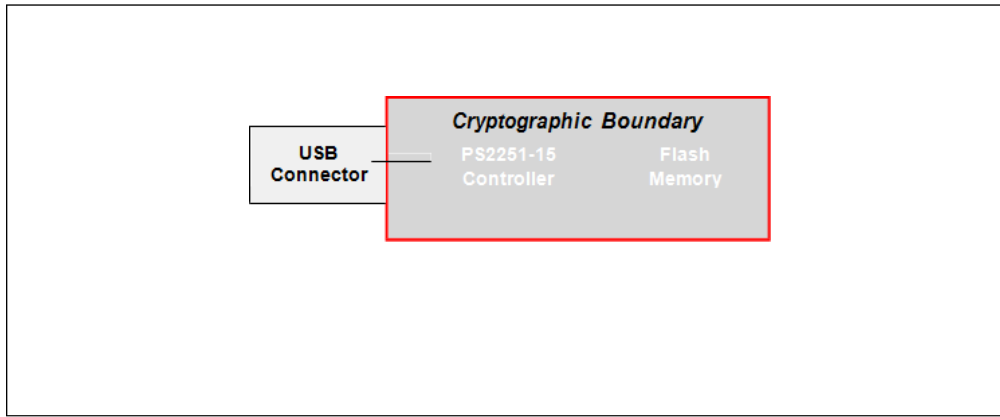


Figure 1 – Cryptographic Module Block Diagram

## 2.3 Module Compliance to FIPS 140-2 Sections

The Integral Crypto AES 256 Bit USB 3.0 conforms to the following Sections of FIPS 140-2:

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

Table - 1 Level of Compliance

## 2.4 Tested Module Configurations

The Integral Crypto AES 256 Bit USB 3.0 executes in a proprietary operational environment. The configurations which have been tested are listed as follows in Table 2:

Crypto USB 3.0 FIPS 140-2			
USB Size	Hardware Version	Crypto Processor	Firmware Version
4GB	INFD4GCRY3.0140-2	PS2251-15	4.06.10
8GB	INFD8GCRY3.0140-2	PS2251-15	4.06.10
16GB	INFD16GCRY3.0140-2	PS2251-15	4.06.10
32GB	INFD32GCRY3.0140-2	PS2251-15	4.06.10
64GB	INFD64GCRY3.0140-2	PS2251-15	4.06.10
128GB	INFD128GCRY3.0140-2	PS2251-15	4.06.10
256GB	INFD256GCRY3.0140-2	PS2251-15	4.06.10
512GB	INFD512GCRY3.0140-2	PS2251-15	4.06.10
1TB	INFD1TCRY3.0140-2	PS2251-15	4.06.10
2TB	INFD2TCRY3.0140-2	PS2251-15	4.06.10
Crypto Dual USB 3.0 FIPS 140-2			
USB Size	Hardware Version	Crypto Processor	Firmware Version
4GB	INFD4GCRYDL3.0140-2	PS2251-15	4.06.10
8GB	INFD8GCRYDL3.0140-2	PS2251-15	4.06.10
16GB	INFD16GCRYDL3.0140-2	PS2251-15	4.06.10
32GB	INFD32GCRYDL3.0140-2	PS2251-15	4.06.10
64GB	INFD64GCRYDL3.0140-2	PS2251-15	4.06.10
128GB	INFD128GCRYDL3.0140-2	PS2251-15	4.06.10
256GB	INFD256GCRYDL3.0140-2	PS2251-15	4.06.10
512GB	INFD512GCRYDL3.0140-2	PS2251-15	4.06.10
1TB	INFD1TCRYDL3.0140-2	PS2251-15	4.06.10
2TB	INFD2TCRYDL3.0140-2	PS2251-15	4.06.10

Envoy Dual USB 3.0 FIPS 140-2			
USB Size	Hardware Version	Crypto Processor	Firmware Version
4GB	INFD4GENVDL3.0-140	PS2251-15	4.06.10
8GB	INFD8GENVDL3.0-140	PS2251-15	4.06.10
16GB	INFD16GENVDL3.0-140	PS2251-15	4.06.10
32GB	INFD32GENVDL3.0-140	PS2251-15	4.06.10
64GB	INFD64GENVDL3.0-140	PS2251-15	4.06.10
128GB	INFD128GENVDL3.0-140	PS2251-15	4.06.10
256GB	INFD256GENVDL3.0-140	PS2251-15	4.06.10
512GB	INFD512GENVDL3.0-140	PS2251-15	4.06.10
1TB	INFD1TENVDL3.0-140	PS2251-15	4.06.10
2TB	INFD2TENVDL3.0-140	PS2251-15	4.06.10

Table 2 - Module Information

## 3. Mode of Operation

### 3.1 FIPS Approved Mode

The Integral Crypto AES 256 Bit Hardware Encrypted USB 3.0 contains only an Approved mode of operation, meaning that no configuration exists whereby the module can operate in a non-Approved mode. The instructions to securely configure and initialize the modules into the Approved mode are as follows:

#### **FIPS Approved Mode Operation**

- Plug the Integral Hardware encrypted Crypto AES 256 Bit USB 3.0 into the host computer.
- USB Runs Power-On Self tests.
- Execute the Dual Lock or Total Lock Software when presented.
- Accept the Terms and Conditions.
- Choose Language.
- Create a Personal ID.
- Create a User or Master Password minimum of 8 and maximum 16 characters long. (Password requires upper- and lower-case letters and must include at least one numeric and one special character).
- Your Integral Hardware encrypted Crypto AES 256 Bit USB 3.0 is Now Running in FIPS approved Mode. The module will confirm that the Approved mode has been entered by showing on-screen that the device status is “unlocked”.



## 3.2 Rules & Recommendations

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

- Encrypting data using AES 256 (default setting).
- Setting of a minimum of 8 to maximum of 16-character password (this is default value and the operator cannot select any less than 8 characters and a maximum of 16 characters).
- The Crypto-Officer shall periodically inspect the module for signs of physical tampering to the enclosure. (See the Physical Security Section for details).
- The Crypto-Officer shall retain the correct password. If the password is incorrect after 6 attempts, all keys, CSPs and user data will be zeroed from the module.

## 4. Module Ports & Interfaces

### 4.1 Physical Interface Description

The modules support five pins that lead to the PCB. The following Table demonstrates the PIN, Function and how it maps to the logical FIPS 140-2 interface.

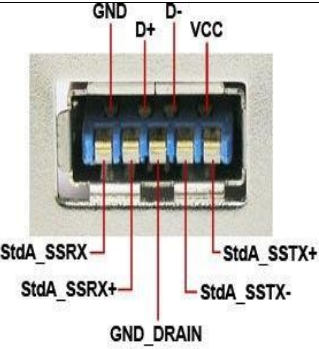
	PIN	Function	FIPS 140-2 Logical Interface
	USB 1	Data Input	Data Pin within the USB Port Data Input
	USB 2	Data Output	Data Pins within the USB Status Output
	USB 3	Control Output	Data Pins within the USB, Control Output
	USB 4	Status Output	Data Pins within the USB Port Status Output
	USB 5	Power supply voltage 4.75V – 5.25V	Power Pin within the USB Port

Table - 3 USB Pin Out

## 4.2 Logical Interface Description

FIPS 140-2 Logical Interface	I/O Type
Data Input	I/O bidirectional line
Data Output	I/O bidirectional line
Control Input	I/O bidirectional line
Status Output	I/O bidirectional line and LED
Power	Power Pin within the USB Port

Table 4 - Logical Interfaces

The USB 3.0 protocol ensures these logical interfaces are distinct. The module does not support the input or output of plaintext cryptographic key components, authentication data and CSPs.

## 5. Roles, Services & Authentication

### 5.1 Identification & Authentication

The authentication methods employed by the module are described here in Table 5. An operator has 6 attempts to enter the correct password before zeroization of the module occurs. This limitation provides a weaker attack vector than the one-minute limitation.

Role	FIPS 140-2 Auth. Type	Authentication	Auth. Strength	Multi-Attempt in 60 sec Strength
Crypto-Officer	Identity Based	Master username and minimum 8 to a maximum of 16 alpha/numeric & special character password	1 in $(94^8) = 1$ in 6,095,689,385,410,816	1 in $(94^8)/6 = 1$ in 1,015,948,230,901,802 (with 6 guesses before zeroization)
User	Identity Based	Username and minimum 8 to a maximum 16 alpha/numeric & Special Character password		

Table 5 - Roles & Authentication Methods

## 5.2 Roles & Services

The modules support the services listed in Table 6. 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.

### Legend

**RSA Public Key** – It is used for Firmware Integrity Test

**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 800-90 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	<b>Self-Test</b>	Crypto-Officer User	RSA Public Key	E
2	<b>Authenticate</b>	Crypto-Officer User	Password	W, E
3	<b>Create Password</b>	Crypto-Officer User	Password	W, E
4	<b>Reset Password</b>	Crypto-Officer user	Password	W, E
5	<b>Lock</b>	Crypto-Officer User	N/A	E
6	<b>Show Status</b>	Crypto-Officer User	N/A	R
7	<b>Key Generation</b>	Crypto-Officer User	HMAC, DEK Seed AES -ECB	W, E
8	<b>Encrypt/Decrypt</b>	Crypto-Officer User	DEK AES-ECB	W, E
9	<b>Password to KEK</b>	Crypto-Officer User	Password, KEK	W
10	<b>Reset (Zeroize)</b>	Crypto-Officer	All Keys & CSPs	W, E
11	<b>Key Wrap</b>	Crypto-Officer User	DEK, KEK	W
12	<b>Logout</b>	Crypto-Officer User	N/A	E

Table 6 - Roles & Services

## 6. Physical Security

### 6.1 Physical Security Mechanisms

The cryptographic boundary for the modules is defined as all components within the steel chassis. Beneath the steel chassis, all PCB circuitry is coated in a tamper resistant epoxy resin. The modules do not have removable doors or covers. They contain components with integrated circuit packaging that is production grade using standard passivation and they are opaque within the visible spectrum.

It is the responsibility of the Crypto-Officer to periodically inspect the module for tamper evidence, on a pre-defined schedule. This requires the inspection of the outer metal chassis to ensure that it has not been breached and does not show signs of damage.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Outer Steel Chassis	Inspect for signs of forced entry on a schedule determined by the Crypto-Officer.	Discontinue use and replace module if obvious signs of chassis penetration have occurred.
Epoxy Resin Coated PCB	N/A	Module will cease to function if underlying circuitry is breached. The module must be replaced.

Table 7 - Inspection/Testing of Physical Security Mechanisms

In the Integral Crypto AES 256 Bit USB 3.0, the Level 3 physical security requirements are met due to the tamper evidence that will occur if attempts are made to breach the outer steel chassis, and also hard coating which protects the underlying circuitry from being breached as per FIPS 140-2, Section 4.5.3. 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 shall be replaced immediately however, if any type of damage to the outer steel chassis is witnessed.

## 7. Operational Environment

The Integral Crypto AES 256 Bit USB 3.0 operates in a proprietary, non-modifiable operational environment and therefore Section 4.6.1 of the standard does not apply.

## 8. Key Management

### 8.1 Cryptographic Keys and CSPs

Key/CSP	Services	Length	Type	Zeroize Method	Establishment	Output	Storage
Data Encryption Key (DEK)	7, 8, 10, and 11	256 bits	AES-XTS	Reset command or attempts beyond six	NIST SP 800-90A HMAC-SHA-256 DRBG	NO	Persistent in Flash (Encrypted)
Password (PBKDF)	2, 3, 4, 9, and 10	8-16 Chars	Password	Reset command or attempts beyond six	Entered Manual	NO	Persistent in Flash (Hashed)
Crypto Officer Password	1 to 12	8-16 Chars	Password	Reset command or attempts beyond six	Entered Manual	NO	Persistent in Flash (Hashed)
User Password	1 to 9, 11, 12	8-16 Chars	Password	Reset command or attempts beyond six	Entered Manual	NO	Persistent in Flash (Hashed)
DRBG Entropy Input	7 and 10	512 bits	DRBG Entropy Input	Reset command or attempts beyond six	Hardware NDRNG	NO	Ephemeral (Plaintext) in Volatile RAM
DRBG V Value	7 and 10	256 bits	DRBG Internal State Value	Reset command or attempts beyond six	Internal State of NIST SP 800-90A DRBG	NO	Ephemeral (Plaintext) in Volatile RAM
DRBG Key Value	7 and 10	256 bits	DRBG Internal State Value	Reset command or attempts beyond six	Internal State of NIST SP 800-90A DRBG	NO	Ephemeral in Volatile (Plaintext) RAM
Key Encryption Key (KEK)	9, and 11	256 bits	AES	Reset command or attempts beyond six	NIST SP 800-132 PBKDF	NO	Ephemeral (Plaintext) in Volatile RAM
DRBG Nonce	7 and 10	512 bits	DRBG Nonce	Reset command or attempts beyond six	Hardware NDRNG	NO	Ephemeral (Plaintext) in Volatile RAM
RSA Public Key	1	2048 bits	RSA	N/A	N/A – Programmed during manufacturing	NO	Persistent in Flash (Plaintext)
DRBG Seed	7 and 10	256 bits	DRBG Seed	Reset command or attempts beyond six	Hardware NDRNG	NO	Ephemeral (Plaintext) in Volatile RAM
AES ECB	7, 8 9 and 10	256 bits	AES	Reset command or attempts beyond six	Key Generation	NO	Ephemeral (Plaintext) in Volatile RAM
HMAC SHA 256 KEY	7 and 10	256 bits	HMAC SHA-256 KEY	Reset command or attempts beyond six	Generated internally	NO	Ephemera (Plaintext) I in Volatile RAM

Table 8 - Cryptographic Keys & CSPs

NOTE 1: In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133 (vendor affirmed) and complies with Section 4 scenario 1. The resulting generated symmetric keys are from the unmodified output of the SP 800-90A DRBG.

NOTE 2 PBKDF (NIST SP 800-132) Option 2a (vendor affirmed) 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.

## 9. Power Up Self Tests

### 9.1. Power up Self tests

- Firmware Integrity Test using 2048-bit RSA Signature Verification
- AES encrypt KAT (XTS mode)
- AES decrypt KAT (XTS mode)
- HMAC\_SHA256 KAT
- SHA 256 KAT
- DRBG KAT
- AES Key Wrap KAT
- AES Key Unwrap KAT
- RSA verify KAT
- DRBG instantiate KAT
- DRBG generate KAT
- DRBG reseed KAT

### 9.2 Conditional Self-Tests

- 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 Cryptographic Algorithms

Algorithm	CAVP Algorithm Certificate	Location	Key Length	Algorithm Usage
AES (CBC, ECB and XTS modes),	C1686	Hardware	256bits	(encrypt/decrypt)
HMAC-SHA-256	C1685	Firmware	256bits	HMAC Functions
Internal NDRNG	N/A	Hardware	NA	Seeding mechanism to the FIPS approved DRBG
NIST SP 800-90A HMAC DRBG	C1685	Firmware	NA	Random Number Generation
SHA-256	C1686	Hardware	N/A	Message Digest
RSA (verify only)	C1686	Hardware	2048bits	Digital Signature Verification
PBKDF NIST SP 800-132	vendor affirmed	Firmware	N/A	Deriving Keys for Storage Application
AES Key Wrap NIST SP 800-38F	C1686	Hardware	256bits	Key Wrapping
CKG	vendor affirmed	Firmware	N/A	Cryptographic Key Generation

Table 9 - Algorithm Certificates

**NOTE: 3 AES CBC was tested but is not used by the module.**

## 9.6 Self-Test Failure

If any self-test fails, authentication to the host computer will not occur, the module will enter the error state and an error message will be displayed on-screen. No cryptographic operations are possible when this occurs, since the interfaces are disabled. The operator can attempt to clear the error by power cycling the host PC with the module connected, however if the module encounters an error for the power-up self-tests specified in Table 9 then the error is considered a permanent hard error. The module should be replaced in this circumstance.

## 9.7 On-Demand Self-Tests

In order to execute the power-up self-tests on demand; the operator can re-initialize the Integral Crypto AES 256 Bit USB 3.0 by removing and re-inserting it into the PC. Self-Tests execute without operator intervention when the module receives power.

## 10. Design Assurance

### 10.1. Secure Delivery

All Shipments from the Factory to the warehouse are shipped by bonded Shipping, the drives are packaged in boxes with tamper proof seals. Inside each of the boxes each drive is then packaged in its own packaging sealed. Once it leaves the warehouse it is then sent to customers buy bonded shipping agencies. Customers are instructed to check all packaging for tampering and if evidence found ship back to factory where they will be checked and replaced.

### 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.

## 11. Mitigation of Other Attacks

The modules do not claim mitigation of other attacks.