Integral Memory PLC.

Crypto Dual (Underlying Steel Chassis) and Crypto Dual Plus (Underlying Steel Chassis)

FIPS 140-2 Security Policy

Table of Contents

1 INTRODUCTION

1.1 Purpose

This is a non-proprietary FIPS 140-2 Security Policy for Crypto Dual (Underlying Steel Chassis) and Crypto Dual Plus (Underlying Steel Chassis) cryptographic modules. It describes how these modules meet all the requirements as specified in the FIPS 140-2 Level 2 requirements. This Policy forms a part of the submission package to the security testing (CST) Laboratory.

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/crypto/

1.3 Document History

Author(s)	Date	Version	Comment
Patrick Warley	October 3rd, 2012	1.8	FIPS Submission Draft

2 PRODUCT DESCRIPTION

The modules are removable storage devices which encrypts documents transferred onto them. The Crypto Dual (Underlying Steel Chassis) come in 2 GB, 4 GB, 8 GB, 16 GB, 32 GB and 64 GB and the Crypto Dual Plus (Underlying Steel Chassis) comes in 2 GB 4 GB 8GB 16 GB 32 GB 64 GB 128 GB, 512 GB and 1 TB versions. The devices feature many security enhancements, like a steel inner chassis, and an epoxy resin coating around both the circuit components and the printed circuit board (PCB). The modules implement AES, SHA, and ANSI X9.31 RNG in FIPS Approved Mode. The only difference in the Crypto Dual (Underlying Steel Chassis) to the Dual Plus (Underlying Steel Chassis) is the capacity of the USB

The devices 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) 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 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.

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.

Modules have mandatory encryption for any data transferred onto it. The encryption is carried out using AES (256 bit 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 and Special character. For further protection modules allow only 6 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 modules have a Multi-Lingual interface in 26 languages.

2.1 Cryptographic Module Specification

The modules are a multi-chip standalone 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 modules (the red line in Figure 1) is defined as all components within the steel chassis. (All components are coated in epoxy and encased in the steel chassis.) The chassis contains integrated circuit packaging that is production grade and opaque within the visible spectrum. The rubber sleeve material which surrounds the module as shipped, has been excluded from the requirements of FIPS 140-2, as it provides no benefit in terms of physical security.

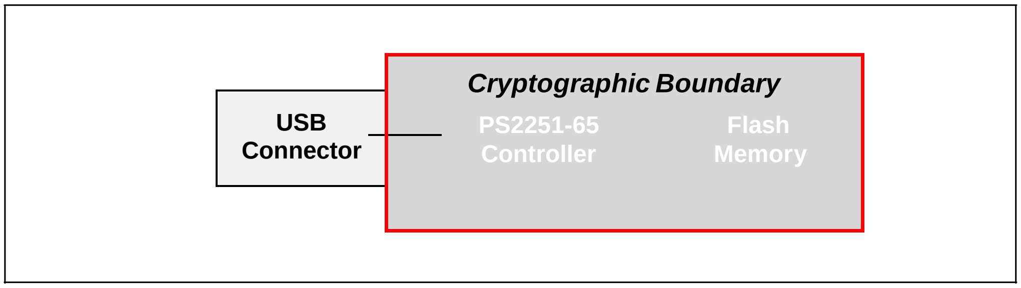

Figure 1 - Module Block Diagram

The Crypto Dual (Underlying Steel Chassis) and Crypto Dual Plus (Underlying Steel Chassis) which are being covered by this validation:

Module Name	*Memory Option*	Hardware Version	*Software Version*	*Firmware Version*
Crypto Dual (Underlying Steel Chassis)	2 GB	INFD2GCRYPTODL140-2(R)	1.00	PS2251-65
Crypto Dual (Underlying Steel Chassis)	4 GB	INFD4GCRYPTODL140-2(R)	1.00	PS2251-65
Crypto Dual (Underlying Steel Chassis)	8 GB	INFD8GCRYPTODL140-2(R)	1.00	PS2251-65
Crypto Dual (Underlying Steel Chassis)	16 GB	INFD16GCRYPTODL140-2(R)	1.00	PS2251-65
Crypto Dual (Underlying Steel Chassis)	32GB	INFD32GCRYTPODL140-2(R)	1.00	PS2251-65
Crypto Dual (Underlying Steel Chassis)	64 GB	INFD64GCRYPTODL140-2(R)	1.00	PS2251-65
Crypto Dual Plus (Underlying Steel Chassis)	2 GB	INFD2GCRYDLP140-2(R)	1.00	PS2251-65
Crypto Dual Plus (Underlying Steel Chassis)	4 GB	INFD4GCRYDLP140-2(R)	1.00	PS2251-65
Crypto Dual Plus (Underlying Steel Chassis)	8 GB	INFD8GCRYDLP140-2(R)	1.00	PS2251-65
Crypto Dual Plus (Underlying Steel Chassis)	16 GB	INFD16GCRYDLP140-2(R)	1.00	PS2251-65
Crypto Dual Plus (Underlying Steel Chassis)	32 GB	INFD32GCRYDLP140-2(R)	1.00	PS2251-65
Crypto Dual Plus (Underlying Steel Chassis)	64GB	INFD64GCRYDLP140-2(R)	1.00	PS2251-65
Crypto Dual Plus (Underlying Steel Chassis)	128GB	INFD128GCRYDLP140-2(R)	1.00	PS2251-65
Crypto Dual Plus (Underlying Steel Chassis)	256GB	INFD256GCRYDLP140-2(R)	1.00	PS2251-65
Crypto Dual Plus (Underlying Steel Chassis)	512GB	INFD512GCRYDLP140-2(R)	1.00	PS2251-65
Crypto Dual Plus (Underlying Steel Chassis)	1TB	INFD1TCRYDLP140-2(R)	1.00	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 modules support four pins that lead to the PCB board.

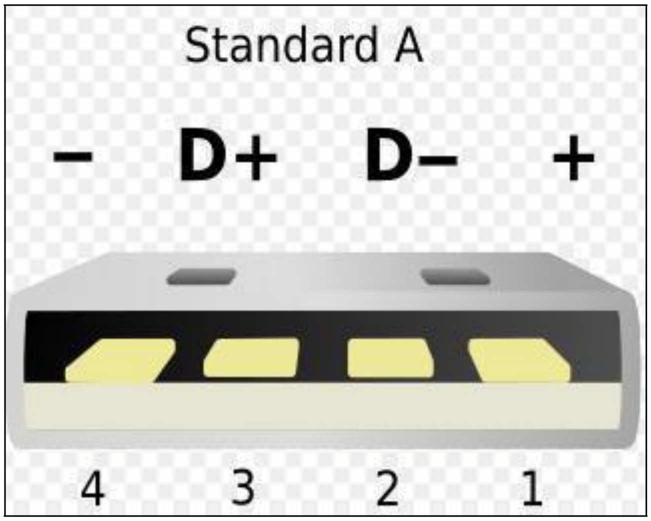

Figure 2 - Functional Specifications of PIN

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 - Specific Functions of USB Contacts

3.2 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 modules support a Crypto-Officer (Master), and a User role that are explicitly assumed. The modules implement Identity-based authentication using a unique user ID and password. The modules do not 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	User Name & 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 $8!x26x10x32x94^5$
Crypto Officer	Identity Based	Master user name 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 $8!x26x10x32x94^5$

Table 4 - Authentication Type Table

4.2 Roles and Services

The modules support 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
	User Password Reset	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 5 - Cryptographic Officer (Master) – 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 6 - User – Roles and Services

5 PHYSICAL SECURITY

The cryptographic boundary for the modules is defined as all components within the steel chassis only. All components are coated in epoxy and encased in the steel chassis. The rubber sleeve material which surrounds the steel chassis is not considered part of the cryptographic boundary, and has been excluded from the FIPS 140-2 requirements on the basis that it contributes nothing to the module's security. 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.

As stated below in Section 8.2, it is the responsibility of the Crypto-Officer to periodically inspect the module for tamper evidence. This requires the removal of the rubber sleeve material by whatever means are necessary to ensure that the underlying steel chassis is intact and undamaged. In the event that the steel chassis shows evidence of tampering, the module shall be replaced.

Figure 3 - Crypto Dual (Underlying Steel Chassis (Upper) & Dual Plus (Underlying Steel Chassis) (Lower)

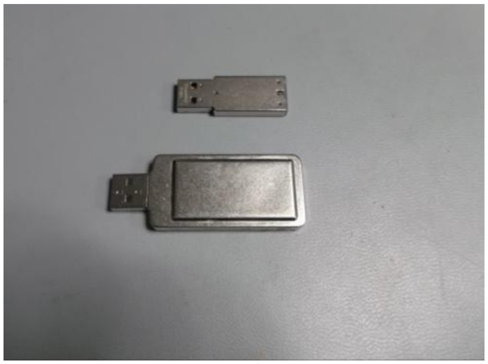

Figure-3

When the modules are shipped to the customer they have the rubber sleeves on and glued to the steel outer case, however the rubber sleeve is not included within the cryptographic boundary.

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 summarizes the module’s keys and CSPs:

Key/CSP	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(SHA-1)	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 7 - Cryptographic Keys and CSPs

6.1 Key Entry / Key Output

The modules do not input / output keys or CSPs.

6.2 Key Destruction

The modules zeroize all keys and CSPs with the reset command or by failing 6 password attempts in User or Master mode.

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) and ECB (enc/dec; 128 and 256)**	1205
SHA-1 and SHA-256, byte-oriented	1108
ANSI X9.31 RNG (256 bit AES)	666

Table 8 - FIPS Approved Algorithms Table

Non-Approved Security Function
H/W RNG for Seeding

Table 9 - Non Approved Security Function

7 SELF-TEST

The modules perform 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 modules check the integrity of their components using 16 bit CRC at power up.

The modules perform 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 the modules 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 is to power down the computer or pull the modules out of the host computer and reinsert.

8 CRYPTO-OFFICER AND USER GUIDANCE

This section shall describe the configuration and administration of the cryptographic modules.

8.1 Secure Setup and Initialization

The procedures to securely setup and initialize the modules include:

1. Plug the modules into USB Flash drive to the host computer;
2. Run the Dual lock software
3. Accept the T&C
4. Enter language;
5. Create a personal ID;
6. Create a user or master password 8-16 Characters long both upper and lower case letters, and include at least one numeric and Special character.
7. The modules are now ready to use.

8.2 Module Security Policy Rules & Recommendations

Security rules enforced by the cryptographic modules 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 shall periodically inspect the modules for signs of physical tampering to the enclosure. (See Section 5 for further information about the inspection process.)
4. The crypto officer shall remember their password as there are only 6 attempts. If the password is incorrect after 6 attempts the Integral 256 bit Cypher Drive will zeroize all keys, CSPs, and user data.

9 MITIGATION OF OTHER ATTACKS

The modules do not mitigate against any specific attacks.