SPYRUS FIPS Sector-based Encryption Module Security Policy

Revision Document No. 1.7

10 March 2011

SPYRUS, Inc.
info@spyrus.com>
<http://www.spyrus.com>

SPYRUS Document No. 550-074002-08

Trademarks

Contents

1 INTRODUCTION **1**
1.1 SPYRUS FIPS Sector-based Encryption Module Overview 2
1.2 SPYRUS FIPS Sector-based Encryption Module Environmental Range 2
1.3 SPYRUS FIPS Sector-based Encryption Module Implementation 2
1.4 SPYRUS FIPS Sector-based Encryption Module Cryptographic Boundary and Tamper Inspection 3
1.5 Approved Mode of Operations 3
2 FIPS 140-2 SECURITY LEVELS **5**
3 SECURITY RULES **5**
3.1 FIPS 140-2 Imposed Security Rules 5
3.2 SPRYUS Imposed Security Rules 10
3.3 Identification and Authentication Policy 10
4 SPYRUS FIPS SECTOR-BASED ENCRYPTION MODULE ROLES AND SERVICES **11**
4.1 Roles 11
4.2 Services 12
5 IDENTIFICATION AND AUTHENTICATION **14**
5.1 Initialization Overview 14
5.2 Operator Authentication 14
5.3 Generation of Random Numbers 14
5.4 Strength of Authentication 15
6 ACCESS CONTROL **16**
6.1 Critical Security Parameters (CSPs) and Public Keys 16
6.2 CSP Access Modes 17
6.3 Access Matrix 18
7 SELF-TESTS **19**
8 MITIGATION OF OTHER ATTACKS **20**
9 ACRONYMS AND REFERENCES **21**

1 Introduction

This Security Policy specifies the security rules under which the SPYRUS FIPS Sector-based Encryption Module operates. Included in these rules are those derived from the security requirements of FIPS 140-2 and additionally, those imposed by SPYRUS, Inc. These rules, in total, define the interrelationship between:

1. Operators,
2. Services, and
3. Critical Security Parameters (CSPs).

Figure 1 SPYRUS FIPS Sector-based Encryption Module (Topside)

Figure 2 SPYRUS FIPS Sector-based Encryption Module (Underside)

1.1 SPYRUS FIPS Sector-based Encryption Module Overview

The SPYRUS FIPS Sector-based Encryption Module enables security critical capabilities such as operator authentication and secure storage in rugged, tamper-evident hardware. The SPYRUS FIPS Sector-based Encryption Module communicates with a host computer via the USB interface. The SPYRUS FIPS Sector-based Encryption Module protects data for government, large enterprises, small organizations, and home users. Key features:

- Encryption technology uses Suite B algorithms approved by the U.S. government for protecting both Unclassified and Classified data
- Encrypted file storage on non-removable flash card
- Strong protection against intruder attacks

Access protection is as important as encryption strength. Data encrypted with the SPYRUS FIPS Sector-based Encryption Module cannot be decrypted until the authorized user gains access to the device.

1.2 SPYRUS FIPS Sector-based Encryption Module Environmental Range

The SPYRUS FIPS Sector-based Encryption Module operates in the following temperature range: -20 degrees C. to 65 degrees C.

The epoxy hardness was evaluated at the normal operating temperature range extremes of -20 degrees to 65 degrees Celsius inclusive, as well as at ambient temperature. No penetration to the underlying components of the module was possible utilizing Level 3 physical security testing techniques.

1.3 SPYRUS FIPS Sector-based Encryption Module Implementation

The SPYRUS FIPS Sector-based Encryption Module is implemented as a multi-chip standalone module as defined by FIPS 140-2. The FIPS 140-2 module identification data for the SPYRUS FIPS Sector-based Encryption Module is shown in the table below:

Part Number	FW Version	HW Version
880074002F	03.00.0C	02.00.01

880074003F	03.00.0C	02.00.01
880074004F	03.00.0C	02.00.01

The SPYRUS FIPS Sector-based Encryption Module is available with a USB interface compliant to the *Universal Serial Bus Specification*, Revision 2.0, dated 23 September 1998. All Interfaces have been tested for compliance with FIPS 140-2.

1.4 SPYRUS FIPS Sector-based Encryption Module Cryptographic Boundary and Tamper Inspection

The Cryptographic Boundary is defined to be the outer perimeter of the hard, opaque epoxy potting. Please see Figure 1.

The operator detects physical attacks against the module by direct physical inspection. If the module is packaged in a plastic case or similar outer coating that is not inside the cryptographic boundary, any sign of entry, cracking, breakage or damage to the case due to prying or forcing using a sharp tool may require further inspection to confirm whether a penetration attack has taken place on the module's epoxy coating. The epoxy coating will either show tamper evidence or not. If it shows tamper evidence, the module has been compromised and the operator must treat the device in accordance with organizational security policy. This would include issuance of a new device. If it does not show tamper evidence, the operator may continue to use the device in accordance with organizational security policy.

No hardware, firmware, or software components that comprise the SPYRUS FIPS Sector-based Encryption Module are excluded from the requirements of FIPS 140-2.

1.5 Approved Mode of Operations

The SPYRUS FIPS Sector-based Encryption Module operates only in a FIPS Approved mode. The indicator that shows the operator that the module is in the Approved mode is the “GetCapabilities” command, which shows the module’s firmware and hardware versions as well as the product indicator.

The SPYRUS FIPS Sector-based Encryption Module supports the FIPS 140-2 Approved algorithms in Table 1-1 below and the following allowed algorithms:

- EC Diffie-Hellman (ECDH) for key agreement as allowed by FIPS 140-2 Implementation Guidance D.2 (key agreement; key establishment methodology provides between 128, 192 or 256 bits of encryption strength).
- NDRNG to seed the FIPS 186-2 Approved RNG.

Table 1-1 Approved Algorithms supported by the SPYRUS FIPS Sector-based Encryption Module

Encryption & Decryption
AES-128/192/256 (Certs. #1259, #1260, #1261, #1262, #1263, and #1264)
Digital Signatures
ECDSA, key sizes: 256, 384, 521 (Certs. #147, #148, and #149)
Hash
SHA-224, SHA-256, SHA-384, SHA-512 (Certs. #1155, #1156, #1157, #1158,#1159, and #1160) SHA-1 (Certs. #1161, #1162, and #1163)
DRBG
HASH_DRBG (SP 800-90) (Certs. #29, #30, and #31)
RNG for Seeding
FIPS 186-2 (Certs. #703, #704, and #705)

2 FIPS 140-2 Security Levels

The SPYRUS FIPS Sector-based Encryption Module cryptographic module complies with the requirements for FIPS 140-2 validation to the levels defined in Table 2.1. The FIPS 140-2 overall rating of the SPYRUS FIPS Sector-based Encryption Module is Level 3.

Table 2-1 FIPS 140-2 Validation Levels

FIPS 140-2 Category	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

3 Security Rules

The SPYRUS FIPS Sector-based Encryption Module enforces the following security rules. These rules are separated into two categories: 1) rules imposed by FIPS 140-2; and 2) rules imposed by SPYRUS.

3.1 FIPS 140-2 Imposed Security Rules

Table 3-1 FIPS 140-2 Policies and Rule Statements

Policy	Rule Statement
Authentication Feedback	The SPYRUS FIPS Sector-based Encryption Module shall obscure feedback of authentication data to an operator during authentication (e.g., no visible display of characters result when entering a password).

Policy	Rule Statement
Authentication Mechanism	The SPYRUS FIPS Sector-based Encryption Module shall enforce Identity-Based authentication.
Authentication Strength (1)	The SPYRUS FIPS Sector-based Encryption Module shall ensure that feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism.
Authentication Strength (2)	The SPYRUS FIPS Sector-based Encryption Module shall satisfy the requirement for a single–attempt false acceptance rate of no more than one in 1,000,000 authentications.
Authentication Strength (3)	The SPYRUS FIPS Sector-based Encryption Module shall satisfy the requirement for a false acceptance rate of no more than one in 100,000 for multiple authentication attempts during a one minute interval.
Configuration Management	The SPYRUS FIPS Sector-based Encryption Module shall be under a configuration management system and each configuration item shall be assigned a unique identification number.
CSP Protection	The SPYRUS FIPS Sector-based Encryption Module shall protect all CSPs from unauthorized disclosure, modification, and substitution.
Emissions Security	The SPYRUS FIPS Sector-based Encryption Module shall conform to the EMI/EMC requirements specified in FCC Part 15, Subpart B, Class B.
Error State (1)	The SPYRUS FIPS Sector-based Encryption Module shall inhibit all data output via the data output interface whenever an error state exists and during self-tests.
Error State (2)	The SPYRUS FIPS Sector-based Encryption Module shall not perform any cryptographic functions while in an Error State.

Policy	Rule Statement
Guidance Documentation	The SPYRUS FIPS Sector-based Encryption Module documentation shall provide Administrator and User Guidance per FIPS 140-2, Section 4.10.4.
Hardware Quality	The SPYRUS FIPS Sector-based Encryption Module shall contain production quality ICs with standard passivation.
Interfaces (1)	The SPYRUS FIPS Sector-based Encryption Module interfaces shall be logically distinct from each other.
Interfaces (2)	The SPYRUS FIPS Sector-based Encryption Module shall support the following five (5) interfaces: • data input • data output • control input • status output • power interface
Key Association	The SPYRUS FIPS Sector-based Encryption Module shall provide that: a key entered into, stored within, or output from the SPYRUS FIPS Sector-based Encryption Module is associated with the correct entity to which the key is assigned.
Logical Separation	The SPYRUS FIPS Sector-based Encryption Module shall logically disconnect the output data path from the circuitry and processes performing the following key functions: • key generation, • key zeroization
Mode of Operation	The SPYRUS FIPS Sector-based Encryption Module services shall indicate that the module is in an approved mode of operation with a standard success return code and the output of the “GetCapabilities” command.

Policy	Rule Statement
Public Key Protection	The SPYRUS FIPS Sector-based Encryption Module shall protect public keys against unauthorized modification and substitution.
Re-authentication	The SPYRUS FIPS Sector-based Encryption Module shall re-authenticate an identity when it is powered-up after being powered-off.
RNG Strength	The SPYRUS FIPS Sector-based Encryption Module shall use a 'seed input' into the deterministic random bit generator of sufficient length that ensures at least the same amount of operations are required to determine the value of the generated key.
Secure Development (1)	The SPYRUS FIPS Sector-based Encryption Module source code shall be annotated.
Secure Development (2)	The SPYRUS FIPS Sector-based Encryption Module software shall be implemented using a high-level language except that limited use of a low-level language is used to enhance the performance of the module.
Secure Distribution	The SPYRUS FIPS Sector-based Encryption Module documentation shall include procedures for maintaining security while distributing and delivering the module.
Self-tests (1)	The power-up tests shall not require operator intervention in order to run.
Self-tests (2)	The SPYRUS FIPS Sector-based Encryption Module shall perform the self-tests identified in Section 7.
Self-tests (3)	The SPYRUS FIPS Sector-based Encryption Module shall enter an Error State and output an error indicator via the status interface whenever self-test is failed.
Services	The SPYRUS FIPS Sector-based Encryption Module shall provide the following services: (see Reference Table 4.2).

Policy	Rule Statement
Software Integrity	The SPYRUS FIPS Sector-based Encryption Module shall apply a SHA-384 hash to check the integrity of all firmware components
Status Output	The SPYRUS FIPS Sector-based Encryption Module shall provide an indication via the "GetUserState" command if all of the power-up tests are passed successfully. The module also provides status via the LED.
Strength of Key Establishment	The SPYRUS FIPS Sector-based Encryption Module shall use a key establishment methodology that ensures at least the same amount of operations are required to determine the value of the transported/agreed upon key.
Unauthorized Disclosure	The SPYRUS FIPS Sector-based Encryption Module shall protect the following keys from unauthorized disclosure, modification and substitution: • secret keys • private keys
Zeroization (1)	The SPYRUS FIPS Sector-based Encryption Module shall provide a zeroization mechanism that can be performed either procedurally by the operator *or* automatically by the SPYRUS FIPS Sector-based Encryption Module interface software on the connected host platform.
Zeroization (2)	The SPYRUS FIPS Sector-based Encryption Module shall provide the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the SPYRUS FIPS Sector-based Encryption Module (HPC140-F).

3.2 SPRYUS Imposed Security Rules

Table 3-2 SPYRUS Imposed Policies and Rule Statements

Policy	Rule Statement
Single User Session	The SPYRUS FIPS Sector-based Encryption Module shall not support multiple concurrent operators.
No Maintenance Interface	The SPYRUS FIPS Sector-based Encryption Module shall not provide a maintenance role/interface.
No Bypass Mode	The SPYRUS FIPS Sector-based Encryption Module shall not support a bypass mode.

3.3 Identification and Authentication Policy

The table below describes the type of authentication and the authentication data to be used by operators, by role. For a description of the roles, see section 4.2.

Table 3-3 Identification and Authentication Roles and Data

Role	Type of Authentication	Authentication Data
Administrator (CO)	Identity-based	Service and ECDSA Signature (384-bits)
User	Identity-based	Service and PIN (minimum 7 to 262 characters)

4 SPYRUS FIPS Sector-based Encryption Module Roles and Services

4.1 Roles

The SPYRUS FIPS Sector-based Encryption Module supports two roles, Administrator (Crypto Officer) and User, and enforces the separation of these roles by restricting the services available to each one. Each role is associated with a single user identity, namely the service that has been requested and is associated with the role.

Table 4-1 Roles and Responsibilities

Role	Responsibilities
Administrator	The Administrator is responsible for performing Firmware Updates and setting configuration of the SPYRUS FIPS Sector-based Encryption Module (HPC140-F). The SPYRUS FIPS Sector-based Encryption Module validates the Administrator identity by way of a signature before accepting any FirmwareUpdate or SetConfiguration commands.
User	The User role is available after the SPYRUS FIPS Sector-based Encryption Module has been initialized. The user can load, generate and use secret keys for encryption services.

The SPYRUS FIPS Sector-based Encryption Module validates the User identity by password before access is granted.

4.2 Services

The following table describes the services provided by the SPYRUS FIPS Sector-based Encryption Module.

Table 4-2 SPYRUS FIPS Sector-based Encryption Module Services

Service	CO	User	Unauthen-ticated	Description
ChangePassword		X		Changes User Password
Format		X		Formats the mounted CDROM
GetCapabilities	X	X	X	Returns the current capabilities of the system including: global Information, Sector storage size and the product name. This service provides a response that indicates the approved mode of operation (see Section 3.1).
GetConfig	X	X	X	Returns the card configuration structure
GetUserState	X	X	X	Returns the state and the Logon attempts remaining.
Initialize		X		Generates a new encryption key and changes the PIN. Secure channel is required. Formats the media.
LogOff		X		Log Off; Return to unauthenticated state.
LogOn		X		Log on with the user PIN if system is initialized.

Service	CO	User	Unauthen-ticated	Description
MountCDROM		X		Allows the CDROM drive to be mounted as the read/write drive. This permits the CDROM software to be updated by a user application.
ReadMedia		X		Read user media from SCSI drive.
ReadUserArea	X	X	X	Get a block of data from a specified user area.
SelfTest	X	X	X	Pass/Fail Test of SPYRUS FIPS Sector-based Encryption Module. Will run the Power On Self Tests again.
SetConfig	X			Writes the card configuration structure if the signature on the structure is valid
SetupBasicSecureChannel	X	X	X	Initializes secure channel.
UpdateFirmware	X			Writes signed blocks to the firmware area of the module
WriteMedia		X		Writes user media to SCSI drive.
WriteUserArea		X		Write a block of data to a specified user area. All areas will require the token to be logged on for writes and updates
Zeroize	X	X		Clears the encryption keys. Requires the Initialize command to be run again.

5 Identification and Authentication

5.1 Initialization Overview

The SPYRUS FIPS Sector-based Encryption Module modules are initialized at the factory to be in the zeroized state. Before an operator can access or operate a SPYRUS FIPS Sector-based Encryption Module, the User must first initialize the module with a User ID and PIN.

5.2 Operator Authentication

Operator Authentication is accomplished by PIN entry by the User or valid ECDSA signature by the CO. Once valid authentication information has been accepted, the SPYRUS FIPS Sector-based Encryption Module is ready for operation.

The SPYRUS FIPS Sector-based Encryption Module stores the number of User logon attempts in non-volatile memory. The count is reset after every successful entry of a User PIN. If an incorrect PIN is entered during the authentication process, the count of unsuccessful logon attempts is incremented by one.

If the User fails to log on to the SPYRUS FIPS Sector-based Encryption Module in 10 consecutive attempts, the SPYRUS FIPS Sector-based Encryption Module will block the user's access to the module, by transitioning to the blocked state. To restore operation to the SPYRUS FIPS Sector-based Encryption Module (HPC140-F), the User will have to zeroize the token and reload the User PIN and optional details. When the SPYRUS FIPS Sector-based Encryption Module is inserted after zeroization, it will power up and transition to the Zeroized State, where it can be initialized.

5.3 Generation of Random Numbers

The Random Number Generators are not invoked directly by the user. The Random Number output is generated by the HASH-DRBG algorithm specified in SP 800-90 in the case of static private keys and associated key wrapping keys, ephemeral keys and symmetric keys.

5.4 Strength of Authentication

The strength of the authentication mechanism is stated in Table 5-1 below.

Table 5-1 Strength of Authentication

Authentication Mechanism	Strength of Mechanism
User Single PIN-entry attempt / False Acceptance Rate	The probability that a random PIN-entry attempt will succeed or a false acceptance will occur is 1.66 $x10^{-14}$. The requirement for a single–attempt / false acceptance rate of no more than 1 in 1,000,000 (i.e., less than a probability of 10^{-6}) is therefore met.
User Multiple PIN-entry attempt in one minute	SPYRUS FIPS Sector-based Encryption Module authentication mechanism has a feature that doubles the time of authentication with each successive failed attempt. There is also a maximum bound of 10 successive failed authentication attempts before zeroization occurs. The probability of a successful attack of multiple attempts in a one minute period is 1.66 $x10^{-13}$ due to the time doubling mechanism. This is less than one in 100,000 (i.e., 1×10^{-5}), as required.
Crypto-Officer Single attempt / False Acceptance Rate	The probability that a random ECDSA signature verification authentication attempt will succeed or a false acceptance will occur is 1/2^192. The requirement for a single–attempt / false acceptance rate of no more than 1 in 1,000,000 (i.e., less than a probability of 10^{-6}) is therefore met.
Crypto-Officer Multiple Signature verification attempt in one minute	The probability of a successful attack of multiple ECDSA signature authentication attempts in a one minute period is 1/2^192. The computational power needed to process this is outside of the ability of the module. This is less than one in 100,000 (i.e., 1×10^{-5}), as required.

6 Access Control

6.1 Critical Security Parameters (CSPs) and Public Keys

Table 6-1 SPYRUS FIPS Sector-based Encryption Module CSPs

CSP Designation	Algorithm(s) / Standards	Symbolic Form	Description
Disk Ephemeral Private	SP 800-56A	$d_{e,U}$	ECDH ephemeral private key used to generate shared secret.
Disk Key Encryption Key (DKEK)	AES 256	DKEK	AES key used to unwrap the Disk Encryption Key (DEK).
Drive Encryption Key (DEK)	AES 512	DEK	A pair of AES 256 keys. The concatenated value is used to encrypt and decrypt the User's encrypted drive.
Hash-DRBG Seed	SP 800-90	S	FIPS 186-2-generated seed used to seed the Hash-DRBG RNG.
Hash-DRBG State	SP 800-90	s_{HDRBG}	Hash_DRBG state value
Master Encryption Key (MEK)	AES 256	MEK	AES 256 wraps / unwraps user's static private keys in storage.
Secure Channel HYDRA Private	SP 800-56A	$d_{e,SCHP}$	ECDH Ephemeral Transport Private
Secure Channel Session Key	SP 800-56A	k_{SCSK}	ECDH / AES key used to encrypt and decrypt commands and responses to and from the card.
User PIN		PIN	The user's 7 character PIN for authentication to the module
User's Static Signature Private	X9.62	$d_{ECDSA,s,U}$	ECDSA Static Signature private key
User's Static Transport Private	SP 800-56A	$d_{s,U}$	ECDH Static Transport private key
FIPS 186-2 RNG Seed	Hardware RNG	Seed	Seed value generated for use with the RNGs.

Table 6-2 SPYRUS FIPS Sector-based Encryption Module Public Keys

Key	Algorithm(s) Standards	Description/Usage
Configuration Update Key	ANSI X9.62	The ECDSA P-384 public Key is used to verify the signature of the CO before the settings are changed
Card Firmware Update Key	ANSI X9.62	The ECDSA P-384 public Key is used to verify the signature of the CO before loading firmware.
Disk Ephemeral Public	SP 800-56A	ECDH Ephemeral Transport Public P384. The key is used to generate a shared secret using ECDH with the User's Static Transport Private key.
Secure Channel Host Public	SP 800-56A	ECDH Ephemeral Transport Public P256
Secure Channel HYDRA Public	SP 800-56A	ECDH Ephemeral Transport Public P256. The key is used to generate a shared secret between the host and the card.
User's Static Signature Public	SP 800-56A	ECDH Static Signature Public P384. The key for ECDSA.
User's Static Transport Public	SP 800-56A	ECDH Static Transport Public P384. The key for ECDH.

6.2 CSP Access Modes

Table 6-3 SPYRUS FIPS Sector-based Encryption Module Access Modes

Access Type	Description
Generate (G)	"Generate" is defined as the creation of a CSP
Delete (D)	"Delete" is defined as the zeroization of a CSP
Use (U)	"Use" is defined as the process in which a CSP is employed. This can be in the form of loading, encryption, decryption, signature verification, or key wrapping.

6.3 Access Matrix

The following table shows the services (see section 4.2) of the SPYRUS FIPS Sector-based Encryption Module (HPC140-F), the roles (see section 4.1) capable of performing the service, the CSPs (see section 6.1) that are accessed by the service and the mode of access (see section 6.3) required for each CSP. The following convention is used: if the role column has an 'X', then that role may execute the command.

Table 6-4 SPYRUS FIPS Sector-based Encryption Module Access Matrix

Service Name	Roles		Access to Critical Security Parameters	
	Admin	User	CSPs	Access Mode
ChangePassword		X	k_{SCSK} $d_{s,U}$ $d_{ECDSA,s,U}$ $d_{e,U,}$ DKEK DEK PIN	**U** **U** **U** **U** **G, U, D** **U** **D,G**
Format		X	$d_{e,U}$ DKEK, DEK	**G, U, D** **G,U,D** **G,U**
GetCapabilities	X	X		
GetConfiguration	X	X		
GetUserState	X	X		
Initialize		X	k_{SCSK} $d_{s,U}$ $d_{ECDSA,s,U}$ $d_{e,U,}$ DKEK DEK MEK	**U** **G** **G** **G, U, D** **G, U, D** **G** **U**
LogOff		X		
LogOn		X	k_{SCSK} $d_{s,U}$ DKEK DEK PIN	**U** **U** **G,U,D** **U** **U**
MountCDROM		X	DEK	**U**
ReadMedia		X	DEK	**U**
ReadUserArea	X	X		
SelfTest	X	X	S, S_{HDRBG},	**G**

Service Name	Roles		Access to Critical Security Parameters	
	Admin	User	CSPs	Access Mode
SetConfiguration	X		$d_{s,U}$ $d_{ECDSA,s,U}$ DEK	D D D
SetupBasicSecureChannel		X	$d_{e,SCHP}$ k_{SCSK}	G,D G,D
UpdateFirmware	X		$d_{s,U}$ $d_{ECDSA,s,U}$ DEK	D D D
WriteMedia		X	DEK	U
WriteUserArea		X		
Zeroize	X	X	$d_{s,U}$ $d_{ECDSA,s,U}$ DEK	D D D

7 Self-Tests

The module performs both power-on and conditional self-tests. The module performs the following power-on self-tests:

- Cryptographic Algorithm Tests:
  - AES-128, 192, 256 KATs
  - ECDSA-256, 384, 521 KATs
  - EC-Diffie-Hellman-256, 384, 521 KATs
  - SHA-224 KAT
  - SHA-256 KAT
  - SHA-384 KAT
  - SHA-512 KAT
  - HASH-DRBG KAT
  - FIPS 186-2 RNG KAT (includes SHA-1 KAT)
- Firmware Test
  - SHA-384 Hash

The module performs the following Conditional Tests:

- Firmware Load Test
  - ECDSA P-384 signed SHA-384 hash verification
- Pairwise Consistency Test
  - ECDSA key pair generation
  - EC-Diffie-Hellman key pair generation
- Continuous Random Number Generator Test
  - HASH-DRBG SP800-90
  - FIPS 186-2 RNG
  - NDRNG

8 Mitigation of Other Attacks

No claims of mitigation of other attacks listed in Section 4.11 of FIPS 140-2 by the SPYRUS FIPS Sector-based Encryption Module are made or implied in this document.

9 Acronyms and References

Acronyms

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSP	Critical Security Parameter
DPA	Differential Power Analysis
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECMQV	Elliptic Curve Menezes-Qu-Vanstone
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interface
FEK	File Encryption Key
FIPS	Federal Information Processing Standard
HAC	Host Authentication Code
MKEK	Master Key Encryption Key
NDRNG	Non-deterministic Random Number Generator
PC	Personal Computer
PCB	Printed Circuit Board
PIN	Personal Identification Number
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman Algorithm
SD	Secure Digital (flash memory card)
SDHC	Secure Digital High-capacity
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
SSD	Solid-state Drive
USB	Universal Serial Bus

References

FIPS 140-2	FIPS PUB 140-2, Change Notice, Federal Information Processing Standards Publication (Supersedes FIPS PUB 140-1, 1994 January 11) **Security Requirements For Cryptographic Modules,** Information Technology Laboratory, National Institute of Standards and Technology (NIST), Gaithersburg, MD, Issued May 25, 2001.
FIPS 186-2	**FIPS PUB 186-2,** (+ Change Notice), Federal Information Processing Standards Publication **DIGITAL SIGNATURE STANDARD (DSS),** National Institute of Standards and Technology (NIST), Gaithersburg, MD, Issued 2000 January 27
SP 800-56A	NIST Special Publication 800-56A **Recommendation for Pairwise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised),** Barker, E., Johnson, D., Smid, M., Computer Security Division, NIST, March 2007.
SP 800-90	NIST Special Publication 800-90 **Recommendation for Random Number Generation Using Deterministic Random Bit Generators,** Barker, E., Kelsey, J., Computer Security Division, Information Technology Laboratory, NIST, June 2006.
X9.62	American National Standards Institute (ANSI) **Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA),** 2005.

