SPYCOS® Module Security Policy

Revision: 1.3

SECURED BY SPYRUS™

SPYRUS Document number: 550-051001-04

This document is provided only for informational purposes and is accurate as of the date of publication. This document may be copied subject to the following conditions:

- All text must be copied without modification and all pages must be included.
- All copies must contain the SPYRUS copyright notices and any other notices provided herein.

Trademarks
SPYRUS, the SPYRUS logos, Hydra Privacy Card, Hydra PC and Hydra PC Locksmith are either registered trademarks or trademarks of SPYRUS, Inc. in the United States and/or other countries.

All other trademarks are the property of their respective owners.

Contents

1 Introduction

This Security Policy specifies the security rules under which the SPYCOS® MODULE operates. The Acronym SPYCOS stands for "SPYRUS Cryptographic Operating System". 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 the modules:

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

1.1 SPYCOS® MODULE Overview

The SPYCOS® MODULE is the latest addition to the SPYRUS family of cryptographic module ICs that enable both smart card and USB cryptographic tokens.

The SPYCOS® MODULE IC enables security critical capabilities such as user authentication, message privacy and integrity, authentication, and secure storage in tamper-evident protective coating. The SPYCOS® MODULE communicates with a host computer via the smart card or USB interface.

1.2 SPYCOS® MODULE Implementation

The SPYCOS® MODULE is implemented as a single-chip module as defined by FIPS 140-2.

The SPYCOS® MODULE is available with an ISO 7816 smart card module with standard interface *OR* a mounted package with product name: Rosetta Micro. It is also supplied as individual modules on a reel for embedding / surface mounting etc. All Interfaces have been tested and are compliant with FIPS 140-2.

Product Identification (including unique part number) for the SPYCOS® MODULE is shown in the table below:

Form Factor	**Part Number**	**FW Version**
Rosetta Smart Card Module	740100002F	2.4
Rosetta Micro	742100002F	2.4

Photographs of the above form factors are shown in the figures below:

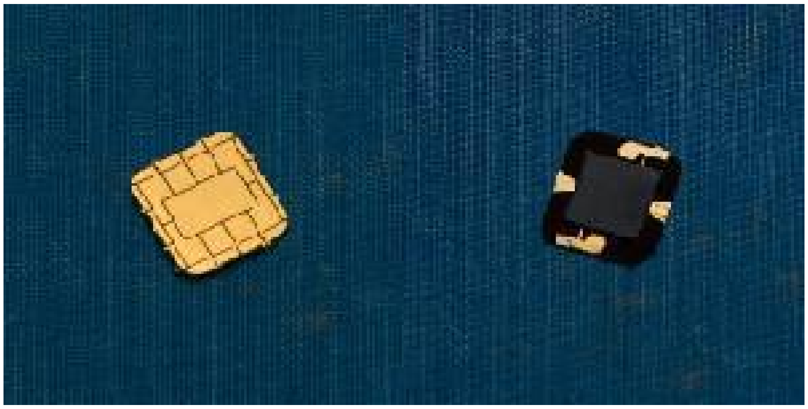

Figure 1 SPYCOS® MODULE Smart Card Module

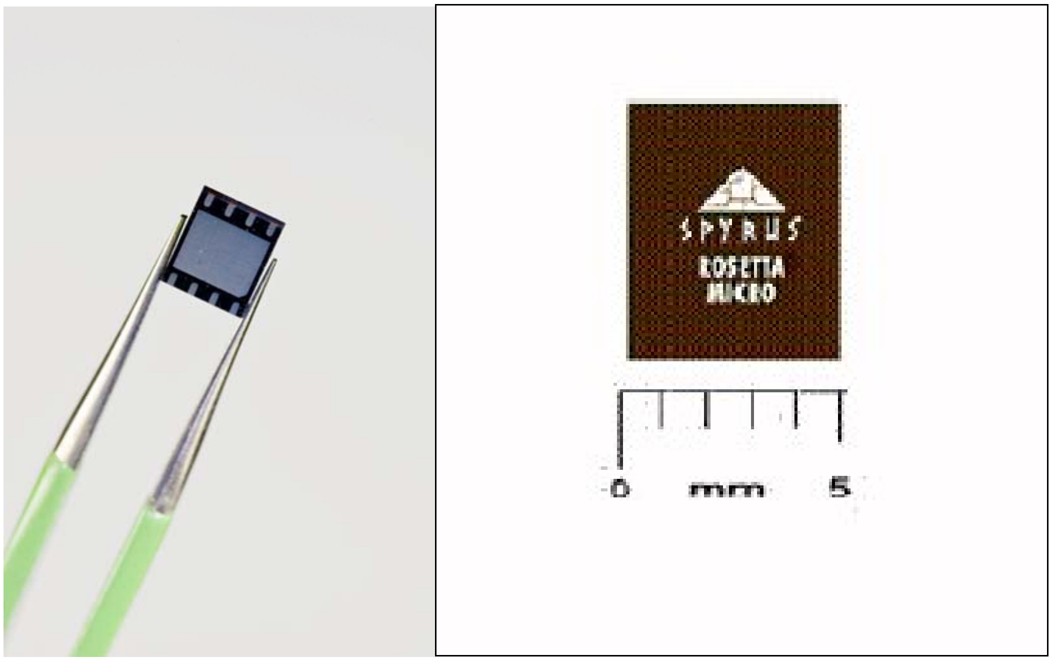

Figure 2 Rosetta® Micro® Form Factor

1.3 SPYCOS® MODULE Cryptographic Boundary

The Cryptographic Boundary is defined to be the physical perimeter of the SPYCOS® MODULE IC and the potting material it is embedded in.

No hardware, firmware, or software components that comprise the SPYCOS® MODULE are excluded from the requirements of FIPS 140-2.

1.4 Approved Mode of Operation

The SPYCOS® MODULE approved mode of operation is comprised of the SPYCOS® MODULE command set. All commands that use FIPS 140-2 approved security functions (e.g. algorithms) are defined to be in the "approved mode of operation."

Approved mode of operation commands which are successfully completed will return a standard success return code. The command Get FIPS returns a Boolean value "1" confirming the system is in the approved mode (see Table 3-1). Services available under the approved mode of operations are detailed in Table 3-1 of this Security Policy.

The module only operates in an approved mode of operation. The Error return codes are dependent upon the cause of the failure.

The SPYCOS® MODULE supports the following FIPS 140-2 approved or allowed algorithms:

Table 1-1 SPYCOS 2.4 Approved or Allowed Algorithms

Encryption & Decryption	**Certificate #**
Triple DES	699
AES	842
Skipjack	18
Key Wrap & Unwrap	
RSA (key wrapping / key establishment methodology provides 80 and 112 bits of encryption strength)	404
Digital Signatures	
ECDSA (sign only), RSA (sign and verify)	95, 404
Message Authentication Code	
HMAC	463
Hash	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	834
RNG	
FIPS 186-2 (Appendix 3.1 Change Notice) RNG	481
Key Agreement / Key Establishment	
ECDH, ECMQV (key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)	--

The following services are available as “non-approved” algorithms:

Table 1-2 SPYCOS 2.4 Non-approved Algorithms

RNG
HW NDRNG
RNG
Firmware Random Number Generator (FWRNG)

1.5 FIPS 140-2 Security Levels

The SPYCOS® MODULE cryptographic module complies with the requirements for FIPS 140-2 validation to the levels defined in Table 1-3. The FIPS 140-2 overall rating of the SPYCOS® MODULE is Level 3.

Table 1-3
FIPS 140-2 Certification 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
14. Cryptographic Module Security Policy	3
Overall Security Level	3

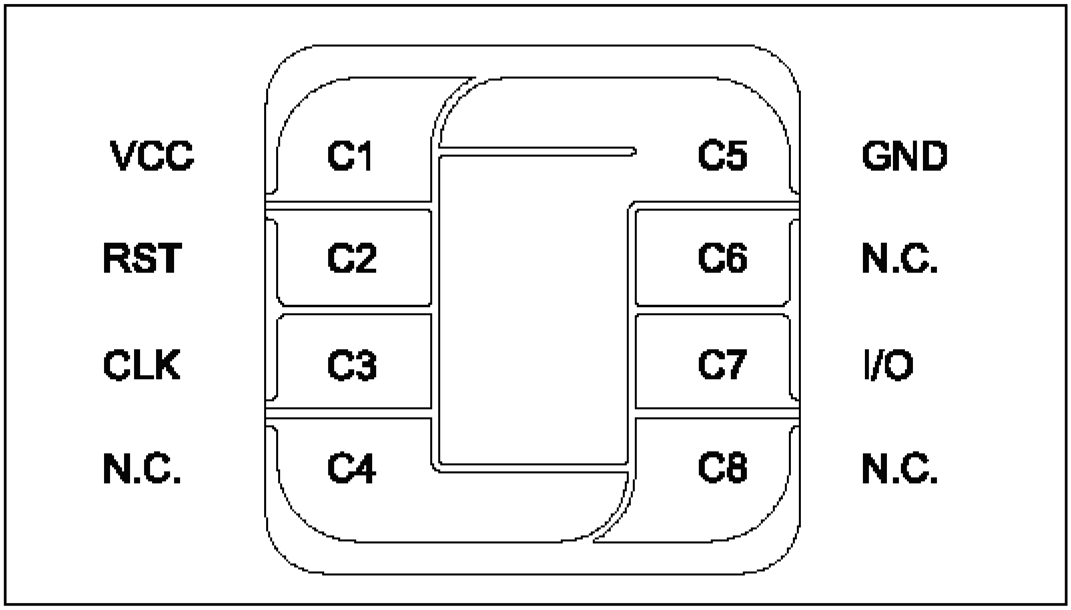

Figure 3 SPYCOS® Module PIN Configuration

2 Ports and Interfaces

The pin configuration of the SPYCOS® MODULE cryptographic module is shown in Figure 3. The pins form a set of 8 contact points that comprise the only electronic interface with external devices. They are the sole externally visible portion of the microprocessor assembly. Only 5 of the 8 pins are active: C4, C6 and C8 are not connected (N.C.). The remaining pins perform the following functions:

Pin	Function	FIPS 140-2 Logical Interface
C1	Operating voltage	Power Interface
C2	Reset input	Control Input
C3	Processor clock input	Control Input
C5	Ground	N/A
C7	Bi-directional data port	Data Input / Data Output; Status

As is standard, the physical interface that connects the integrated circuit chip to the card acceptor device (CAD) is limited to a 9600 bits per second rate of data transfer. This communication line is a full duplex serial transmission line and conforms to ISO standard 7816/3. The central processing unit controls all data exchanges between the SPYCOS® MODULE cryptographic module and the CAD. Card commands and data are sent to the microprocessor and responses are issued by the microprocessor upon receipt of the commands and/or data. Responses take the form of standard status words.

Information sent from the SPYCOS® MODULE cryptographic module to the CAD is issued in a half duplex transmission mode. Transmission of data is therefore carried on in one direction only at any given time. Data flooding attacks are prevented by the protocol and restrictive data transmission rate of the card.

3 Roles and Services

The SPYCOS® MODULE supports two roles, Crypto-officer (CO) and User, and enforces the separation of these roles by restricting the services available to each one.

Crypto-officer Role: The Crypto-officer is responsible for initializing the SPYCOS® MODULE. Before issuing a SPYCOS® MODULE to an end user, the Crypto-officer initializes the SPYCOS® MODULE with private keying material and certificate information. The Crypto-officer cannot use private keys loaded on the module. The SPYCOS® MODULE validates the Crypto-officer identity before accepting any initialization commands. The Crypto-officer is also referred to as the Site Security Officer (SSO).

User Role: The User role is available after the SPYCOS® MODULE has been loaded with a User personality. The user can load, generate and use private keys.

The SPYCOS® MODULE validates the User identity before access is granted.

3.1 Services

The following table (Table 3-1) describes the services provided by the SPYCOS® MODULE. The User/SSO column denotes the roles that may execute the service.

Table 3-1
SPYCOS® MODULE Services

Service	Description	User / SSO
ASYMMETRIC SIGNATURE	Signs data using RSA or ECDSA signing key	User
BLOCK PIN	This command is used to block a PIN register. This command can only be executed after the principal assigned as the blocking/unblocking master has been authenticated (see the PIN file format for additional details).	User, SSO
CHANGE PIN	Enables the SSO to change either the User PIN or SSO PIN. The SSO must provide the original and new PIN phrases. When the user PIN is successfully changed or the command fails, the SSO is automatically logged out.	User or SSO
CHECK PIN	Inputs a PIN Phrase to authenticate the SSO or the User.	User, SSO
CREATE FILE	Create a Dedicated File (DF) or Elementary File (EF) providing the parent directory access conditions for the create command have been fulfilled.	User or SSO
DELETE FILE	Delete a file, directory. In the non-recursive mode a DF containing files or directories will not be deleted. In the recursive mode a DF and all of its contents are deleted (provided the parent directories access conditions for the "Delete" command have been fulfilled). The recursive form of this command is used to achieve zeroization.	User or SSO
LOAD-DELETE KEY	Deletes keys, or loads keys internally from file system (but not externally).	User, SSO
DIRECTORY	Retrieves a directory listing from the current directory and sub-directories if the recursive mode is used (providing appropriate access conditions have been fulfilled)	User or SSO
DISABLE FILE	Disable all operations on this file. The file can still be selected and the status information can still be retrieved, however its contents cannot be accessed. This command is valid on all ISO/IEC 7816-4 files: i.e., Master File (MF), Dedicated File (DF), or Elementary File (EF). If the MF is invalidated, the only valid commands are: Select, Status, Get Response and Rehabilitate.	User, SSO
ECDSA SIGN	Computes a digital signature using the ECDSA algorithm using the hash value passed to the card. The private key of the currently selected personality is used for this computation.	User
ENABLE FILE	Enable a previously disabled file. If executed on a file that is not disabled, no change is made to the file	User, SSO

Service	Description	User / SSO
	state and the command returns a success response code.	
ERASE FILE	Erase a file.	User, SSO
ESTABLISH DH SHARED SECRET	Generates a Diffie-Hellman shared secret Z and returns it to the caller.	User
EXTEND FILE	Extend the length of a file or directory. Valid only on a DF, or EF (not valid on MF). Space is allocated from the current parent DF.	User or SSO
EXTERNAL AUTHENTICATE	TDES authentication for SSO, to support a challenge-response protocol on external platforms.	SSO
GENERATE ASYMMETRIC KEY	Generic RSA or ECC key generator. The command requires the User to have created the private keying file (with appropriate access controls) prior to issuing this command.	User, SSO
GENERATE RANDOM	Generate a random number and return the value in the Data Out-Block. This will also handle the generation of Initialization Vectors (IVs) and Message Encryption Keys (MEKs).	User, SSO
GENERATE OATH ONE-TIME PASSWORD	Generates a one-time password for external use.	User, SSO
GET CHALLENGE	Get a nonce for the EXTERNAL AUTHENTICATE command.	User, SSO
GET FILE STATUS	Allows the SSO or user to obtain the current status of the File. Gets the information for a given file or directory (file id, size, type access permissions and related information).	User, SSO
GET FIPS	Responds with status response “1” indicating that the module is in the FIPS-approved mode.	User, SSO
GET RESPONSE	Retrieve the module response. Provides a generic method for transmitting APDU(s), or part of APDU(s) from the card to the application when the available protocols cannot be used.	User, SSO
GET RSA PUBLIC KEY	This command returns public information associated with the currently selected RSA key pair. The information returned is the key type, size and public modulus. Also retrieves the public key.	User, SSO
HASH DATA	Generate the SHA-1, SHA-2 Hash of a message or data object	User
HMAC DATA	Generates a HMAC message authentication code.	User
LOAD CRYPTOGRAPHIC DATA	Supports RSA and EDSA signature verification as well as the RSA Wrap Key command.	User, SSO
READ BINARY	Performs a binary read from a file, given the offset and length.	User, SSO
RSA SIGN	Signs a message or data object using either RSA signature	User

Service	Description	User / SSO
RSA VERIFY SIGNATURE	Verifies the RSA signature on a message.	User
RSA WRAP KEY	Facilitates public key exchange of an MEK. This function uses the public key information that was downloaded with the Load Cryptographic Data command.	User, SSO
SECURE UPDATE BINARY	Update the data in the currently selected EF with the data provided. The data is secured using message encryption, storage encryption or a combination of both.	User, SSO
SELECT FILE	Sets a current file within a logical channel. This could, for example, allow for the application to make further implicit EF file selections, based on the selected DF.	User or SSO
SELF TEST	Performs all power-on self-tests and responds with success or, on failure, transition to Error State. Selection of individual self-tests or all self-tests is a user option using bit flags in the parameter field.	User or SSO
SET KEY POINTER	Sets one of the 3 key pointers to the key registers. Facilitates setting an MEK to be the first, second or third key for use with the TDES engine.	User, SSO
SYMMETRIC DECRYPT	Supports symmetric cryptographic decryption modes.	User
SYMMETRIC ENCRYPT	Supports symmetric encryption modes.	User
UNBLOCK PIN	Allows a PIN that has been blocked using the BLOCK PIN command or after too many unsuccessful CHECK PIN attempts to be unblocked. This is so providing the master PIN data associated with the blocked PIN is correct (mode=0) or has been correctly provided in a previous CHECK PIN command (during the same session).	SSO
UPDATE BINARY	The UPDATE BINARY command updates the data in the currently selected EF with the data provided.	User or SSO
ZEROIZE	To zeroize the module, a recursive DELETE FILE is performed	User, SSO

4 Identification and Authentication

4.1 Initialization Overview

The SPYCOS® MODULE IC hardware security modules (HSMs) are initialized at the factory with a Default SSO PIN Phrase. The SSO (Site Security Officer) must change the default value during logon to make the module ready for initialization. During initialization the module allows the execution of only the commands required to complete the initialization process.

Before a user can access or operate the module, the SSO must initialize it with the user PIN. The SSO is authorized to log on to the module any time after initialization to change parameters. The module allows 10 consecutive failed SSO logon attempts before it zeroizes all key material and initialization values. In the *zeroized* state, the SSO must use the Zeroize PIN Phrase to log on to the module and must reinitialize all module parameters.

A user must log on to a module to access any on-board cryptographic functions. To log on the user must provide the correct User PIN. The module allows 10 consecutive failed logon attempts before it blocks the stored User PIN. User information stored in the module in non-volatile memory remains resident.

4.2 Authentication

The SPYCOS® MODULE implements identity-based authentication which is accomplished by PIN entry by the operator. On invocation by the user, the SPYCOS® MODULE waits for authentication of the user or SSO role by entry of a PIN phrase. There is only one user and one SSO PIN allowed per module. Multiple user and SSO accounts are not permitted. Once a valid PIN phrase has been accepted the SPYCOS® MODULE cryptographic services may be accessed. The CheckPIN command includes the user's PIN as a parameter. When this command is received by the Module, the PIN value is used to generate a Skipjack key that is used to decrypt a validation phrase. If successful, the user gains access to the module.

The SPYCOS® MODULE stores the number of logon attempts in non-volatile memory. The count is reset after every successful entry of a User PIN Phrase by a user and after every successful entry of the SSO PIN Phrase by the SSO. If the user fails to logon to the SPYCOS® MODULE in 10 consecutive attempts, the SPYCOS® MODULE will zeroize the User PIN and then transitions to a state that is initialized only for the SSO to perform restorative actions. . To restore operation to the SPYCOS® MODULE, the SSO will have to reload the initialization parameters and User PIN phrase. If the SSO Enabled User fails to logon to the SPYCOS® MODULE in 10 consecutive attempts, the SPYCOS® MODULE will block all of the certificates, Private Components, Key Registers and disallow User access. When the SPYCOS® MODULE is inserted after a zeroize, it will power up and transition to the Zeroized State, where it will only accept the Zeroize Default PIN phrase. After the Zeroize Default PIN phrase has been accepted, the SPYCOS® MODULE transitions to the Uninitialized State and must be reinitialized, as described in section 6.

4.3 Strength of Authentication

The strength of the authentication mechanism conforms to the following specifications.

Table 4-1 Strength of Authentication

Authentication Mechanism	Strength of Mechanism
Single PIN-entry attempt / False Acceptance Rate	The probability that a random 20-byte PIN-entry (using only 93 keyboard characters[1]) attempt will succeed or a false acceptance will occur is 4.269 x 10^{-40}. 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.
Multiple PIN-entry attempt in one minute	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 no more than 4.269 x 10^{-39} due to the maximum of 10 attempts. This is less than one in 100,000 (i.e.,1×10^{-5}), as required.

4.3.1 Obscuration of Feedback

Feedback of authentication data to an operator is obscured during authentication (e.g., no visible display of characters result when entering a password). The PIN value is input to the CheckPIN command as a parameter by the calling application. No return code or pointer to a return value that contains the PIN is provided.

4.3.2 Non-weakening Effect of Feedback

Feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism. The only feedback provided by the CheckPIN command is a return code denoting success or failure of the operation. This information in no way affects the probability of success or failure in either single or multiple attacks.

[1] The character set available for PINs is at least all alphanumeric characters (upper and lower cases) and 31 special keyboard characters comprising the set {~ ! @ # $ % ^ & * ( ) _ + - = { } [ ] | \ : ; " ' < , > . ? /}.

4.3.3 Generation of Random Numbers

The Generate Random Number command can be invoked only after authentication of the user. The FIPS 186-2 (Change Notice version) algorithm is used for all authenticated RNG calls.

5 Key Management

5.1 CSP Management

Table 5-1
SPYCOS® MODULE CSPs

CSP Designation	Type	Generate / Input	Output	Storage	Use
ECDSA Private Key	X9.62	Generate Asymmetric Key command	None	EEPROM storage	The Private Key of the User employed in Elliptic Curve digital signing operations.
EC-keypair	SP 800-56A	Generated ECDH / ECMQV variables using FIPS 186-2 RNG	Establish DH shared secret command; Authentication PIN transmission	Transient in RAM	Used in ECDH / ECMQV key agreement
Secure Channel Session Key	SP 800-56A	Generated by ECDH	None	Transient in RAM	ECDH / TDES key used to encrypt and decrypt PIN data transmitted to the module.
HMAC Key	FIPS 198 Key	Generated by the FIPS 186-2 RNG	None	Key Register	Used to generate HMAC message authentication code
Message Encryption Key (MEK)	AES, TDES	Generated by the FIPS 186-2 RNG	None	Key Register	Generated by the SPYCOS® MODULE RNG for data encryption
RNG Key	FIPS 186-2 XKEY	Generated by the Hardware NDRNG	None	Transient in RAM	Used to seed the FIPS 186-2 RNG.
RNG Seed	FIPS 186-2 XSEED	Generated by the	None	Transient in RAM	Used to seed the FIPS 186-2 RNG.

CSP Designation	Type	Generate / Input	Output	Storage	Use
		Hardware NDRNG, GenRandom			
RSA Private Key[2]	X9.31	Generate Asymmetric Key command	None	EEPROM storage	The Private Key of the User employed in RSA digital signing operations or wrapping keys.
SSO PIN Phrase	20-byte PIN	CheckPIN, ChangePIN parameter	None	Not Stored	A secret 20 byte value used for SSO authentication.
Storage Key	SKIPJACK	Generated by the FIPS 186-2 RNG	None	In plaintext in EEPROM	Used to encrypt all asymmetric private keys stored in internal memory
User PIN Phrase	20-byte PIN	CheckPIN, ChangePIN parameter	None	Not Stored	A secret 20 byte value used for user authentication.

5.2 Public Key Management Parameters

Table 5-2
SPYCOS® MODULE Public Key Management Parameters

Key Management Parameter	Type	Generate / Input	Output	Storage	Use
ECDSA Public Key	X9.62	GENERATE ASYMMETRIC KEY command	GENERATE ASYMMETRIC KEY command	EEPROM storage	The Public Key of the User employed in Elliptic Curve digital signing operations.
RSA Public Key	X9.31	GENERATE ASYMMETRIC KEY command	GET RSA PUBLIC KEY command; GENERATE ASYMMETRIC KEY command	EEPROM storage	The Public Key of the User employed in RSA digital signing operations.

[2] RSA key pair use varies with the user application. Some keys are used for signatures and some for encryption / key wrapping.

5.3 CSP Access Matrix

The following table (Table 5-3) shows the services (see section 3.1) of the SPYCOS® MODULE, the roles (see section 3) capable of performing the service, the CSPs (see section 5.1) that are accessed by the service and the mode of access (see next paragraph) required for each CSP. The following convention is used: If only one of the roles applies to the service, that role appears alone. If both roles may execute the service, then “User, SSO” is indicated. If either one (but not the other) then “User or SSO” is indicated. In the last option it is a matter of organizational policy which of the rules may execute the service.

Access modes are R (read), W (write) and E (execute). Destruction is represented as a W.

Table 5-3
SPYCOS® MODULE Access Matrix

Service	User / SSO	Access Type	CSP Acess
ASYMMETRIC SIGNATURE	User	R,E	RSA/ECDSA Private Key
BLOCK PIN	User or SSO	E	User PIN, SSO PIN
CHANGE PIN	User or SSO	W,E	User PIN, SSO PIN
CHECK PIN	User, SSO	R,E	User PIN, SSO PIN
CREATE FILE	User or SSO	N/A	N/A
DELETE FILE	User or SSO	N/A	N/A
LOAD-DELETE KEY	User, SSO	W	AES/TDES Secret Key
DIRECTORY	User or SSO	N/A	N/A
DISABLE FILE	User, SSO	N/A	N/A
ECDSA SIGN	SSO	W	ECDSA Private Key
ENABLE FILE	User, SSO	N/A	N/A
ERASE FILE	User, SSO	N/A	N/A
ESTABLISH DH SHARED SECRET	SSO	W,E	EC keypair, Secure Channel Session Key
EXTEND FILE	User or SSO	N/A	N/A
EXTERNAL AUTHENTICATE	SSO	R	TDES Secret Key
GENERATE ASYMMETRIC KEY	User, SSO	W	RSA/ECDSA Private Key
GENERATE RANDOM	User, SSO	R,W	XSEED, XKEY
GENERATE OATH ONE-TIME PASSWORD	User	W	N/A
GET CHALLENGE	SSO	N/A	N/A
GET FILE STATUS	User, SSO	N/A	N/A
GET FIPS	User, SSO	N/A	N/A
GET RESPONSE	User, SSO	N/A	N/A
GET RSA PUBLIC	User, SSO	N/A	N/A

Service	User / SSO	Access Type	CSP Acess
KEY			
HASH DATA	User	N/A	N/A
HMAC DATA	User	R,E	HMAC Key
LOAD CRYPTOGRAPHIC DATA	User, SSO	R	RSA Private Key
READ BINARY	User or SSO	N/A	N/A
RSA SIGN	SSO	W	RSA Private Key
RSA VERIFY SIGNATURE	SSO	N/A	N/A
RSA WRAP KEY	SSO	W	RSA Private Key
SECURE UPDATE	User	R,E	AES Secret Key
SECURE UPDATE BINARY	User or SSO	R,E	RSA Private Key
SECURE UPDATE ENCRYPTED	User	R,E R,E	AES Secret Key, RSA Private Key
SELECT FILE	User or SSO	N/A	N/A
SELF TEST	User or SSO	E	RSA Private Key, ECDSA Private Key HMAC Key RNG Key RNG Seed RSA Private Key
SET KEY POINTER	User	N/A	N/A
SYMMETRIC DECRYPT	User	R,E	AES/TDES Secret Key
SYMMETRIC ENCRYPT	User	R,E	AES/TDES Secret Key
UNBLOCK PIN	SSO	W	User PIN, SSO PIN
UPDATE BINARY	User or SSO	N/A	N/A
ZEROIZE	User, SSO	W	AES Secret Key, TDES Secret Key, RSA Private Key, ECDSA Private Key Secure Channel Session Key HMAC Key Message Encryption Key (MEK) RNG Key RNG Seed RSA Private Key Storage Key

5.4 Destruction of Keys and CSPs

The module has the ability to destroy all keys and CSPs by a recursive DELETE FILE command. All keys and CSPs are stored in files. The contents of the file(s) being recursively deleted are erased and over written. Should a power-down occur during the execution of the recursive DELETE FILE, the action of zeroization will resume on a subsequent power-on event, ensuring that access to zeroized information is prevented.

6 Setup and Initialization

The uninitialized module has only a root directory with minimal version and manufacturing information in specific files. There is no information pertaining to the user or SSO or their authentication data, such as PINs, stored on the uninitialized module as shipped to the customer.

Initialization of the module is accomplished by setting up a security domain by way of the following actions:

- The SSO creates a new application directory on the module;
- The SSO creates a PIN file that is associated with the SSO and User;
- The SSO initializes the PIN files by writing an encrypted authentication key to the file. No PIN information is ever written to the PIN file.
- The SSO may optionally set a default PIN or set the user PIN:
    - If the user PIN is set by the SSO, the user will not be able to change their PIN.
- The SSO uses Get FIPS to confirm FIPS mode

The module is now in FIPS mode and operators may logon with the CheckPIN command. See Section 4.2 for a description of the CheckPIN process. If organizational policy permits, the User may execute the ChangePIN command to change his/her PIN. Otherwise the SSO may change the PIN of the user when required.

7 Physical Security

The following module physical packages are available:

- Rosetta Micro
- Rosetta Smart Card Module

The module is packaged to meet FIPS 140-2 Level 3 Security for 2 package formats. The chip is packaged with physical security mechanisms that destroy the chip if physical attacks are launched against it. This is achieved using a hard, opaque, tamper-evident coating on the chip.

8 Self-Tests

The module performs both power-on and conditional self-tests. The power-on self-tests run automatically when power is restored to the module, without requiring any actions or inputs from the user. The module performs the following power-on self-tests:

- Firmware Integrity Test with CRC-16
- Cryptographic algorithm known answer tests (KAT) for:
  - Triple-DES (encrypt-decrypt)
  - AES (encrypt-decrypt)
  - Skipjack (encrypt-decrypt)
  - ECDSA (sign)
  - RSA (sign – verify)
  - HMAC (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)
  - FIPS 186-2 deterministic random number generator.

The module performs the following conditional tests:

- Pairwise consistency test for ECDSA
- Pairwise consistency test for RSA
- Continuous test for non-approved and approved random number generators.

Note that the use of the SELF TEST service (see Table 3-1) allows the user or SSO to perform any or all of the above tests on demand.

9 Cryptographic Officer and User Guidance

9.1 Setup and Initialization

See Section 6.

9.2 Identification and Authentication Policy

The table below (Table 9-1) describes the type of authentication and the authentication data to be used by operators, by role. For a description of the roles, see section 3.

Table 9-1 Identification and Authentication Roles and Data

Role	Type of Authentication	Authentication Data – (Strength)
Administrator	Manual Login	PIN (20 Bytes)
User	Manual Login	PIN (20 Bytes)

10 Mitigation of Other Attacks

The module is not claimed to mitigate against any specific attacks.