# Sun Microsystems
# Sun Cryptographic Accelerator 4000
### Firmware Version 1.1

# FIPS 140-2 Non-Proprietary Security Policy

**Level 3 Validation**

**August 6, 2004**

# Table of Contents

**INTRODUCTION ........ 3**

Purpose ........ 3
References ........ 3
Document Organization ........ 3

**SUN CRYPTOGRAPHIC ACCELERATOR 4000 ........ 4**

Overview ........ 4
Module Interfaces ........ 4
Roles and Services ........ 5
*Crypto Officer Role ........ 5*
*User Role ........ 6*
*Driver Role ........ 8*
*Admin Secure Channel ........ 10*
*Unauthenticated Services ........ 10*
Physical Security ........ 12
Cryptographic Key Management ........ 12
*Random Number Generator ........ 15*
*Key Zeroization ........ 15*
EMI/EMC ........ 16
Self-Tests ........ 16
Design Assurance ........ 17

**SECURE OPERATION ........ 18**

Crypto Officer Guidance ........ 18
*Initialization ........ 18*
*Termination ........ 19*
User Guidance ........ 19

**ACRONYMS ........ 19**

# Introduction

## *Purpose*

This is a non-proprietary Cryptographic Module Security Policy for the Sun Cryptographic Accelerator 4000 from Sun Microsystems. This security policy describes how the Sun Cryptographic Accelerator 4000 meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 3 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

## *References*

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Sun Microsystems website (www.sun.com) contains information on the full line of products from Sun Microsystems.

- The NIST Validated Modules website (http://csrc.ncsl.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

## *Document Organization*

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Sun Microsystems Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Sun Microsystems. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Sun Microsystems and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Sun Microsystems.

# SUN CRYPTOGRAPHIC ACCELERATOR 4000

## *Overview*

The Sun Cryptographic Accelerator 4000 (SCA 4000) is designed to provide the highest level of security to customers. The Sun Cryptographic Accelerator 4000 and secure key store is not defined to be secure as an afterthought, security has been incorporated into the Sun Cryptographic Accelerator 4000 since product inception. The SCA 4000 comes with either a copper or Fiber interface to provide networking services. The hardware version numbers of the module are 501-6040-02 and 501-6040-03 (Fiber), 501-6039-05 and 501-6039-06 (UTP/Copper)

In order to achieve such a high level of security, the Sun Cryptographic Accelerator 4000 product design, development, test and production has satisfied the requirements to ensure a secure product. Security has been the focus of the development team from the outset, and the Sun Cryptographic Accelerator 4000 product has been designed from the ground up to incorporate security in all design and development steps.

The Sun Cryptographic Accelerator 4000 integrates a 1GB Ethernet performance with hardware cryptographic functionality. The card enhances server network performance by off-loading computer intensive cryptographic calculations (asymmetric and symmetric) from the server's CPU, accelerating both IPsec and SSL/TLS processing. The SCA 4000 also provides a secure remote administration capability. It is tightly integrated with Sun's server hardware and software.

## *Module Interfaces*

The cryptographic boundary of the Sun Cryptographic Accelerator 4000 is defined by the perimeter of the PCI card itself. The networking components and interfaces, LED indicators and jumper pins are excluded from the security requirements of FIPS 140-2. The module is accessible only through well-defined interfaces, and these interfaces include a PCI slot, LEDs, and a jumper.

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

| Module Physical Interface | FIPS 140-2 Logical Interface |
|---|---|
| PCI, UTP/fiber interface | Data Input Interface |
| PCI, UTP/fiber interface | Data Output Interface |
| PCI, Jumper | Control Input Interface |
| PCI, LEDs | Status Output Interface |
| PCI | Power Interface |

**Table 1 – FIPS 140-2 Logical Interfaces**

## *Roles and Services*

The module supports identity based authentication. There are three main roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto Officer role (or Security Officer role as defined in SCA 4000 documents), User role, and a Driver. There is also an additional set of unauthenticated services which are not security relevant to the Sun Cryptographic Accelerator 4000 card.

The Crypto-Officer accesses the module using a command line interface (CLI) over the PCI port using the administration tool, vcaadm, on the host machine. The Crypto Officer authenticates with a password and is able to configure the module. When vcaadm is executing in interactive mode, a sub-shell style interface is supplied that allows the Crypto Officer to interact with the interface. Commands may be entered one at a time, and the output from the commands is sent to standard output device.

There are 4 registers that execute the CO administration at the PCI interface level. There are 2 command buffers that perform data input from the card to the host machine and 2 command buffers that receive a response from the host machine. All administrative commands from the application level are sent encrypted with AES session keys using these 4 registers. To issue a command, the host driver uses these registers to define a command block on the host and generates an interrupt to the SCA 4000 firmware via the command bit of the SCA 4000 IRQ register. When the firmware has finished processing the command, it will notify the host via command complete bit of the Host IRQ register.

### *Crypto Officer Role*

The Crypto Officer role has the ability perform all the management and the administration of the board. Descriptions of the services available to the Crypto Officer role are provided in the table below.

| Service | Description | Input | Output |
|---|---|---|---|
| Backup | Backup master key | Command and path | Status of command over secure admin channel |
| Connect | Begin admin session w/ firmware | Command | Login prompt |
| Create | Creates users and CO accounts | Command and user name | Status of command over secure admin channel |
| Delete | Delete users and CO accounts | Command and user name | Status of command over secure admin channel |
| Diagnostics | Runs diagnostics for the card | Command | Status of command over secure admin channel |
| Disable | Disable a user | Command and user name | Status of command over secure admin channel |
| Enable | Enable a user | Command and user name | Status of command over secure admin channel |
| Exit | Exit vcaadm | Command | Status of command over secure admin channel |

| Service | Description | Input | Output |
|---|---|---|---|
| Loadfw | Load new firmware | Command and path | Status of command over secure admin channel |
| Logout | Logout current session | Command | Exit command line |
| Quit | Exit vcaadm | Command | Status of command over secure admin channel |
| Rekey | Generate new master key or remote access key | Command and select option | Status of command over secure admin channel |
| Reset | Reset the hardware | Command | Hardware is reset |
| Set | Change password for crypto officer, set password strength | Command and select option | Options to change password or set password strength |
| Show | Show system settings | Command and select option | Status of command over secure admin channel |
| Zeroize | Delete all keys and reset board | Command | INIT led is off |

**Table 2 – Crypto Officer Services, Descriptions, Inputs and Outputs**

*User Role*

The User role can perform cryptographic operations such as owning and accessing keying material within the key store. Users can also perform bulk encryption, asymmetric encryption, and object management services for cryptographic acceleration. Service descriptions and inputs/outputs are listed in the following tables:

| Service | Description | Input | Output |
|---|---|---|---|
| 3DES Encryption | Raw 3DES encryption | Plaintext data | Ciphertext data |
| 3DES Decryption | Raw 3DES decryption | Ciphertext data | Plaintext data |
| HMAC-SHA1 | HMAC-SHA1 processing | Ciphertext data | Hashed data |
| MD5 HMAC | MD5 HMAC processing | Ciphertext data | Hashed data |
| MD5 | MD5 hashing | Plaintext/ciphertext data | Perform MD5 hashing |
| SHA-1 | SHA-1 hashing | Plaintext/ciphertext data | Perform SHA-1 hashing |
| Diagnostics | Perform diagnostics on the SCA 4000 card | Command | Blinking of LED |
| Display | Display public key information | Command | Displaying the public key and the public key fingerprint used by the Cryptographic Accelerator 4000 board for securing administration sessions. |
| Status | Displays status of keystore information | Command | Output is a colon-separated list of the following pieces of information: device, internal function, keystore name, keystore serial number, and keystore reference count. You can use this command to determine the association between |

| Service | Description | Input | Output |
|---|---|---|---|
|  |  |  | devices and keystores. |
| Reset | Reset the SCA 4000 card | Command | This function resets the SCA 4000 firmware and initiates all the POSTs. |
| Zeroize | Zeroizing all CSPs | Command | All CSPs and Keys on the card are zeroized. The Cryptographic Accelerator 4000 is returned to its factory state. |

**Table 3a – User Services-Bulk Encryption, Descriptions, Inputs and Outputs**

| Service | Description | Input | Output |
|---|---|---|---|
| DSA Sign | DSA signing operation | Plaintext/ciphertext data | Digital Signature |
| Verify DSA key | DSA verification operation | Signed data | Verify response |
| Access RNG | Direct access to the RNG | Random data | Calls FIPS PRNG to use random data |
| RNG SHA-1 | RNG output processed by SHA-1 | Random data | Calls FIPS PRNG to use random data |
| RSA encrypt | RSA_PKCS#1 encrypt | Plaintext data | Cyphertext data |
| RSA decrypt | RSA_PKCS#1 decrypt | Ciphertext data | Plaintext data |
| RSA Sign | RSA_PKCS#1 sign | Plaintext/ciphertext data | Digital Signature |
| Verify RSA key | RSA_PKCS#1 verify | Signed data | Verify response |

**Table 3b – User Services-Asymmetric Encryption, Descriptions, Inputs and Outputs**

| Service | Description | Input | Output |
|---|---|---|---|
| Login | User login | User's login information | Login successful/failed |
| Setpass | User change password | Command | New password |
| Enumerate key | Enumerate user's keys | Command | List of keys |
| Retrieve key | Retrieve a key | Command | Obtain user key |
| Delete key | Delete a key | Command | Key is deleted |
| Create key | Create a key | Command | New key |
| Change key attribute | Change key attribute | Command | Updated key attribute |
| Generate DES key | Generate DES key | Command | New DES key |
| Generate DES2 key | Generate DES 2-key | Command | New DES 2 key |
| Generate DES3 key | Generate DES 3-key | Command | New DES 3 key |
| Generate RSA | Generate RSA keypair | Command | New RSA keypair |

| Service | Description | Input | Output |
|---|---|---|---|
| keypair | | | |
| Generate DSA keypair | Generate DSA keypair | Command | New DSA keypair |
| Wrap Key | Wrap an asymmetric key using the given key | Command | Wrapped key |
| Unwrap Key | Unwrap a wrapped key using the given key | Command | Unwrapped key (encrypted with KTK in FIPS mode) |
| Copy Object | Copy a key object | Command | Copy of key |

**Table 3c – User Services-Object Management, Descriptions, Inputs and Outputs**

*Driver Role*

The Driver role authenticates with a hardcoded login and password in the driver to authenticate its identity to the SCA 4000. The driver can perform similar services as the user role such as bulk encryption and asymmetric encryption, but cannot perform object management services.

| Service | Description | Input | Output |
|---|---|---|---|
| 3DES Encryption | Raw 3DES encryption | Plaintext data | Ciphertext data |
| 3DES Decryption | Raw 3DES decryption | Ciphertext data | Plaintext data |
| HMAC-SHA1 | HMAC-SHA1 processing | Ciphertext data | Hashed data |
| MD5 HMAC | MD5 HMAC processing | Input data | Signed data |
| MD5 | MD5 hashing | Plaintext/ciphertext data | Hashed data |
| SHA-1 | SHA-1 hashing | Plaintext/ciphertext data | Hashed data |
| Load KTK | Authenticate to card and Load Key Transport Key (KTK) Function | Data structure containing encrypted KTK, driver username and password | Authentication and KTK decryption result |
| Diagnostics | Perform diagnostics on the SCA 4000 card | Command | Blinking of LED |
| Display | Display public key information | Command | Displaying the public key and the public key fingerprint used by the Cryptographic Accelerator 4000 board for securing administration sessions. |
| Status | Displays status of keystore information | Command | Output is a colon-separated list of the following pieces of information: device, internal function, keystore name, keystore serial number, and keystore reference count. You can use this command to determine the association between devices and keystores. |

| Service | Description | Input | Output |
|---|---|---|---|
| Reset | Reset the SCA 4000 card | Command | This function resets the SCA 4000 firmware and initiates all the POSTs. |
| Zeroize | Zeroizing all CSPs | Command | All CSPs and Keys on the card are zeroized. The Cryptographic Accelerator 4000 is returned to its factory state. |
| IPSec DES Encryption | IPSec DES encryption | Plaintext data | Ciphertext data |
| IPSec DES Decryption | IPSec DES Decryption | Ciphertext data | Plaintext data |
| IPSec 3DES Encryption | IPSec 3DES encryption | Plaintext data | Ciphertext data |
| IPSec 3DES Decryption | IPSec 3DES Decryption | Ciphertext data | Plaintext data |
| IPSec MD5 HMAC | IPSec MD5 HMAC processing | Input data | Hashed data |
| IPSec SHA1 HMAC | IPSec HMAC-SHA1 processing | Ciphertext data | Hashed data |
| IPSec add SA | Adds an IPSec SA to the SADB | SA data | Return code to indicate success or failure |
| IPSec delete SA | Deletes an IPSec SA from the SADB | SA data, identifier for SA to be deleted | Return code to indicate success or failure |
| IPSec set SA | Updates or adds an IPSec SA to the SADB | SA data | Return code to indicate success or failure |
| IPSec update SA | Updates an IPSec SA in the SADB | SA data | Return code to indicate success or failure |
| IPSec flush SADB | Removes all IPSec SAs of the specified type from the SADB | The type of SA (AH or ESP) to be deleted | Return code to indicate success or failure |
| IPSec SA checkout | Checks a SA out of the SADB | Type pf SA (AH or ESP) to checkout, identifier for SA, structure to hold SA | Return code to indicate success or failure |
| IPSec SA checkin | Checks a SA back into the SADB | SA data | Return code to indicate success or failure |

**Table 4a – Driver Services-Bulk Encryption, Descriptions, Inputs and Outputs**

| Service | Description | Input | Output |
|---|---|---|---|
| DSA Sign | DSA signing operation | Plaintext/ciphertext data | Digital Signature |
| Verify DSA key | DSA verification operation | Signed data | Verify response |
| Access RNG | Direct access to the RNG | Random data | Calls FIPS PRNG to use random data |
| RNG SHA-1 | RNG output processed by SHA-1 | Random data | Calls FIPS PRNG to use random data |
| RSA encrypt | RSA_PKCS#1 encrypt | Plaintext data | CipherText data |
| RSA decrypt | RSA_PKCS#1 decrypt | Ciphertext data | Plaintext data |
| RSA Sign | RSA_PKCS#1 sign | Plaintext/ciphertext data | Digital Signature |
| Verify RSA key | RSA_PKCS#1 verify | Signed data | Verify response |

**Table 4b – Driver Services-Asymmetric Encryption, Descriptions, Inputs and Outputs**

*Admin Secure Channel*

The Crypto Officer authentication takes place within a secure admin channel using a TLS-like negotiation using RSA for key establishment. The algorithm used is always AES-128 bit session keys and the MAC algorithm is always HMAC-SHA1. The public key exchange protocol begins with the Sun Cryptographic Accelerator 4000 providing a public RSA key to the host machine (where the admin application is running from) along with the hardware Ethernet address. A pre master secret is generated by the host machine, encrypted using the SCA 4000 public RSA key, and than sent to the firmware. At this point, both the host machine and the SCA 4000 derive the master secret, and the 2 AES keys, 2 Message Authentication Code (MAC) keys, and 2 Initialization Vectors (IVs). The MAC keys are 20-byte keys that will be used with HMAC-SHA-1. The SCA 4000 will verify the value using TLS. The host machine will compute its own verify on the messages and compare them to the SCA 4000 before this exchange is completed.

The module uses passwords to authenticate an operator in the Crypto Officer, User and Driver role. The following table shows the strength of authentication used by the module:

| Authentication Type | Strength |
|---|---|
| Password | The SCA 4000 accepts 93 different characters for a password and the probability that a random access will succeed with a 6 digit password is 1 in 646,990,183,449 with repetition of characters. |

**Table 5 – Estimated Strength of Authentication Mechanisms**

*Unauthenticated Services*

The module has unauthenticated services that provide no security relevant functionality, and these services are available to all roles. The LEDs on the rear of the module provide status information.

| Service | Description | Input | Output |
|---|---|---|---|
| Diagnostics | Perform diagnostics on the SCA 4000 card | Command | Blinking of LED |
| Display | Display public key information | Command | Displaying the public key and the public key fingerprint used by the Cryptographic Accelerator 4000 board for securing administration sessions. |

| Service | Description | Input | Output |
|---|---|---|---|
| Status | Displays status of keystore information | Command | Output is a colon-separated list of the following pieces of information: device, internal function, keystore name, keystore serial number, and keystore reference count. You can use this command to determine the association between devices and keystores. |
| Reset | Reset the SCA 4000 card | Command | This function resets the SCA 4000 firmware and initiates all the POSTs. |
| Zeroize | Zeroizing all CSPs | Command | All CSPs and Keys on the card are zeroized. The Cryptographic Accelerator 4000 is returned to its factory state. |
| **Debug Services** | | | |
| debugInfo | Displays the registered debug routines callable from vcadebug[1] | None | List of debug routines callable from the host. |
| vexInfo | Display all exception headers currently on the card | None | Exception headers stored in FLASH |
| vexShow | Displays segments (data blocks) associated with an exception | Exception number and segment number | Information relating to a specific exception and segment |
| vexProcInfo | Lists additional processes added to the exception dump | None | List of processes in the process list |
| vexSegInfo | Displays individual segment data for a given exception | Exception number | List of segments in the segment list |
| vce_mii_dump | Displays all the Cassini MII registers | None | Contents of all Cassini MII registers |
| vce_mii_reg_dump | Displays a specified Cassini MII register | Register value | Contents of specified register |
| vce_dump_rings | Dumps the network descriptor rings for debug | None | Contents of the network descriptor rings |
| vcfCfg | Displays the core firmware configuration register | None | Contents of the card configuration registers |
| vcfCsrs | Displays the core firmware control/status registers | None | Contents of the card control/status registers |
| cfgDump | Displays the firmware configuration data | None | Firmware configuration data |
| ksDump | Displays high level information about the module keystore | None | Information about on-card keystore |
| partDisplayAll | Displays memory partition data (if debug messages enabled) | None | Memory partition data |
| vSadbDump | Displays high level information about the card SADB | None | High level information about the card SADB |

[1] Vcadebug is a host application provided by Sun to invoke the firmware debug interface commands

**Table 6 – Unauthenticated Services**

## *Physical Security*

The SCA 4000 card is a multi-chip embedded cryptographic module. The SCA 4000 card is completely enclosed in a hard epoxy coating with only specific interfaces providing access to the module.

## *Cryptographic Key Management*

The implementations of the FIPS-approved algorithms have following FIPS algorithm certifications:

- SHA-1 (firmware certificate #171) as per NIST's FIPS PUB 180-1
- SHA-1 (hardware certificate #172) as per NIST's FIPS PUB 180-1
- DES CBC (certificate #225) as per NIST's FIPS PUB 46-3
- 3DES CBC (certificate #190) as per NIST's FIPS PUB 46-3
- AES (certificate #79) as per NIST's FIPS PUB 197
- DSA (certificate #92) as per NIST's FIPS PUB 186-2
- RSA (PKCS #1, vendor affirmed)
- HMAC with SHA-1 (vendor affirmed) as per NIST's FIPS PUB 198

3DES and AES are the recommended algorithms to be used for encryption and decryption. DES is only to be used in legacy systems.

The Sun Cryptographic Accelerator 4000 also performs RSA encrypt/decrypt functions for the User Role. RSA encryption/decryption must be used only for performing key transport such as in SSL/TLS protocols in a FIPS mode of operation. The module also performs RSA digital signature generation/verification

The follow algorithms are not supported when the SCA 4000 card is operating in FIPS mode:

- MD5
- HMAC-MD5
- RC2 (ECB, CBC modes)

The module supports the following critical security parameters listed below:

| Key | Key type | Generation | Storage | Use |
|---|---|---|---|---|
| Factory Remote Access Key | RSA 1024-bit Public/Private Keys | FIPS approved PRNG | Plaintext read-only Flash memory | Initiate the secure tunnel for the first connection to the SCA 4000 card |
| Remote Access Key (RAK) | RSA 1024-bit Public/Private Keys | FIPS approved PRNG | Plaintext in flash memory | Authenticate the administration application with the SCA 4000, Allows driver to send the KTK to the device encrypted |
| Key Transport Key (KTK) | AES Key 128-bit | Generated outside the crypto boundary | Plaintext in flash memory<br>Runs for a given boot cycle | Wraps CSPs crossing the FIPS boundary b/w the SCA 4000 firmware and the Solaris host |
| Master Keys | AES Key 128-bit | FIPS approved PRNG | Plaintext in flash memory | Encrypt keystore data |
| User Keys | RSA Public/Private Keypairs, DSA Public/Private Keypairs, DES/3DES Keys | FIPS approved PRNG | Plaintext in SDRAM | Performing Crypto functions |
| Session Keys (Crypto Officer) | AES Keys 128-bit | FIPS approved PRNG | Plaintext in SDRAM | Encrypts/decrypts admin commands and responses |
| Session keys (User) | DES/3DES Keys | FIPS approved PRNG | Plaintext in SDRAM | They are symmetric keys (DES/TDES) used for symmetric key operations. They may be used in SSL/TLS/IPSec by the application that generates |

| | | | | |
|---|---|---|---|---|
| | | | | them. |
| Driver Password | Password | Generated outside the crypto boundary | Plaintext in flash memory | Authenticate driver to module |
| User Password | Password | User entered | Plaintext in SDRAM | Authenticate user to the module |
| Crypto Officer Password | Password | Crypto Officer entered | Plaintext in SDRAM | Authenticate Crypto Officer to the module |
| IPSec session keys | DES/3DES keys and/or HMAC-SHA1 key | Generated outside the crypto boundary | Plaintext in SDRAM | Used during IPSec negotiations to encrypt/decrypt and authenticate data packets |

**Table 7 – Description of the Keys used on the SCA 4000**

A default Remote Access Key (RAK) is shipped with the SCA 4000 card from the factory. This Factory Remote Access Key is an RSA public/private keypair that is used to establish secure administration channels when the device is not initialized. The Factory Remote Access Public Key is used to encrypt the Key Transport Key and host machine driver login/password information, and sent down to the module. Once the driver is authenticated, the driver can send encrypted commands with the KTK securely to the module.

Once the card has been initialized, the module generates a new Remote Access Keypair. The RAK is used to negotiate two AES session keys for a single secure tunnel encryption session that are used for Security Officer and card communication. These AES session keys will be negotiated at the time a Security Officer selects a keystore, and will terminate when the Security Officer terminates the session with the module. Each subsequent session will renegotiate new AES session keys, using the Remote Access Key. These SO session keys are generated by a key agreement using TLS master secret derivation TLS session. 32 bytes of a pre-master secret enter the module encrypted by the public Remote Access Key. There are two different SO session keys generated to create sessions; one session key to receive data and one session key to send out data. These keys are used to encrypt/decrypt admin commands and encrypt/decrypt responses from the administration application tool. The Remote Access Key also allows the host machine driver to send the Key Transport Key to the device encrypted with an RSA public key. RAKs are generated using a FIPS approved PRNG and the RSA private keys are never output from the module except for backup purposes.

When the SCA 4000 card is operating in FIPS mode, the Key Transport Key is used when transporting passwords or session keys crossing the FIPS boundary between the SCA 4000 firmware and the Solaris host. This transport key is created when the module is powered up after the host machine authenticates to the SCA 4000 card. The KTK is generated outside the FIPS boundary and are input into the card at startup using the public Remote Access Key; the KTK is never output from the module.

Master Keys on the module are used to wrap all User and Crypto Officer account information and keying material associated with the SCA 4000 device. When the system and the card powers-up, the Solaris host reads the Master Key wrapped data from an encrypted file on the host file system. This data is sent down to the SCA 4000 card in the wrapped form. When the module receives this encrypted data, the card unwraps the data using the Master Key. The unwrapped data is then used to populate the user account information, and user owned data stores holding User Keys. Master Keys are generated using a FIPS approved PRNG and are only output when they are backed up as part of the device backup command. The Crypto Officer session key encrypts the Master Key to be stored on the host machine's filesystem.

User Keys are used to perform cryptographic operations and are created on demand by the User. However, prior storage of a user application keying material within the SCA 4000 keystore, a number of steps must have already taken place:

- SCA 4000 device must be initialized
- A keystore must be created
- A user account must be created within the keystore

The creation of a SCA 4000 keystore establishes a name space for the creation of users within the keystore. The creation of a user account establishes data for enforcing ownership and access rights to the keying material based on password based authentication. The User Keys are generated using a FIPS approved RNG and are stored outside of the module encrypted with the Master Key.

*Random Number Generator*

The SCA 4000 card uses the FIPS-approved RNG specified in FIPS 186-2 DSA-RNG using SHA-1 for generation of cryptographic keys.

*Key Zeroization*

There are three ways to zeroize all the keying material on the SCA 4000 card:

1) A jumper located on the board will zeroize all keying material, and all updated firmware, taking the device back to factory state, when it is next powered up. The jumper must be subsequently removed to use the device again.

2) An operator with access to the root login on the host machine can present the correct commands to initiate a zeroization of all the keys on the SCA 4000 card taking the device back to the initial Factory Remote Access Key. This application can be performed when an operator is unauthenticated to the module.

3) The Crypto Officer can zeroize all the keys and updated Remote Access Key via a remote channel (protected under a session key generated using the Remote Access Key) after the operator has properly authenticated.

### *EMI/EMC*

The module conforms to FCC Part 15 Class B requirements for home use.

### *Self-Tests*

The SCA 4000 card performs self-tests to monitor the proper functioning of the module. These self-tests are divided into two categories, those run during power-up and those run upon certain conditions.

The module consists of the following Power-up Tests:

- DES CBC Known Answer Test
- 3DES CBC Known Answer Test
- AES CBC Known Answer Test
- DSA Known Answer Test
- PRNG Known Answer Test
- HMAC with SHA-1 KAT
- RSA Sign/Verify Known Answer Test
- CRC-32 Firmware Integrity Check

The module consists of the following Conditional Tests:

- Continuous Random Number Test
- RSA Pair-wise Consistency Check
- Firmware Load Test
- DSA Pairwise Consistency Test

### *Design Assurance*

Hardware builds are controlled by a build release process. Each hardware build is named, e.g: P0, P0.1, P1.0, P1.1, P2.0, etc.  The hardware version is contained in a PROM part on the device which is accessible by software.

User documentation is versioned like source. Each release of the documentation is stored in a separate repository named by release number. Manual pages, and other miscellaneous documentation delivered with the software packages are stored and controlled in the software gates.  The source code and firmware version control is done using Source Code Control System

## SECURE OPERATION

The Sun Microsystems SCA 4000 meets Level 3 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

### *Crypto Officer Guidance*

The Crypto-Officer is responsible for initialization of the module, configuration and management of the module, and termination of the module. Detailed information for the Crypto-Officer can be found in the Sun Microsystems SCA 4000 Installation and User Guide. The module should be checked regularly for signs of tamper-evidence (scratches, holes in the epoxy, etc.). .

#### *Initialization*

The Crypto-Officer receives the module from Sun Microsystems via a secure delivery mechanism. The Crypto-Officer can either pick the module up directly from a Sun Microsystems facility, or the module can be shipped to the Crypto-Officer.

Before the initial configuration of the module, there is no access control provided by the module. The Crypto-Officer must maintain control of the module and restrict any access to the module.

The Crypto-Officer must follow the Sun Microsystems instructions for setting up the module. The Crypto Officer first installs the card, installs the host software packages and uses the administration interface from the host machine to configure the card. The Factory Remote Access Key is used to authenticate to the card and initiate a secure login. Once the card has been initialized with a keystore, the “INIT” led is lit. Additional steps include setting the access control password for users and configuring the module’s network settings. The Crypto Officer must also select FIPS mode during the SCA 4000 card configuration. The FIPS led indicator will be lit when the module is operating in a FIPS mode of operation.

After this process is complete, the Crypto-Officer is able to begin managing the module through the host machine’s vcaadm application and can generate new Users.

Additionally, while in a FIPS mode, the module only supports FIPS-approved algorithms (DSA, RSA Signature Generation/Verification, SHA-1, HMAC-SHA-1, DES Triple-DES and AES) and algorithms permitted for use in a FIPS mode of operation (RSA encryption/decryption for key transport).

*Termination*

When a module's usage has been completed, the module should be zeroized by the Crypto-Officer in order to wipe all sensitive data. The module should than be stored in a secure location.

### *User Guidance*

The User is able to use the module as defined above in the description of the User role. The User must be careful not to provide session keys and secret keys to other parties. The User must also not provide the User password to anyone.

## ACRONYMS

| Term | Definition |
|---|---|
| AES | Advanced Encryption Standard |
| ANSI | American National Standards Institute |
| CBC | Cipher Block Chaining |
| CLI | Command Line Interface |
| CMVP | Cryptographic Module Validation Program |
| CO | Crypto Officer |
| CRC | Cyclic Redundancy Checksum |
| CSE | Communications Security Establishment |
| CSP | Critical Security Parameter |
| DES | Data Encryption Standard |
| DSA | Digital Signature Algorithm |
| EDC | Error Detection Code |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| FCC | Federal Communication Commission |
| FIPS | Federal Information Processing Standard |
| HMAC | Hashing for Message Authentication Code |
| IPSec | Internet Protocol Security |
| IRQ | Interrupt Request Line |
| KAT | Known Answer Test |
| KTK | Key Transport Key |
| LAN | Local Area Network |
| LED | Light Emitting Diode |
| MAC | Message Authentication Code |
| NIC | Network Interface Card |
| NIST | National Institute of Standards and Technology |
| PCI | Peripheral Component Interconnect |
| PKCS | Public Key Cryptographic Standard |
| POST | Power On Self Test |
| PROM | Programmable Read Only Memory |

| | |
|---|---|
| RAK | Remote Access Key |
| RAM | Random Access Memory |
| RNG | Random Number Generator |
| ROM | Read Only Memory |
| RSA | Rivest Shamir and Adleman |
| SA | Security Association |
| SADB | Security Association Database |
| SHA | Secure Hash Algorithm |
| SSL | Secure Socket Layer |
| TLS | Transport Layer Security |

**Table 8 – Terms and Definitions**