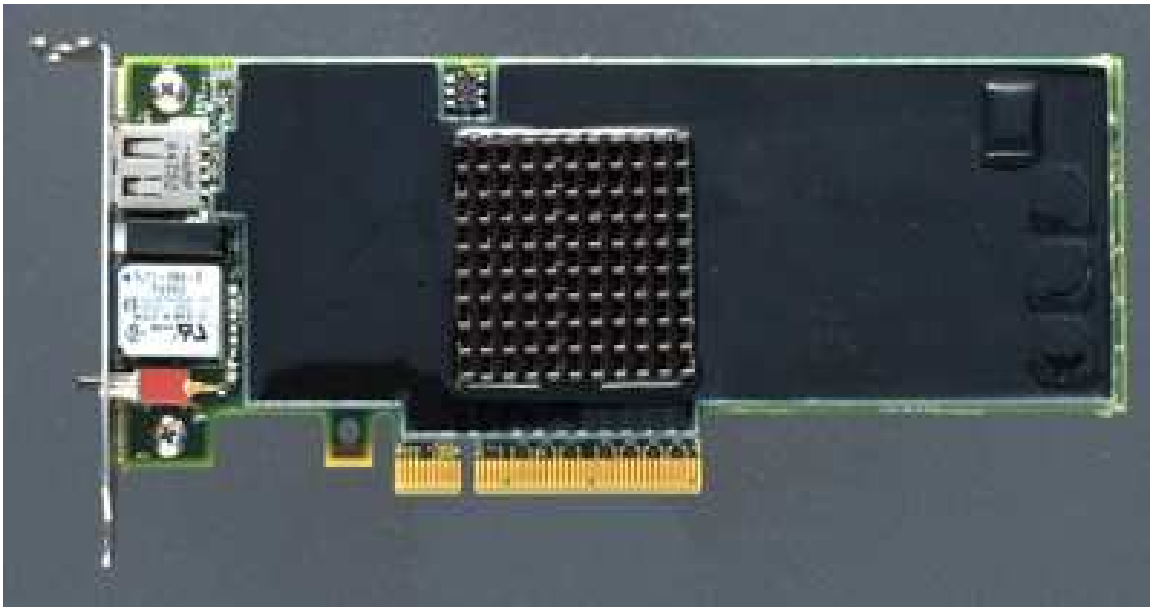
Sun Microsystems
Sun Crypto Accelerator 6000



Bootstrap Version 1.0.1 and 1.0.10, Firmware Version 1.0.11

FIPS 140-2 Non-Proprietary Security Policy

Level 3 Validation

Table of Contents

1Introduction

1.1Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Sun Crypto Accelerator 6000 from Sun Microsystems Inc. This security policy describes how the Sun Crypto Accelerator 6000 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/.

1.2References

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 (http://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.

1.3Document 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

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.

2SUN CRYPTO ACCELERATOR 6000

2.1Overview

The Sun Crypto Accelerator 6000 (SCA 6000) is a X8 PCI-Express card in low profile and short form factor and is designed to provide the highest level of security to customers. The Sun Crypto Accelerator 6000 is the next generation of the already FIPS 140-2 Level 3 certified product line by Sun Microsystems Inc. The hardware version number of the module is: 375-3424, Revisions -02 and -03. The bootstrap versions are 1.0.1 and 1.0.10, and the firmware version is 1.0.11.

In order to achieve such a high level of security, the Sun Crypto Accelerator 6000 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 Crypto Accelerator 6000 product has been designed from the ground up to incorporate security in all design and development steps. The design team also took advantage of the experience gained from previous generation of the security product.

The card enhances server system performance by off-loading computer intensive cryptographic calculations (asymmetric and symmetric) from the server's CPU, accelerating both IPsec and TLS processing. The SCA 6000 also provides a secure remote administration capability. It also provides local administration via a serial port directly connected to the card. There is also a USB port on the product to backup and restore keys directly to the product.

2.2Module Interfaces

The cryptographic boundary of the Sun Crypto Accelerator 6000 is defined by the perimeter of the PCI-Express card itself. The local interfaces to the card through on-board serial and USB ports, LED indicators, jumper pins and physical presence push-button 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-Express slot, RJ-11 Serial port, USB port, LEDs, and a jumper. It also has a physical presence push-button switch that is currently not used by the operational firmware. Since this push-button may be used in future versions of the firmware, it is tested during hardware diagnostics to verify that it functions correctly.

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-E, USB Port, Serial Port	Data Input/Output Interface
PCI-E, Jumper, Push-Button	Control Input Interface
PCI-E, LEDs	Status Output Interface
PCI-E, USB Port, Serial Port	Power Interface

Table 1 – FIPS 140-2 Logical Interfaces

2.3Roles 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 6000 documents), User role, and a Driver. There is also an additional set of unauthenticated services which are not security relevant to the Sun Crypto Accelerator 6000 card.

2.3.1Crypto Officer Role

The CO (Crypto Officer) accesses the module using a command line interface (CLI) over the PCI-E port using the administration tool, scamgr, on the host machine, or using a serial hand-held device directly connected to card. The Crypto Officer identifies him/herself with a login name and authenticates with a password and is able to configure the module. When scamgr 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-E 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 6000 firmware via the command bit of the SCA 6000 IRQ register. When the firmware has finished processing the command, it will notify the host via command complete bit of the Host IRQ register.

The CO can also perform direct administration of the card using the serial port interface. The serial port interface supports a subset of the commands provided by the remote PCI-E interface and also provides several additional commands to support Financial Services (FS) activities. When performing keystore backup and restore the encrypted backup data file is stored on a USB mass storage device connected to the USB port rather than sent to the host for archiving to disk. Information is also output in an abbreviated form to the serial port to support the use of a stateless handheld input device.

This serial interface has a similar look and feel to that of scamgr, but is designed to work with hand-held serial devices or laptop serial connections. This interface provides most of the functionality that scamgr does, with the exception of the following tasks:

- reset SCA 6000 hardware

- zeroize SCA 6000 hardware

- firmware upgrades

- deletion of decimalization tables

Administrative functions that are limited to the serial interface only are:

- Entry of key components and User, CO passwords

- Entry of decimalization tables

- Control of financial services operating mode

- Deletion of financial services keys

Backup and restore of the key material will be done via the USB port.

Descriptions of the services available to the Crypto Officer role are provided in the table below.

Service	Description	Input	Output
Backup	Backup master key and keystore (on local host)[1]	Command, password and path	Status of command and encrypted keystore file over secure admin channel
	Backup master key and keystore (on USB[3] port)[1]	Command, password and path (multiple SO names and passwords required in multi-admin mode)	Status of command and encrypted keystore file using UWK.
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

Service	Description	Input	Output
Delete	Delete users and CO accounts	Command and user name	Status of command over serial port
	Delete FS MFK[3]	Command and label	Status of command over serial port
	Delete FS KEKs and decimalization tables[3]	Command and label	Status of command over serial port
	Delete UWK [3]	Command and label	Status of command over serial port
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
	Disable multiadmin mode	Command	Status of command over secure admin channel
	Disable CO as a Multiadmin CO[1]	Command and CO name	Status of command over secure admin channel
Enable	Enable a user	Command and user name	Status of command over secure admin channel
	Enable multiadmin mode	Command, M value and timeout value	Status of command over secure admin channel
	Enable a MFK	Command	Status of command over Serial port
	Enable CO as a Multiadmin CO[1]	Command and CO name	Status of command over serial port
Exit	Exit current session	Command	Status of command over secure admin channel
Load	Load new firmware[2]	Command and path	Status of command over secure admin channel
	Load FS MFK component[3]	Command and MFK component	Status of command over serial port
	Load a decimalization table[3]	Command, decimalization table and label	Status of command over serial port
	Load KEK component[3]	Command, KEK label, KEK component	Status of command over serial port
	Load UWK component[3]	Command and UWK component	Status of command over serial port
Logout	Logout current session	Command	Exit command line
Quit	Exit current session	Command	Status of command over secure admin channel

Service	Description	Input	Output
Rekey	Generate new master key or remote access key	Command and select option	Status of command over secure admin channel
Reset	Reset the hardware[2]	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
	Set minimum number of CO logins required (M) to authorize a multiadmin command[1]	Command and M value	Status of command over secure admin channel
	Set multiadmin timeout[1]	Command and timeout value	Status of command over secure admin channel
	Set Financial Services operating mode[3]	Command and mode value	Status of command over serial port
Show	Show system settings	Command and select option	Status of command over secure admin channel
Zeroize	Delete all keys and reset board[2]	Command	INIT led is off
Restore	Restore backup file (on local host)[1]	Command, backup file, and password	Status of command over secure admin channel
	Restore backup file (on USB[3])[1]	Command, backup file, UWK components and password (multiple SO names and passwords required in multi-admin mode)	Status of command
Approve/Reject	Approve/reject multiadmin command	Command	Status of command over secure admin channel
Cancel	Cancel multiadmin command	Command	Status of command over secure admin channel
	Cancel FS MFK, UWK and KEK entry[3]	Command	Status of command over serial port

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

1 These services require multi-admin authentication and authorization in multi-admin mode
2 These services are only available via the local host.
3 These services are only available when using the direct (serial) interface

2.3.2User 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 cryptographic functions, and object management services for cryptographic acceleration. Service descriptions and inputs/outputs are listed in the following tables:

Service	Description	Input	Output
TDES Encryption	Raw TDES encryption	Plaintext data	Ciphertext data
TDES Decryption	Raw TDES decryption	Ciphertext data	Plaintext data
AES Encryption	Raw AES encryption	Plaintext data	Ciphertext data
AES Decryption	Raw AES decryption	Ciphertext data	Plaintext 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 6000 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 6000 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.

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 signature	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	CyphertextCiphertext data
RSA decrypt	RSA_PKCS#1 decrypt	Ciphertext data	Plaintext data
RSA Sign	RSA_PKCS#1 sign	Plaintext/ciphertext data	Digital Signature
Verify RSA signature	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 AES key	Generate AES key	Command	New AES key
Generate RSA keypair	Generate RSA keypair	Command	New RSA keypair
Generate DSA keypair	Generate DSA keypair	Command	New DSA keypair
Generate DH key	Generate DH key	Command	New DH key
Wrap Key	Wrap an asymmetric key using the given key. Wrapping using RC2 is not allowed in FIPS mode.	Command	Wrapped key
Unwrap Key	Unwrap a wrapped key using the given key. Unwrapping using RC2 is not allowed in FIPS mode.	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

* Services not allowed in FIPS mode

2.3.3Driver Role

The Driver role authenticates with a login and password in the driver to authenticate its identity to the SCA 6000. The driver can perform similar services as the user role such as bulk encryption and asymmetric cryptographic function, but cannot perform object management services.

Service	Description	Input	Output
TDES Encryption	Raw TDES encryption	Plaintext data	Ciphertext data
TDES Decryption	Raw TDES decryption	Ciphertext data	Plaintext data
AES Encryption	Raw AES encryption	Plaintext data	Ciphertext data
AES Decryption	Raw AES decryption	Ciphertext data	Plaintext 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

Service	Description	Input	Output
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 6000 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 6000 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.
Reset	Reset the SCA 6000 card and initiates all the POSTs.	Command	This function resets the SCA 6000 firmware
Zeroize	Zeroizing all CSPs	Command	All CSPs and Keys on the card are zeroized. The Cryptographic Accelerator 6000 is returned to its factory state.

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 signature	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 signature	RSA_PKCS#1 verify	Signed data	Verify response
DH Key Derive	DH shared secret generation	DH public key values	Shared secret

Table 4b – Driver Services-Asymmetric cryptographic function, Descriptions, Inputs and Outputs

2.3.4Admin Secure Channel & Authentication

The Crypto Officer authentication takes place within a secure admin channel using RSA for key establishment as specified in the TLS protocol. The algorithm used is always AES-128 bit session keys and the MAC algorithm is always HMAC-SHA-1. The public key exchange protocol begins with the Sun Crypto Accelerator 6000 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 6000 public RSA key, and than sent to the firmware. At this point, both the host machine and the SCA 6000 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 6000 will verify the value using TLS. The host machine will compute its own verify on the messages and compare them to the SCA 6000 before this exchange is completed.

A CO is identified using a username. When a command requiring multi-admin authentication is issued in multi-admin mode the card goes into a polling mode and waits for COs belonging to multi-admin group to login to the card. A separate secure session is established for each CO.

Assuming the CO login and password are correct, one of following three things happens:

- If the authenticated CO does not belong to the multi-admin group, no services can be invoked by that CO. The CO is given a message indicating that the board is in the middle of authorizing a Multi-Admin command and the CO cannot administer the board.

- If the CO belongs to the multi-admin group (and is not the initiator of the multi-admin command), the CO has the option to either authorize or reject the multi-admin command. In case the CO has authorized the command already a message indicating that the CO has already approved this is given.

- If the initiating CO authenticates to the card, the CO has the option to cancel the ongoing multi-admin command.

A total of M COs of the multi-admin group must login and authorize the command. If M COs do not authorize the command within the timeout period the multi-admin command is terminated. At the end of the command, control is transferred back to the initiating CO. The module allows multiple CO logins only in multi-admin mode.

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 6000 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. A failed login is accompanied by a 1 second delay allowing for no more than 60 attempts within one minute. The chance that any of these attempts will succeed within a one-minute time period is 1 in 10,783,169,724.

Table 5 – Estimated Strength of Authentication Mechanisms

2.3.5Unauthenticated Services[1]

The module has unauthenticated services that provide no security relevant functionality, and these services are available to all roles. None of the services listed below provides information related to CSPs. The LEDs on the rear of the module provide status information.

Service	Description	Input	Output
Diagnostics	Perform diagnostics on the SCA 6000 card	Command	Blinking of LED
Display	Display public key information	Command	Displaying the public key and the public key fingerprint used by the Crypto Accelerator 6000 board for securing administration sessions.

[1] These services are only available to the root user on the host Solaris system

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 6000 card	Command	This function resets the SCA 6000 firmware and initiates all the POSTs.
Zeroize	Zeroizing all CSPs	Command	All CSPs and Keys on the card are zeroized. The Crypto Accelerator 6000 is returned to its factory state.
Debug Services			
debugInfo	Displays the registered debug routines callable from vcadebug[2]	None	List of debug routines callable from the host.
mexInfo	Display all exception headers currently on the card	None	Exception headers stored in FLASH
mexShow	Displays segments (data blocks) associated with an exception	Exception number and segment number	Information relating to a specific exception and segment
mexProcInfo	Lists additional processes added to the exception dump	None	List of processes in the process list
mexSegInfo	Displays individual segment data for a given exception	Exception number	List of segments in the segment list
mcfCfg	Displays the core firmware configuration register	None	Contents of the card configuration registers
mcfCsrs	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
Load	Load firmware Load bootstrap	Firmware image Bootstrap image	Status of load Status of load

Table 6 – Unauthenticated Services

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

2.4Physical Security

The SCA 6000 card is a multi-chip embedded cryptographic module. The SCA 6000 card is completely enclosed in a hard epoxy coating with only specific interfaces providing access to the module. Components excluded from the cryptographic boundary are not covered in epoxy (see section 2.2).

2.5Cryptographic Key Management

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

- SHA-1 (Certs. #469 and #850) as per NIST's FIPS PUB 180-1
- TDES CBC (Cert. #435) as per NIST's FIPS PUB 46-3
- AES (Certs. #397 and #856) as per NIST's FIPS PUB 197
- DSA (Cert. #309) as per NIST's FIPS PUB 186-2
- HMAC-SHA-1 (Cert. #473) as per NIST's FIPS PUB 198
- RNG (Cert. #490) as per NIST FIPS PUB 186-2 Appendix 3.1
- RSA (Certs. #409 and #410) as per PKCS#1 v1.5

The module provides following algorithms allowed for use in FIPS mode for key establishment:

- RSA Encrypt/Decrypt, 1024-2048 bit modulus sizes. This key transport methodology provides 80-112-bits of security strength
- Diffie Hellman, 1024-2048 modulus sizes. This key transport methodology provides 80-112-bits of security strength.
- MD5 used internally for TLS only.
- HMAC-MD5 used internally for TLS only

The Sun Crypto Accelerator 6000 provides RSA encrypt/decrypt functions for the User Role. RSA encryption/decryption must be used only for performing key transport such as in TLS protocols in a FIPS mode of operation.

The follow algorithms are not supported when the SCA 6000 card is operating in FIPS mode:

- DES

- MD5 (used internally for TLS in FIPS mode)
- HMAC-MD5 (used internally for TLS in FIPS mode)
- 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 EEPROM	Initiate the secure tunnel for the first connection to the SCA 6000 card
Remote Access Key (RAK)	RSA 1024-bit Public/Private Keys	FIPS approved PRNG	Plaintext in SDRAM	Authenticate the administration application with the SCA 6000, 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 Runs for a given boot cycle	Wraps CSPs crossing the FIPS boundary b/w the SCA 6000 firmware and the Solaris host
Master Keys	AES Key 128-bit	FIPS approved PRNG	Encrypted using protection key in flash memory	Encrypt keystore data
User Keys	RSA Public/Private Keypairs, DSA Public/Private Keypairs, DES/TDES and AES 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
Driver Password	Password	Generated outside the crypto boundary	Plaintext in EEPROM	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/TDES keys	Generated outside the crypto boundary	Plaintext in SDRAM	Used during IPSec negotiations to encrypt/decrypt and authenticate data packets

Key	Key type	Generation	Storage	Use
AES shares key	AES Key 128-bit	FIPS approved PRNG	Plaintext in SDRAM	Used to encrypt the key shares calculated from the backup data
Key shares	Share values calculated from the backup configuration data	Shamir's secret sharing scheme based on interpolation of polynomials	Plaintext in SDRAM	Used to re-create the backup configuration data once M COs have been authenticated
Protection key	AES Key 128-bit	FIPS approved PRNG	EEPROM	Encrypted data item in Flash
Master File Key	AES Key 192-bit	Crypto officer entered in component form	Plaintext in SDRAM	Encrypt/Decrypt Financial services keys
Key Encrypting Key	2DES or TDES key	Crypto officer entered in component form	Encrypted with the MFK and user-maintained. These keys are not persistently stored in SCA 6000 device.	Used to encrypt/decrypt financial service keys for import/export for other HSMs
USB Wrapping Key (UWK)	AES 128, 192 or 256-bit	Generated outside the crypto boundary	EEPROM	Encrypt keystore during backup using USB port

Table 7 – Description of the Keys used on the SCA 6000

A default Remote Access Key (RAK) is shipped with the SCA 6000 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 Crypto Officer and card communication. These AES session keys will be negotiated at the time a Crypto Officer selects a keystore, and will terminate when the Crypto Officer terminates the session with the module. Each subsequent session will renegotiate new AES session keys, using the Remote Access Key. These CO 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 CO 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. The RSA private key is wrapped using the Master key and stored on the host file system.

When the SCA 6000 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 6000 firmware and the Solaris host. This transport key is created when the module is powered up after the host machine authenticates to the SCA 6000 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 6000 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 6000 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 file system.

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 6000 keystore, a number of steps must have already taken place:

- SCA 6000 device must be initialized
- A keystore must be created
- A user account must be created within the keystore

The creation of a SCA 6000 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.

The Master File Key (MFK) and Key Encrypting Key (KEK) both are generated by multiple crypto officers entering individual key components which are XOR'ed

together to form the finished key. For both types of keys, component entry may only happen through the serial interface. The purpose of the MFK is to act as a master encrypting key for any financial services CSPs which reside outside the cryptographic boundary (like the KEK). The purpose of the KEK is for key import and export between different HSM products. The KEK is stored outside the cryptographic boundary and is always encrypted using the MFK.

2.5.1Random Number Generator

The SCA 6000 card uses the FIPS-approved RNG specified in FIPS 186-2 DSA-RNG using SHA-1 for generation of cryptographic keys.

2.5.2Key Zeroization

There are three ways to zeroize all the keying material on the SCA 6000 card. In all cases, all keys, passwords and other CSPs are removed from within the cryptographic boundary:

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 6000 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.

2.6EMI/EMC

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

2.7Self-Tests

The SCA 6000 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 for firmware algorithms:

- Firmware AES CBC Known Answer Test

- Firmware HMAC-SHA-1 KAT
- PRNG Known Answer Test
- Firmware RSA Sign/Verify Known Answer Test
- CRC-32 Firmware Integrity Check

The module consists of the following Power-up Tests for hardware algorithms:

- Hardware AES CBC Known Answer Test
- DSA Sign/Verify Known Answer Test
- Hardware HMAC-SHA-1 KAT
- Hardware RSA Sign/Verify Known Answer Test
- TDES CBC Known Answer Test

The module consists of the following Conditional Tests:

- Continuous Random Number Test
- DSA Pairwise Consistency Test
- Main Firmware Load Test (using RSA PKCS#1 1.5 for authentication)
- Bootstrap Firmware Load Test (using RSA PKCS#1 1.5 for authentication)
- Manual Key Entry Test
- RSA Pair-wise Consistency Check

2.8Design 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

3SECURE OPERATION

The Sun Microsystems SCA 6000 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.

3.1Crypto 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 6000 Installation and User Guide. The module should be checked regularly for signs of tamper-evidence (scratches, holes in the epoxy, etc.).

3.1.1Initialization

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 6000 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 scamgr application and can generate new Users.

Additionally, while in a FIPS mode, the module only supports FIPS-approved algorithms (DSA, SHA-1, HMAC-SHA-1, RSA, Triple-DES and AES) and

algorithms permitted for use in a FIPS mode of operation (RSA encryption/decryption for key transport, Diffie Hellman for key agreement, MD and HMAC-MD5 for use in TLS internally). Please see tables 3a, 3b, 3c, 4a and 4b for a complete listing of cryptographic services available in FIPS mode.

3.1.2Termination

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.

3.2User 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. The User must not use RSA and Diffie Hellman modulus sizes smaller than 1024-bits in FIPS mode.

4ACRONYMS

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
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
FS	Financial Services
HMAC	Hashing for Message Authentication Code
IPSec	Internet Protocol Security
IRQ	Interrupt Request Line
KAT	Known Answer Test
KEK	Key Encryption Key
KTK	Key Transport Key
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
MFK	Master File Key
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
UWK	USB Wrapping Key

Table 8 – Terms and Definitions

