Sun Crypto Accelerator 6000 Board

Product Notes for Version 1.1

Part No. 820-4145-16
May 2010, Revision A

Contents

Sun Crypto Accelerator 6000 Board Product Notes for Version 1.1

These release notes describe updates and known issues of the Sun Crypto Accelerator 6000 Board. This document includes the following sections:

Important URLs

The following is a list of important URLs for the board:

- Documentation (including latest version of this document):

  `http://docs.sun.com/app/docs/prod/ssl.accel`

- Product specifications:

  `http://www.oracle.com/us/products/servers-storage/networking/031146.htm`

- Latest available patches listed in "Latest Patch Revisions and CR Fixes" on page 3:

  `http://sunsolve.sun.com`

- Base software packages and patches from Update 1 and 2 patch releases listed in: "Patches and CR Fixes in Update 2" on page 5 and "Patches and CR Fixes in Update 1" on page 6:

  `http://www.sun.com/download`

Oracle Solaris Operating System update releases contain patches to previous releases. Use the `showrev -p` command to determine whether the required patches have been previously installed.

Always install the latest version of the patches. The dash number (-01, for example) becomes higher with each new revision of the patch. If the version on the SunSolve web site is higher than that shown in this document, it is a later version. If the patch you need is not available at the SunSolve web site, contact your local sales or service representative.

Caution – If you want the ability to return to a Version 1.0 environment, you must make a backup of the 1.0 keystore and master key prior to upgrading to 1.1. See "Migrating Back to Version 1.0 From 1.1" on page 12.

FIPS 140-2 Level 3 Validated Firmware

Both the Sun Crypto Accelerator 6000 hardware and firmware are required to make the FIPS 140-2 Level 3 validated cryptographic module. The latest Sun Crypto Accelerator 6000 Board Version 1.0 FIPS compliant firmware is contained in Patch 128371-02.

Product Patches

The following tables list the required patches for the Sun Crypto Accelerator 6000 Version 1.1 software available for the Oracle Solaris 10 OS. You can download these patches at: `http://sunsolve.sun.com`.

Note – Always check for the latest revision of the patch, -01, -02, and so on.

TABLE 1 Required NSS/NSPR Patches

Patch ID	Description
119213	NSPR/NSS (Solaris SPARC)
119214	NSPR/NSS (Solaris i386)
121656	NSPR/NSS (Linux i386 and x86_64)

TABLE 2 Required Sun Crypto Accelerator 6000 Version 1.1 Patches

Patch ID SPARC, x86	Description
128364 SPARC & x86	Version 1.1 Bootstrap Firmware
128365 SPARC, 128366 x86	Version 1.1 Core Components
128367 SPARC, 128368 x86	Version 1.1 IPSec Enabler
128369 SPARC, 128370 x86	Version 1.1 Financial Services
128371 SPARC & x86	Version 1.1 Firmware
128372 SPARC, 128373 x86	Version 1.1 Admin Components
128374 Linux, All	Software (Linux, all architectures)
140532 SPARC, 140533 x86	Version 1.1 Administration Man Pages Patch

Latest Patch Revisions and CR Fixes

Note – Patches in this section are available at: `http://sunsolve.sun.com`

When patches are updated, they accumulate changes from previous updates. It is only necessary to download the latest patch to get all of the change request (CR) fixes included in that patch.

The following is a list of the latest patch revisions with tables containing the CR fixes per patch.

- Patches **128365-04/128366-04** and **128367-04/128368-04** CR fixes are in TABLE 3.
- Patches **140532-01/140533-01** CR fixes are in TABLE 4.
- Patches **128371-03/128371-04** (firmware) CR fixes are in TABLE 5.

Note – The firmware included in Patch 128371-04 is not currently FIPS 140-2 Level 3 validated.

- Patch **128374-01** (Linux) CR fixes are in TABLE 6.

TABLE 3 CRs Fixed in Patches 128365-04/128366-04 and 128367-04/128368-04

CR ID	CR Description
6768285	Add DES/3DES and AES ECB modes to board/driver
6838518	SCA6000 driver needs larger delay for manufacturing board initialization
6840642	SCA6000 does not report sensitive attributes correctly
6883831	Add wrap/unwrap template support and better handling of key attributes
6928284	Key buffer DMA mapping optimization needed

TABLE 4 CRs Fixed in Patches 140532-01/140533-01

CR ID	CR Description
6770346	Request adding the ability to display firmware, hardware, and `bootrom` levels from `scadiag`

TABLE 5 CRs Fixed in Patches 128371-03/128371-04 (firmware)

CR ID	CR Description
From Patch 128371-04:	
6951548	`scamgr` memory leaks - backup, and `scamgr` connections
6941194	SCA 6000 card hangs when generating key wrapping keys (using AES KEY WRAP)
6958418	Card hangs when control task dies
From Patch 128371-03:	
6768283	Add DES/3DES and AES ECB modes to SCA 6000
6791280	bootstrap version number not updated after software reset
6883831	add wrap/unwrap template support and better handling of key attributes
6928283	memory leak in unwrap code

TABLE 5 CRs Fixed in Patches 128371-03/128371-04 (firmware) *(Continued)*

CR ID	CR Description
6813658	Copy object fails converting session keys to token keys
6927788	Copy object broken by wrap/unwrap template changes
6928564	Buffer overwite for RSA, DSA, DH sensitive session key creation

TABLE 6 CRs Fixed in Patch 128374-01 (Linux)

CR ID	CR Description
6768283	Add DES/3DES and AES ECB modes to SCA 6000
6791280	Bootstrap version number not updated after software reset
6883831	Add wrap/unwrap template support and better handling of key attributes
6928283	Memory leak in unwrap code
6813658	Copy object fails converting session keys to token keys
6927788	Copy object broken by wrap/unwrap template changes
6928564	Buffer overwite for RSA, DSA, DH sensitive session key creation
6941194	SCA 6000 card hangs when generating key wrapping keys (using AES KEY WRAP)
6768285	Add DES/3DES and AES ECB modes to SCA 6000/driver
6838518	SCA 6000 driver needs larger delay for manufacturing board initialization
6840642	`sca6000` does not report sensitive attributes correctly
6928284	Key buffer dma mapping optimization needed
6951548	`scamgr` memory leaks - backup, and `scamgr` connections
6930601	Consistent memory on Linux should not be `dma` sync'd (update)
6958418	Card hangs when control task dies

Patches and CR Fixes in Update 2

Note – Patches in this section are available at: `http://www.sun.com/download`

- Patches **128365-03/128366-03** and **128367-03/128368-03** CR fixes are in TABLE 7
- Patches **128372-03/128373-03** CR fixes are in TABLE 8

TABLE 7 CRs Fixed in Patches 128365-03/128366-03 and 128367-03/128368-03

CR ID	CR Description
6719985	`mca` modifies the input crypto_data offset and length fields
6752709	Public key exchange fails in FIPS mode
6771936	Running VTS Crypto test with `Sun_Crypto_Acc_6000-1_1-u1-Solaris` patches causes domain panic
6774456	SCA6000 card zeroize can cause domain panic
6779296	Warning messages in x86 nightly builds
6770346	Request adding the ability to display firmware, hardware, and `bootrom` levels from `scadiag`

TABLE 8 CRs Fixed in Patches 128372-03/128373-03

CR ID	CR Description
6770346	Request adding the ability to display firmware, hardware, and `bootrom` levels from `scadiag`
6781798	Cannot load 1.0 keystore backups to 1.1 systems

Patches and CR Fixes in Update 1

Note – Patches in this section are available at: `http://www.sun.com/download`

- Patch **128364-02** CR fixes are in TABLE 9.
- Patch **128371-02** CR fixes are in TABLE 10.
- Patches **128365-02/128366-02** and **128367-02/128368-02** CR fixes are in TABLE 11.
- Patches **128372-02/128373-02** CR fixes are in TABLE 12.

TABLE 9 CRs Fixed in Patch 128364-02

CR ID	CR Description
6688357	x6000a crypto card fails to initialize
6564332 (from Patch 128364-01)	SCA6000 card does not respond to host pci configuration cycles within 1 second

TABLE 10 CRs Fixed in Patch 128371-02

CR ID	CR Description
6732403	`C_Unwrap` key using `AESKeyWrap` mechanism fails after 512 calls
From Patch 128371-01:	
6635158	Do not allow bootstrap firmware upgrades with higher version number than operational firmware
6648868	USB full keystore backup failure
6663931	`CKM_ECDSA` with `NULL` output returns `CRYPTO_ATTRIBUTE_VALUE_INVALID` (firmware)
6666806	FIPS rng test code
6666818	Incorrect UWK handling
6674700	Multi-admin commands no longer work from local interface
6674748	AES firmware test code for FIPS validation
6675063	Need to implement aeskeywrap mechanism in mars (firmware)
6675068	Need to run sw alg. POST for SHA512 and ECDSA
6675774	Pairwise-consistency test for EC
6676832	`mca`: [ID 250583 `kern.warning`] `WARNING: mca1: cacheKey:obj_mb_alloc(120)ENOMEM`
6677641	Need to change RSA known answer tests to sign/verify tests in SCA6000 firmware
6681139	Need possibility to test software RSA implementation from PKCS#11 interface
6681723	Power-on self test (POST) failures not handled correctly
6684159	ECC pairwise consistency test failures should halt system
6684609	`pk11wrap` fails with two boards in the same system
6689090	Firmware known answer tests no longer work during diagnostcs
6689657	Additional check needed in ECDSA known answer test
6697898	Move token ID out of eeprom
6705027	Keystore token ID not initialized correctly during keystore loads

TABLE 11 CRs Fixed in Patches 128365-02/128366-02 & 128367-02/128368-02

CR ID	CR Description
6724155	Stack overflow found on 32-bit Linux platform
6719985	`mca` modifies the input `cyrpto_data` offset and length fields
6699723	PKCS#11 function `C_SetPIN` the Sun Fire X4200 reboots instantly
6693598	`mca` needs support for >64 bits long AES counter
From (128365-01/128366-01):	
6636747	Allow bootstrap upgrades on Linux
6647909	Linux cannot allocate more than 1M size session table due to kernel memory allocation limitation
6662427	Hot-plug of SCA6000 card might cause panic if the same slot was in use by Sun Quad GbE UTP x8 PCI Express Card QGC
6663934	`CKM_ECDSA` with NULL output returns `CRYPTO_ATTRIBUTE_VALUE_INVALID` (driver)
6666814	`CKM_EC_KEY_PAIR_GEN` not advertised through PKCS#11 interface
6666948	Hash operation fails when an input is larger than 4K on x86
6675231	Need to implement `aeskeywrap` mechanism in SCA6000 (driver)
6680625	System panics when `crypto_loop` test is run on uninitialized SCA6000 card
6685039	Driver does not dma sync input buffer for wrap operations
6693112	x86_64_Lin ux not able to destroy key index
6693760	ECC mechanisms fail on Linux (Disable ECC for Linux 1.1 FCS)
6698821	Login twice with wrong password causes assertion failure
6709618	SCA6000 1.1 panics Oracle Solaris system during installation

TABLE 12 CRs Fixed in Patch 128372-02/128373-02

CR ID	CR Description
6731037	`scakiod` needs an option to not send messages to the `syslog`
From (128372-01):	
6700942	`scakiod` needs to periodically purge transaction logs
6635098	Make `bootrom` version an optional scamgr show status field
6636747	Allow bootstrap upgrades on Linux
6671767	`scakiod` uses wrong read object by ID routine for centralized keystore

Known Issues on Linux Platforms

This section describes known issues on x86 Linux platforms.

Only One Sun Crypto Accelerator 6000 Board Is Supported on Linux Redhat or SuSE OS Systems (CR 6436859)

The default memory size in IOMMU for the Opteron system is not enough for two Sun Crypto Accelerator boards.

Workaround: Increase the I/O memory size by passing the following Linux boot parameter:

```
iommu=memaper=2
```

This parameter can be passed during boot for the current boot. This parameter can also be stored in `/boot/grub/menu.lst` for subsequent boots. The `/boot/grub/menu.lst`, parameter looks like the following:

```
###Don't change this comment - YaST2 identifier: Original name: linux###
title Linux
    kernel (hd0,1)/boot/vmlinuz root=/dev/sda2 selinux=0 resume=
/dev/VolGroup00/LogVol01 splash=silent elevator=cfq showopts console=tty0
console=ttyS0,9600n8 iommu=memaper=2
    initrd (hd0,1)/boot/initrd
```

Note the location of `iommu=memaper=2`.

Known Issues With Solaris Cryptographic Framework

Managing the NCP (UltraSPARC® T1 Processor) Provider With the `cryptoadm`(1M) Utility (CR 6414116)

The NCP driver cannot be disabled with the `cryptoadm`(1M) utility by default.

Workaround: To manage the NCP provider with the `cryptoadm`(1M) utility, add the following lines to the end of the `/etc/crypto/kcf.conf` file:

```
# Start  SUNWcakr.v driver_names=ncp
# End SUNWcakr.v
```

Need Key Check Function Group Flag (RFE 6407944)

Currently, the only method to determine if a provider supports a key check entry point is to verify that the key check entry point in the operations vector is non-null. This verification still proves only that the provider can check the key of at least one mechanism.

Known Issues With Specific Platforms

CKR_SIGNATURE_INVALID Error During crypto_loop Test in FIPS Mode (CR 6632968)

DSA signature verification might fail with CKR_SIGNATURE_INVALID error under heavy crypto load on Sun SPARC Enterprise M4000/M5000/M8000/M9000 servers, in FIPS mode. This problem has only been seen with an internal stress test utility, and we are still investigating whether it is a problem in the test program or in the product.

Sun Ultra 40 Workstation Not Powering on With Board in Slot 0 (CR 6395330)

Using a Sun Crypto Accelerator 6000 board in slot 0 of a Sun Ultra 40 workstation might prevent the workstation from powering on. This issue is more prevalent with older versions of the BIOS.

Workaround: Install version 1.20 or later of the BIOS, which is available at:

http://www.sun.com/desktop/workstation/ultra40/downloads.jsp

Migrating Back to Version 1.0 From 1.1

There are changes in the keystore implementation for the board that make it incompatible with version 1.0 firmware. If you want the ability to return to a version 1.0 environment, you must make a backup of the 1.0 keystore and master key prior to upgrading to 1.1.

▼ Back Up the 1.0 Keystore

1. **With the 1.0 software and firmware running, use `scamgr` to log into the board and run the `show status` command. Make a note of the `Keystore Name` and `Keystore ID` fields.**

   For details, refer to the *Sun Crypto Accelerator 6000 User's Guide* (819-5536) at: `http://docs.sun.com/app/docs/prod/ssl.accel`

2. **Type the `backup` command to save the master key.**

3. **Change to the `/var/sca/keydata` directory and archive the correct keystore directory and configuration file.**

   The keystore name and ID are shown in the filename for the `.conf` file and the corresponding directory.

   For example, if the keystore name is `ks.600054` and the keystore ID is `0000000069efe289`, then you will find the following files and directories in `/var/sca/keydata`:

   ```
   ks.600054.{69efe289}        ks.600054.{69efe289}.conf
   ```

4. **Use the `tar` command to archive both the `.conf` file and the entire contents of the directory:**

   ```
   # tar cvfz ks.600054.{69efe289}.tar ks.600054.{69efe289}.conf ks.600054.{69efe289}
   ```

5. **Place the master key backup and keystore tar file in a safe location.**

   You can now safely upgrade to the 1.1 software and retain the ability to revert back to 1.0 software and firmware.

▼ Restore the 1.0 Software and Firmware:

1. **While the 1.1 software and firmware is still running, log into the board as the device security officer using `scamgr -D` and type the `zeroize` command.**
2. **Change directories into `/var/sca/keydata` and remove the `.conf` file and correspinding keystore directory.**
3. **Using `scadiag -u`, load the 1.0 firmware onto the system.**
4. **After the 1.0 firmware loads, reset the board with the `scadiag -r` command.**

```
# scadiag -u firmware-file  device
# scadiag -r device
```

When the board finishes resetting, it will be placed in failsafe mode.

5. **Execute the `remove` script to remove the Sun Crypto Accelerator 6000 1.1 software components from the system.**
6. **From the 1.0 installation media, execute the `install` script to load the 1.0 software components.**
7. **Apply any 1.0 software and firmware patches that are necessary.**

   Refer to the *Sun Crypto Accelerator 6000 Board Release Notes* (819-5537) at: http://docs.sun.com/app/docs/prod/ssl.accel
8. **Unpack the 1.0 keystore `tar` file into `/var/sca/keydata`.**

```
# cd /var/sca/keydata
# tar xvf path-to-tar-file
```

9. **Verify that the `.conf` file and all the contents of the keystore directory are owned by `daemon`. If not, set them to that ownership:**

```
# chown -R daemon:other keystore.conf_file  keystore-directory
```

10. **Start the `scamgr` utility and initialize the board to use an existing keystore, providing the master key backup file in the process.**

    You have now restored the 1.0 keystore.