

# Sun Crypto Accelerator 6000 Board

---

Product Notes for Version 1.0



Part No. 819-5537-13  
May 2010, Revision A

Copyright © 2006, 2010 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

---

Copyright © 2006, 2010, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quel que procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. UNIX est une marque déposée concédée sous licence par X/Open Company, Ltd.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

# Contents

---

<b>Sun Crypto Accelerator 6000 Board Product Notes for Version 1.0</b>	<b>1</b>
FIPS 140-2 Level 3 Validated Firmware	2
Required Patches	2
openCryptoki 2.2.2-rc6 Software Requirements for Linux Platforms	3
Known Issues With the Sun Crypto Accelerator 6000 Software	4
CR 6451534 Mismatch Between Expected Serial and Modulus	4
CR 6426911 Disconnect USB Devices Before Zeroizing With the <code>scdiag</code> Utility	4
CR 6421532 Financial Services Support Disabled by Default	5
CR 6375771 Locking Out <code>scamgr</code> Users	5
CR 6421355 Changing a User Password on a Dual-Board System Creates a Duplicate User on One of the Boards	5
CR 6419906 Instance Numbers Must be Correct When Resetting or Zeroizing the Board From a Command-Line Interface (CLI)	6
CR 6421475 Some Error Returns Cause Firmware CLI Task to Exit	6
CR 6421880 Keystore Names Must be Unique Within Each System	7
Known Issues With Solaris Cryptographic Framework	7
CR 6414116 Managing the NCP (UltraSPARC T1 Processor) Provider With the <code>cryptoadm(1M)</code> Utility	7
RFE 6407944 Need Key Check Function Group Flag	8
Known Issues With Specific Platforms	8

CR 6395330 Sun Ultra 40 Workstation Not Powering on With Board in Slot 0  
8

Sun Ultra 20 Workstation Hangs During Reboot 8

Sun Fire X2100 Server Hangs During Reboot 8

# Sun Crypto Accelerator 6000 Board Product Notes for Version 1.0

---

This document describes known issues of the Sun Crypto Accelerator 6000 Board from Oracle. For the latest version of this document, go to:

<http://docs.sun.com/app/docs/prod/ssl.accel>

For the latest patches, updates, and requirements, visit the product web pages at:

<http://www.sun.com/products/networking/sslaccel/suncryptoaccel6000>

The patches listed in this document are available at: <http://sunsolve.sun.com>. Solaris Operating System (OS) update releases contain patches to previous releases. Use the `showrev -p` command to determine whether the required patches have already been 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.

This document includes the following sections:

- [“Required Patches” on page 2](#)
- [“Known Issues With the Sun Crypto Accelerator 6000 Software” on page 4](#)
- [“Known Issues With Solaris Cryptographic Framework” on page 7](#)
- [“Known Issues With Specific Platforms” on page 8](#)

---

# 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 122889-08.

---

## Required Patches

The following tables list the required patches available for Solaris 10. The patches for the Sun Crypto Accelerator 6000 Version 1.0 board are available from <http://sunsolve.sun.com>.

---

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

---

**TABLE 1** Required Sun Crypto Accelerator 6000 Patches

Patch ID SPARC, x86	Description
138564 SPARC & x86	Version 1.0 Bootstrap Firmware
122883 SPARC, 122884 x86	Version 1.0 Core Components
122885 SPARC, 122886 x86	Version 1.0 IPSec Enabler
122887 SPARC, 122888 x86	Version 1.0 Financial Services
122889 SPARC & x86	Version 1.0 Firmware
122890 SPARC, 122891 x86	Version 1.0 Admin Components
124893 Linux, All	Software (Linux, all architectures)

**TABLE 2** Required Solaris Patches

Patch	Description
118918-18 SPARC	SunOS 5.10: Solaris Crypto Framework Patch
118919-17* x86	SunOS 5.10_x86: Solaris Crypto Framework Patch. For Solaris 10 1/06, you must reboot the system after this patch is installed.

\* If you are using the Solaris 10 1/06 OS for x86 platforms, the system must be rebooted after Patch 118919-17 is installed. This patch is installed when you install the Sun Crypto Accelerator 6000 software with the install script. The system reboot is required to register the driver.

---

## openCryptoki 2.2.2-rc6 Software Requirements for Linux Platforms

openCryptoki software is required for Linux platforms. Download the latest openCryptoki 2.2.2-rc6 software (`openCryptoki-2.2.2-rc6.tar.gz`) and the required openCryptoki 2.2.2-rc6 patch (`openCryptoki-2.2.2-rc6.patch.gz`).

For instructions on installing the openCryptoki 2.2.2-rc6 software, refer to Appendix B of the *Sun Crypto Accelerator 6000 Board User's Guide* (819-5536) at:

<http://www.sun.com/documentation>

You must apply the openCryptoki-2.2.2-rc6 patch to the openCryptoki 2.2.2-rc6 software release. To apply the patch, change to the directory that you unpacked the openCryptoki 2.2.2-rc6 software and enter the following command:

```
% patch -p1 < openCryptoki-2.2.2-rc6.patch
```

The 32-bit glibc-devel package is also required if you encounter the following error during the openCryptoki software compilation.

```
/usr/bin/ld: crti.o: No such file: No such file or directory
```

The 32-bit glibc-devel package name is similar to `glibc-devel-2.3.4-2.13` on RHEL4 and `glibc-devel-32bit-9-200512100801` on SuSE9.

To configure the OpenSSL library to use the board, refer to "Preparing OpenSSL Libraries" section in Chapter 7 of the *Sun Crypto Accelerator 6000 Board User's Guide*.

---

# Known Issues With the Sun Crypto Accelerator 6000 Software

## CR 6451534 Mismatch Between Expected Serial and Modulus

A mismatch between the expected serial and modulus could occur when a board is initialized with an existing multi-admin keystore and multi-admin keystore commands are subsequently entered with the `scamgr` utility. After the initialization, the `scamgr` utility incorrectly uses a new remote access key and fingerprint instead of correctly using this information from the existing keystore. If this problem occurs, an error message similar to the following is displayed:

```
scamgr(mca1@localhost, username)> set multiadmin timeout 1440
NOTICE: Please wait while the other required 1 security officer
        authenticates this command. This command will time out
        in 5 minutes.

Mismatch between expected serial and modulus.

Error: A fatal error occured during multi-admin polling.
       Mcaadm will now disconnect from the device and exit.
       You may need to log back into the device and cancel the
       multi-admin command if it is still pending.

Error Code: 0x16
```

Workaround: Exit and restart the `scamgr` utility after initializing the board with an existing multi-admin keystore.

## CR 6426911 Disconnect USB Devices Before Zeroizing With the `scadiag` Utility

With a USB device connected to the board, initiating a `zeroize` or `reset` command with the `scadiag` utility could fail and make the USB device inaccessible.

Workaround: Disconnect USB devices before performing these operations.

## CR 6421532 Financial Services Support Disabled by Default

The Sun Crypto Accelerator 6000 board financial services functionality is disabled by default because enabling it can cause load sharing errors due to a bug in the Solaris Cryptographic Framework (CR 6407944). Enabling financial services in a redundant hardware configuration (two or more boards) might cause errors under heavy loads due to this bug. In a single board configuration, these errors do not occur.

Workaround: Install Patches 118918-18 and 122883 (respectively) for SPARC platforms or Patches 118919-17 and 122884 (respectively) for x86 platforms. Once these patches are installed, financial services support is enabled by default.

You can also enable financial services support manually by making the following change in the `/kernel/drv/mca.conf` file:

```
enable-finsvcs=1;
```

## CR 6375771 Locking Out scamgr Users

One `scamgr` user can lock out all other `scamgr` users by opening a remote connection to a Sun Crypto Accelerator 6000 board and leaving the login prompt up and not logging in. This stale remote connection blocks all other local and remote connections and returns a `device busy` error when users attempt to connect.

## CR 6421355 Changing a User Password on a Dual-Board System Creates a Duplicate User on One of the Boards

If two Sun Crypto Accelerator 6000 boards are sharing a single keystore, when you change the password of a user, a duplicate user appears on one of the boards, not both. That is, one of the boards will have two entries for the same user name, one with the old password, and one with the new password.

The on-disk database file is not affected. The database has only one user record, the one with the latest password stored in it. It is only the internal user database of the board that contains the duplicate user.

Workaround: Reset the board with the duplicate user. When the board comes back online, it will have only one entry per user, and that entry will be the one with the new password, not the old one.

## CR 6419906 Instance Numbers Must be Correct When Resetting or Zeroizing the Board From a Command-Line Interface (CLI)

An unintentional reset or zeroize of a board with an instance number of 0 (mca0) could occur if a nonnumber character is entered for the instance number in the command-line syntax. This issue could occur using the `scamgr` or `scadiag` utilities, or the firmware CLI to reset or zeroize a board. This issue occurs because any nonnumber character in place of the instance number of the board is interpreted as zero.

The following are examples of entering nonnumber characters in place of the instance number with the `scadiag` utility:

```
bash-3.00# scadiag -r mcan
Resetting device mca0, this may take a minute.
Please be patient.
Device mca0 reset ok.
bash-3.00#

bash-3.00# scadiag -z mca-
Zeroizing device mca0, this may take a few minutes.
Please be patient.
Device mca0 zeroized.

bash-3.00# scadiag -z mcan
Zeroizing device mca0, this may take a few minutes.
Please be patient.
Device mca0 zeroized.
bash-3.00#
```

Workaround: Use caution when entering instance numbers in the command-line syntax to reset or zeroize the board.

## CR 6421475 Some Error Returns Cause Firmware CLI Task to Exit

Certain error cases from user input cause the firmware command-line interface (CLI) to hang. For example, if you type `set timeout n` the CLI task hangs.

This occurs due to the return value from the `_init` function in question is returning nonzero and not `ECANCELED`. If the function exits due to incorrect user input and it is not a fatal error, the function returns `ECANCELED`.

## CR 6421880 Keystore Names Must be Unique Within Each System

If two Sun Crypto Accelerator 6000 boards in the same system use a keystore with the same name and do not share a keystore, the driver does not distinguish between the two keystores when registering with the encryption framework (EF).

Thus, if the security officer (SO) for one board creates a new keystore, `myKeystore`, and the SO for another board in the same system creates a new keystore with the same name, the driver registers both keystores as `myKeystore`. The EF will not distinguish between these keystores, even though they are separate keystores both internally in the firmware and driver, and externally on disk.

Workaround: Make all Sun Crypto Accelerator 6000 board keystore names unique within each system.

---

## Known Issues With Solaris Cryptographic Framework

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

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 SUNWcacr.v driver_names=ncp
# End SUNWcacr.v
```

## RFE 6407944 Need Key Check Function Group Flag

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 nonnull. This still proves only that the provider can check the key of at least one mechanism.

---

## Known Issues With Specific Platforms

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

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>

### Sun Ultra 20 Workstation Hangs During Reboot

The Sun Ultra 20 workstation might occasionally hang during reboot when a Sun Crypto Accelerator 6000 board is installed in the system. A system power cycle is required to recover from this condition. This problem is fixed in the latest revision of the system BIOS and will be released as part of the Sun Ultra 20 Workstation Supplemental 1.4 ISO Image. This image can be downloaded at the following URL when available:

<http://www.sun.com/desktop/workstation/ultra20/downloads.html>

### Sun Fire X2100 Server Hangs During Reboot

The Sun Fire X2100 Server may occasionally hang during reboot when an Sun Crypto Accelerator 6000 board is installed in the system. A system power cycle is required to recover from this condition. This problem is fixed in the latest revision of

the system BIOS and will be released as part of the Sun Fire X2100 Server Supplemental 1.4 ISO Image. This image can be downloaded at the following URL when available:

<http://www.sun.com/servers/entry/x2100/downloads.jsp>

