



Sun™ Crypto Accelerator 1000 Board Version 2.0 Installation and User's Guide

Sun Microsystems, Inc.
www.sun.com

Part No. 819-0425-11
October 2005, Revision A

Submit comments about this document at: <http://www.sun.com/hwdocs/feedback>

Copyright 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

This product or document is distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, SunVTS, AnswerBook2, docs.sun.com, Sun ONE, Sun Enterprise, Sun Enterprise Volume Manager, Sun Fire, SunSolve, Netra, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. Netscape is a trademark or registered trademark of Netscape Communications Corporation. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 Etats-Unis. Tous droits réservés.

Ce produit ou document est distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, SunVTS, AnswerBook2, docs.sun.com, Sun ONE, Sun Enterprise, Sun Enterprise Volume Manager, Sun Fire, SunSolve, Netra, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc. Netscape est une marque de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays. Ce produit comprend le logiciel développé par le Project OpenSSL pour l'utilisation dans le Toolkit OpenSSL (<http://www.openssl.org/>). Ce produit comprend le logiciel cryptographique écrite par Eric Young (eay@cryptsoft.com). Ce produit comprend le logiciel développé par Ralf S. Engelschall <rse@engelschall.com> pour l'utilisation dans le projet mod_ssl (<http://www.modssl.org/>).

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.

Contents

- 1. Product Overview 1**
 - Hardware Overview 1
 - Product Features 2
 - Dynamic Reconfiguration and High Availability Considerations 3
 - Load Sharing 4
 - Hardware and Software Requirements 4
 - Required Patches 5

- 2. Installing the Sun Crypto Accelerator 1000 Board 7**
 - Handling the Board 7
 - Installing the Board 8
 - ▼ To Install the Hardware 8
 - Installing the Sun Crypto Accelerator 1000 Software With the install Script 9
 - Version 1.1 and 2.0 Software Contained on the CD-ROM 9
 - ▼ To Install the Software With the install Script 10
 - Directories and Files 12
 - Removing the Software With the remove Script 13
 - ▼ To Remove the Software With the `remove` Script on the CD-ROM 14
 - ▼ To Remove the Software With the `/var/tmp/crypto_acc.remove` Script 14

Installing the Software Without the install Script	14
Version 1.1 and 2.0 Software Contained on the CD-ROM	15
▼ To Install the Software Without the install Script	15
Directories and Files	18
Removing the Software Without the remove Script	19
▼ To Remove the Software Without the remove Script	20
3. Installing and Configuring Sun ONE Server Software	21
Overview of Enabling Sun ONE Web Servers	21
Installing and Configuring Sun ONE Web Server 6.1	22
▼ To Install Sun ONE Web Server 6.1	22
Configuring Sun ONE Web Server 6.1	23
▼ To Create a Trust Database	23
▼ To Register the Board With the Web Server	24
▼ To Generate a Server Certificate	27
▼ To Install the Server Certificate	30
▼ To Enable the Web Server for SSL	31
Configuring Sun ONE Web Servers to Start Up Without User Interaction on Reboot	33
▼ To Create an Encrypted Key for Automatic Startup of Sun ONE Web Servers on Reboot	33
4. Enabling Apache Web Servers	35
Creating a Private Key and Certificate	35
▼ To Create a Private Key and Certificate	35
Enabling Apache Web Servers	37
▼ To Enable the Apache Web Server	38
5. Diagnostics and Troubleshooting	41
SunVTS Diagnostic Software	41
Installing SunVTS	42

Troubleshooting the Sun Crypto Accelerator 1000	42
Using kstat to Determine Cryptographic Activity	43
Sun's Predictive Self-Healing	43
6. Migrating Keys From Version 1.x Realms	45
realmparse Options	45
Examples Using the realmparse Command	47
Listing All Available PKCS#11 Tokens	48
Migrating All Objects Associated With a Realm User to the Sun Software PKCS#11 Softtoken	48
A. Sun Crypto Accelerator 1000 Board Specifications	49
Physical Dimensions	49
Interface Specifications	50
Power Requirements	50
Environmental Specifications	50
B. Building OpenSSL Applications for Use With the Sun Crypto Accelerator 1000 Board	51
C. Building PKCS#11 Applications for Use With the Sun Crypto Accelerator 1000 Board	53
D. Manual Page	57
E. Software Licenses	59
Third-Party Licenses	65
Index	69

Tables

TABLE 1-1	Supported SSL Algorithms	3
TABLE 1-2	Hardware and Software Requirements	4
TABLE 2-1	Files in the /cdrom/cdrom0 Directory	10
TABLE 2-2	Files in the /cdrom/cdrom0/Sun_Crypto_Acc_1000_2_0 Directory	11
TABLE 2-3	Sun Crypto Accelerator 1000 Directories	12
TABLE 2-4	Files in the /cdrom/cdrom0 Directory	16
TABLE 2-5	Files in the /cdrom/cdrom0/Sun_Crypto_Acc_1000_2_0 Directory	16
TABLE 2-6	Sun Crypto Accelerator 1000 Directories	18
TABLE 3-1	Requestor Information Fields	29
TABLE 3-2	Fields for the Certificate to Install	31
TABLE 6-1	realparse Options	46
TABLE A-1	Physical Dimensions	49
TABLE A-2	Interface Specifications	50
TABLE A-3	Power Requirements	50
TABLE A-4	Environmental Specifications	50
TABLE C-1		53
TABLE D-1	Sun Crypto Accelerator 1000 Man Pages	57

Declaration of Conformity

EMC

Compliance Model Number: DEIMOS
Product Family Name: Sun Crypto Accelerator 1000 (X6762A)

European Union

This equipment complies with the following requirements of the EMC Directive 89/336/EEC:

EN55022:1998/CISPR22:1997	Class A
EN55024:1998	Required Limits (as applicable):
EN61000-4-2	4 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m
EN61000-4-4	1 kV AC Power Lines, 0.5 kV Signal and DC Power Lines
EN61000-4-5	1 kV AC Line-Line and Outdoor Signal Lines 2 kV AC Line-Gnd, 0.5 kV DC Power Lines
EN61000-4-6	3 V
EN61000-4-8	1 A/m
EN61000-4-11	Pass
EN61000-3-2:1995 + A1, A2, A14	Pass
EN61000-3-3:1995	Pass

Safety

This equipment complies with the following requirements of the Low Voltage Directive 73/23/EEC:

EC Type Examination Certificates:

EN 60950:2000, 3rd Edition
IEC 60950:1999, 3rd Edition

Supplementary Information

This product was tested and complies with all the requirements for the CE Mark.

/S/

Dennis P. Symanski
Manager, Compliance Engineering
Sun Microsystems, Inc.
901 San Antonio Road, MPK15-102
Palo Alto, CA 94303-4900 U.S.A.
Tel: 650-786-3255
Fax: 650-786-3723

DATE

/S/

Peter Arkless
Quality Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: 0506-670000 Fax: 0506-760011

DATE

Regulatory Compliance Statements

Your Sun product is marked to indicate its compliance class:

- Federal Communications Commission (FCC) — USA
- Industry Canada Equipment Standard for Digital Equipment (ICES-003) — Canada
- Voluntary Control Council for Interference (VCCI) — Japan
- Bureau of Standards Metrology and Inspection (BSMI) — Taiwan

Please read the appropriate section that corresponds to the marking on your Sun product before attempting to install the product.

FCC Class A Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Shielded Cables: Connections between the workstation and peripherals must be made using shielded cables to comply with FCC radio frequency emission limits. Networking connections can be made using unshielded twisted-pair (UTP) cables.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

FCC Class B Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

Shielded Cables: Connections between the workstation and peripherals must be made using shielded cables in order to maintain compliance with FCC radio frequency emission limits. Networking connections can be made using unshielded twisted pair (UTP) cables.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

ICES-003 Class A Notice - Avis NMB-003, Classe A

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

ICES-003 Class B Notice - Avis NMB-003, Classe B

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.


VCCI 基準について

クラス A VCCI 基準について

クラス A VCCI の表示があるワークステーションおよびオプション製品は、クラス A 情報技術装置です。これらの製品には、下記の項目が該当します。

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

クラス B VCCI 基準について

クラス B VCCI の表示  があるワークステーションおよびオプション製品は、クラス B 情報技術装置です。これらの製品には、下記の項目が該当します。

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

BSMI Class A Notice

The following statement is applicable to products shipped to Taiwan and marked as Class A on the product compliance label.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Preface

The *Sun Crypto Accelerator 1000 Board Version 2.0 Installation and User's Guide* provides a description of the features of the Sun™ Crypto Accelerator 1000 board and describes how to install and use the board in your system.

This book assumes that you are a network administrator with experience configuring the Solaris™ Operating System, Sun platforms with PCI I/O cards, Sun ONE and Apache Web Servers, SunVTS™ software, and certification authority acquisitions.

How This Book Is Organized

This book is organized as follows:

- [Chapter 1](#) provides an overview of the Sun Crypto Accelerator 1000 board, and discusses the hardware and software requirements.
- [Chapter 2](#) describes how to install the Sun Crypto Accelerator 1000 hardware and software.
- [Chapter 3](#) explains how to configure and enable the Sun Crypto Accelerator 1000 board for use with Sun ONE Web Servers.
- [Chapter 4](#) explains how to enable the Sun Crypto Accelerator 1000 board for use with Apache Web Servers.
- [Chapter 5](#) describes diagnostic tests and troubleshooting for the Sun Crypto Accelerator 1000 software.
- [Chapter 6](#) describes how to migrate keys from version 1.x realms.
- [Appendix A](#) outlines the various specifications of the Sun Crypto Accelerator 1000 board.

- [Appendix B](#) discusses the software supplied with the Sun Crypto Accelerator 1000 version 1.1, which can be used to build some OpenSSL-compatible applications to take advantage of the cryptographic acceleration features of the Sun Crypto Accelerator 1000 board.
- [Appendix C](#) describes how to build PKCS#11 applications for use with the board.
- [Appendix D](#) describes the online manual page included with Sun Crypto Accelerator 1000 software.
- [Appendix E](#) **provides a copy of the Sun Binary Code License Agreement** and third party licenses.

Using UNIX Commands

This document does not contain information on basic UNIX[®] commands and procedures such as shutting down the system, booting the system, and configuring devices.

See one or more of the following for this information:

- *Solaris Hardware Platform Guide*
- Online documentation for the Solaris Operating System available at `docs.sun.com`
- Other software documentation that you received with your system

Typographic Conventions

Typeface	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. % You have mail.
AaBbCc123	What you type, when contrasted with on-screen computer output	% su Password:
<i>AaBbCc123</i>	Book titles, new words or terms, words to be emphasized	Read Chapter 6 in the <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be superuser to do this.
	Command-line variable; replace with a real name or value	To delete a file, type <code>rm filename</code> .

Shell Prompts

Note – The C shell interprets the `?` character when using `-?` option on the command line. To avoid this interpretation, use the escape character (`\`) directly in front of the `?`. For example in the C shell, the command to display help for the `realmparse` utility, is changed to `realmparse -\?`.

Shell	Prompt
C shell	<i>machine_name%</i>
C shell superuser	<i>machine_name#</i>
Bourne shell and Korn shell	\$
Bourne shell and Korn shell superuser	#

Accessing Sun Documentation Online

A broad selection of Sun system documentation is located at:

<http://www.sun.com/products-n-solutions/hardware/docs>

A complete set of Solaris documentation and many other titles are located at:

<http://docs.sun.com>

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Sun at:

docfeedback@sun.com

Please include the part number (819-0425-11) of your document in the subject line of your email.

Product Overview

This chapter describes the Sun Crypto Accelerator 1000 board. This chapter contains the following sections:

- [“Hardware Overview” on page 1](#)
- [“Hardware and Software Requirements” on page 4](#)

Hardware Overview

The Sun Crypto Accelerator 1000 board is a short PCI board that functions as a cryptographic co-processor to accelerate public key and symmetric cryptography. This product has no external interfaces. The board communicates with the host through the internal PCI bus interface. The purpose of this board is to accelerate a variety of computationally intensive cryptographic algorithms for security protocols in e-commerce applications.

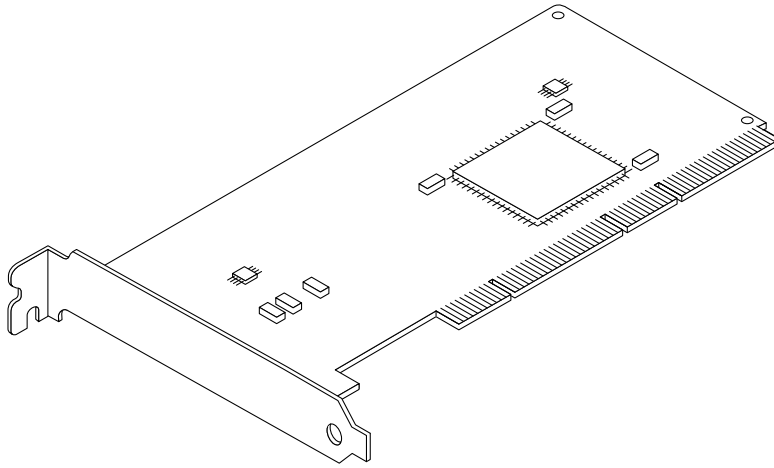


FIGURE 1-1 Sun Crypto Accelerator 1000 Board

Product Features

The Sun Crypto Accelerator 1000 is a cryptographic accelerator board that enhances the performance of SSL on Sun platforms. The main feature of version 2.0 is the integration with the Solaris Cryptographic Framework. The Sun Crypto Accelerator 1000 now accelerates cryptographic algorithms in hardware, and the Solaris Cryptographic Framework complements software implementations of these algorithms. The reason for this complexity is that the cost of accelerating cryptographic algorithms is not uniform across all algorithms. Some cryptographic algorithms were designed specifically to be implemented in hardware, others were designed to be implemented in software. For hardware acceleration, there is the additional cost of moving data from the user application to the hardware acceleration device, and moving the results back to the user application. Note that a few cryptographic algorithms (for example, ARCFOUR) can be performed by highly tuned software as quickly as they can be performed in dedicated hardware.

The Solaris Cryptographic Framework examines each cryptographic request and determines the best location for the acceleration (host processor or Sun Crypto Accelerator 1000), to achieve maximum throughput. Load distribution is based on cryptographic algorithm, current job loading, and data size.

TABLE 1-1 shows which accelerated algorithms may be off-loaded to hardware and which software algorithms are provided for Sun ONE and Apache Web Servers.

TABLE 1-1 Supported SSL Algorithms

Algorithm	Sun ONE Web Servers		Apache Web Servers	
	Hardware	Software	Hardware	Software
RSA	X	X	X	X
DSA	X	X	X	X
Diffie-Hellman				X
DES	X	X	X	X
3DES	X	X	X	X
ARCFOUR				X

Dynamic Reconfiguration and High Availability Considerations

The Sun Crypto Accelerator 1000 hardware and associated software provides the capability to work effectively on Sun platforms supporting Dynamic Reconfiguration (DR) and hot-plugging. During a DR or hot-plug operation, the Sun Crypto Accelerator 1000 software layer automatically detects the addition or removal of a board and adjusts the scheduling algorithms to accommodate the change in hardware resources.

For High Availability (HA) configurations, multiple Sun Crypto Accelerator 1000 boards can be installed within a system or domain to insure that hardware acceleration is continuously available. In the unlikely event of a Sun Crypto Accelerator 1000 hardware failure, the software layer detects the failure and removes the failed card from the list of available hardware cryptographic accelerators. Sun Crypto Accelerator 1000 adjusts the scheduling algorithms to accommodate the reduction in hardware resources. Subsequent cryptographic requests will be scheduled to the remaining cards.

Additionally, the Solaris Cryptographic Framework provides the capability to perform all cryptographic operations in software. This feature supports DR or hot-plug removal of all Sun Crypto Accelerator 1000 boards within a system domain with no adverse functional consequences. A significant performance penalty is incurred until the Sun Crypto Accelerator 1000 hardware is restored to the supported configuration.

Note that the Sun Crypto Accelerator 1000 hardware provides a source for high-quality entropy for the generation of long-term keys. If all the Sun Crypto Accelerator 1000 boards within a domain or system are removed, long-term keys are generated with lower-quality entropy.

Load Sharing

The Solaris Cryptographic Framework distributes load across all boards that are installed within the Solaris domain or system. Incoming cryptographic requests are distributed across the boards based on fixed-length work queues. Cryptographic requests are directed to the first board, and subsequent requests stay directed to the first board until it is running at full capacity. Once the first board is running at full capacity, further requests are queued to the first board available that can accept the request of this type. The queueing mechanism is designed to optimize throughput by facilitating request coalescing at the board.

Hardware and Software Requirements

TABLE 1-2 provides a summary of the hardware and software requirements for the Sun Crypto Accelerator 1000 board.

TABLE 1-2 Hardware and Software Requirements

Hardware and Software	Requirements
Hardware	Sun Blade™ 150, 1500, 2000, 2500 Sun Fire™ 280R, V120, V250, V440, V490, V880, V880z, V890, V1280, 2900, 4800, 4810, 6800, Sun Netra™ 120, T1 1400/5, T4 (20), 1280
Operating system	Solaris 10
PCI slots	32-bit or 64-bit 33 MHz or 66 MHz
Software	Sun ONE Web Server or Apache Web Server on Solaris 10 Any required patches to run the Sun ONE or Apache Web Servers

Required Patches

Refer to the Sun Crypto Accelerator 1000 Board Version 2.0 Release Notes for required patch information.

Installing the Sun Crypto Accelerator 1000 Board

This chapter describes how to install the Sun Crypto Accelerator 1000 hardware and software. This chapter includes the following sections:

- [“Handling the Board” on page 7](#)
 - [“Installing the Board” on page 8](#)
 - [“Directories and Files” on page 18](#)
-

Handling the Board

Each board is packed in a special antistatic bag to protect it during shipping and storage. To avoid damaging the static-sensitive components on the board, reduce any static electricity on your body before touching the board by using one of the following methods:

- Touch the metal frame of the computer.
- Attach an antistatic wrist strap to your wrist and to a grounded metal surface.



Caution – To avoid damaging the sensitive components on the board, wear an antistatic wrist strap when handling the board, hold the board by its edges only, and always place the board on an antistatic surface (such as the plastic bag it came in).

Installing the Board

Installing the Sun Crypto Accelerator 1000 board involves inserting the board into the system and loading the software tools. The hardware installation instructions include only general steps for installing the board. Refer to the documentation that came with your system for specific installation instructions.

▼ To Install the Hardware

1. **As superuser, follow the instructions that came with your system to shut down and power off the computer, disconnect the power cord, and remove the computer cover.**
2. **Locate an unused PCI slot (preferably a 64-bit, 66 MHz slot).**
3. **Attach an antistatic wrist strap to your wrist, and attach the other end to a grounded metal surface.**
4. **Using a Phillips-head screwdriver, remove the screw from the PCI slot cover.**
Save the screw to hold the bracket in Step 5.
5. **Holding the Sun Crypto Accelerator 1000 board by its edges only, take it out of the plastic bag and insert it into the PCI slot**
6. **Secure the screw on the rear bracket.**
7. **Replace the computer cover, reconnect the power cord, and power on the system.**
8. **Verify that the board is properly installed by issuing the `show-devs` command at the `ok` prompt:**

```
ok show-devs
. . .
/pci@1f,2000/pci108e,5455@1
/pci@1f,1000/pci108e,5455@5
. . .
```

The lines `/pci@1f,2000/pci108e,5455@n` show that the board is installed and recognized by the system. There will be one such line for each board in the system.

Installing the Sun Crypto Accelerator 1000 Software With the `install` Script

The Sun Crypto Accelerator 1000 software is included on the Sun Crypto Accelerator 1000 CD. You may need to download patches from the SunSolve web site. Refer to the *Sun Crypto Accelerator 1000 Board Version 2.0 Release Notes* for the required patches.

There are two methods to install the software: manually or with the `install` script. This section describes how to install the software with the `install` script. To install the software manually, refer to [“Installing the Software Without the `install` Script” on page 14](#).

Version 1.1 and 2.0 Software Contained on the CD-ROM

The Sun Crypto Accelerator 1000 Version 2.0 CD-ROM contains both Versions 1.1 and 2.0 of the software.



Caution – Version 1.1 is for Solaris 8 and 9. Version 2.0 is supported on Solaris 10 only.

The `install` script path to each version is as follows:

For Version 1.1:

```
/cdrom/cdrom0/Sun_Crypto_Acc_1000_1_1
```

For Version 2.0:

```
/cdrom/cdrom0/Sun_Crypto_Acc_1000_2_0
```

The respective installation scripts are located in these directories.

▼ To Install the Software With the `install` Script

1. If Version 1.x exists on your Solaris 10 system, use the following command to remove all Version 1.x packages:

```
# pkgrm SUNWcrys1 SUNWdcav SUNWdcar SUNWcrys2 SUNWcrypu SUNWcrypr  
SUNWdcamn SUNWcrypm
```

The Sun Crypto Accelerator 1000 Version 1.x software should not be installed on Solaris 10.

2. Insert the Sun Crypto Accelerator 1000 CD into a CD-ROM drive that is connected to your system.
 - If your system is running Sun Enterprise Volume Manager™, it should automatically mount the CD-ROM to the `/cdrom/cdrom0` directory.
 - If your system is not running Sun Enterprise Volume Manager, mount the CD-ROM as follows:

```
# mount -F hsfs -o ro /dev/dsk/c0t6d0s2 /cdrom
```

You see the following files and directories in the `/cdrom/cdrom0` directory.

TABLE 2-1 Files in the `/cdrom/cdrom0` Directory

File or Directory	Contents
README	Release information
Sun_Crypto_Acc_1000_1_1	Contains the Sun Crypto Accelerator 1000 Version 1.1 software for Solaris 8 and 9
Sun_Crypto_Acc_1000_2_0	Contains the Sun Crypto Accelerator 1000 Version 2.0 software for Solaris 10 only

Refer to the *Sun Crypto Accelerator 1000 Board Version 1.1 Installation and User's Guide* (817-3693-10) for instructions on how to install the Version 1.1 software.

You see the following files and directories in the
/cdrom/cdrom0/Sun_Crypto_Acc_1000_2_0 directory.

TABLE 2-2 Files in the /cdrom/cdrom0/Sun_Crypto_Acc_1000_2_0 Directory

File or Directory	Contents
README	
Copyright	U.S. copyright file
FR_Copyright	French copyright file
install	Script that installs the Sun Crypto Accelerator 1000 software
remove	Script that removes the Sun Crypto Accelerator 1000 software
Docs	<i>Sun Crypto Accelerator 1000 Board Version 2.0 Installation and User's Guide</i> <i>Sun Crypto Accelerator 4000 Board Version 2.0 Release Notes</i>
Packages	Contains the Sun Crypto Accelerator 1000 software packages: SUNWdcamn DCA Crypto Accelerator Manual Page SUNWdcar DCA Crypto Accelerator (Root) SUNWdcaf DCA Crypto Accelerator (usr) SUNWdcau DCA Crypto Accelerator (Utilities)

3. Install the required software by typing:

```
# cd /cdrom/cdrom0/Sun_Crypto_Acc_1000_2_0
# ./install
```

The install script analyzes the system to determine which required patches need to be installed, installs those patches, and installs the main software—for example:

Note – The copyright and license information was omitted from the following example. Refer to [Appendix E](#) for copyright and software licenses.

```
# ./install
This program installs the software for the Sun Crypto Accelerator
1000, Version 2.0.

This script is about to take the following actions:
- Install Sun Crypto Accelerator 1000 support for Solaris 10

Copyright 2005 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.

To cancel installation of this software, press 'q' followed by a Return.
```

****OR****

Press Return key to begin installation:

*** Installing Sun Crypto Accelerator 1000 software for Solaris 10...

Installing required packages:

SUNWdcac SUNWdcac SUNWdcac SUNWdcac

Installation of <SUNWdcac> was successful.

Installation of <SUNWdcac> was successful.

Installation of <SUNWdcac> was successful.

Installation of <SUNWdcac> was successful.

*** Installation complete.

To remove this software, use the 'remove' script on this CDROM, or the following script:

```
/var/tmp/crypto_acc.remove
```

A log of this installation can be found at:

```
/var/tmp/crypto_acc.install.2005.02.04.1507
```

Directories and Files

[TABLE 2-6](#) shows the directories created by the default installation of the Sun Crypto Accelerator 1000 software.

TABLE 2-3 Sun Crypto Accelerator 1000 Directories

Directory	Contents
/opt/SUNWconn/bin	
/opt/SUNWconn/crypto/lib	Soft links to /usr/lib/libpkcs11.so
/opt/SUNWconn/crypto/lib/sparcv9	Soft links to /usr/lib/sparcv9/libpkcs11.so
/opt/SUNWconn/cryptov2/bin	Application executables
/opt/SUNWconn/cryptov2/man	Manual pages
/opt/SUNWconn/man	Manual pages

FIGURE 2-2 shows the hierarchy of these directories and files.

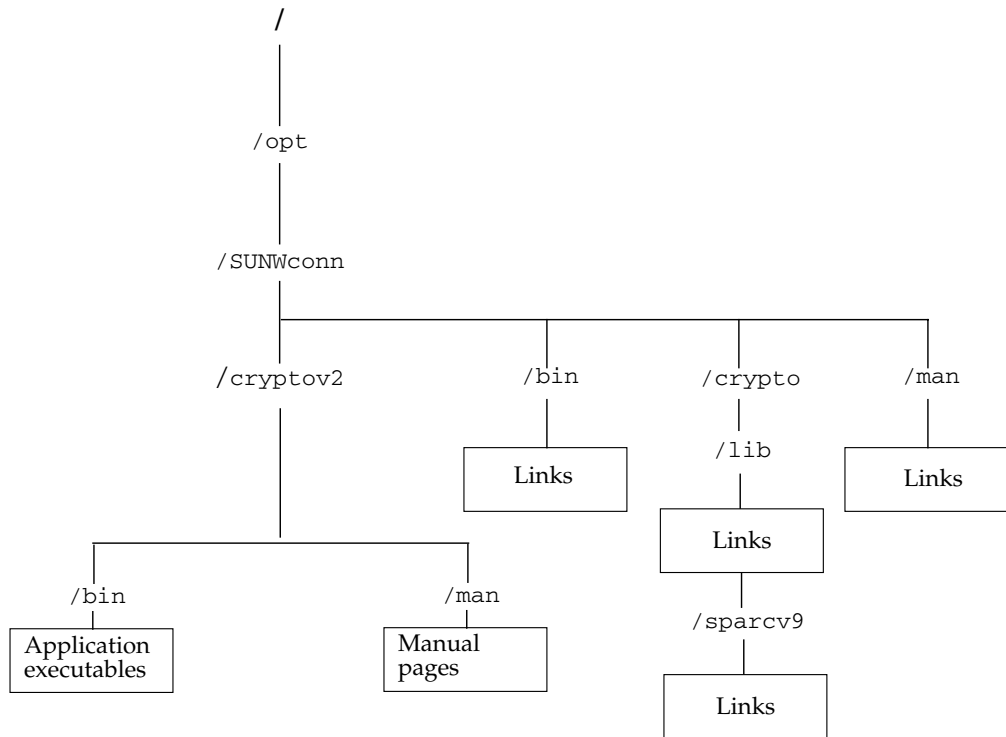


FIGURE 2-1 Sun Crypto Accelerator 1000 Version 2.0 Directories and Files

Removing the Software With the remove Script

There are three methods to remove the software: the `/cdrom/cdrom0/remove` script on the CD-ROM, the `/var/tmp/crypto_acc.remove` script on the server, or the `pkgrm` command. This section describes how to remove the software with the two removal scripts. For instructions on removing the software with the `pkgrm` command refer to [“Removing the Software Without the remove Script” on page 19](#).

Use the `remove` script for software removal if you used the `install` script to install the software. Use the `/var/tmp/crypto_acc.remove` script if you installed the software manually.

▼ To Remove the Software With the `remove` Script on the CD-ROM

- Type the following with the Sun Crypto Accelerator 1000 CD-ROM inserted:

```
# cd /cdrom/cdrom0/Sun_Crypto_Acc_4000_2_0
# ./remove
```

▼ To Remove the Software With the `/var/tmp/crypto_acc.remove` Script

A log of this installation can be found at:

```
/var/tmp/crypto_acc.install.date
```

- Type the following:

```
# /var/tmp/crypto_acc.remove
```

Installing the Software Without the `install` Script

This section describes how to install the Sun Crypto Accelerator 1000 software manually without using the installation script (`/cdrom/cdrom0/Sun_Crypto_Acc_1000_2_0/install`) provided on the product CD.

The Sun Crypto Accelerator 1000 software is included on the Sun Crypto Accelerator 1000 CD. You might need to download patches from the SunSolve web site. Refer to the Sun Crypto Accelerator 1000 Board Version 1.1 Release Notes for the required patches.

Version 1.1 and 2.0 Software Contained on the CD-ROM

The Sun Crypto Accelerator 1000 Version 2.0 CD-ROM contains both Versions 1.1 and 2.0 of the software.



Caution – Version 1.1 is for Solaris 8 and 9. Version 2.0 is supported on Solaris 10 only.

The install script path to each version is as follows:

For Version 1.1:

```
/cdrom/cdrom0/Sun_Crypto_Acc_1000_1_1
```

For Version 2.0:

```
/cdrom/cdrom0/Sun_Crypto_Acc_1000_2_0
```

The respective installation scripts are located in these directories.

▼ To Install the Software Without the `install` Script

1. The Sun Crypto Accelerator 1000 Version 1.x software should not be installed on Solaris 10. If Version 1.x exists on your Solaris 10 system, use the following command to remove all Version 1.x packages:

```
# pkgrm SUNWcrys1 SUNWdcav SUNWdcar SUNWcrys2 SUNWcrypu SUNWcrypr  
SUNWdcam SUNWcrypm
```

2. Insert the Sun Crypto Accelerator 1000 CD into a CD-ROM drive that is connected to your system.
 - If your system is running Sun Enterprise Volume Manager™, it should automatically mount the CD-ROM to the `/cdrom/cdrom0` directory.
 - If your system is not running Sun Enterprise Volume Manager, mount the CD-ROM as follows:

```
# mount -F hsfs -o ro /dev/dsk/c0t6d0s2 /cdrom
```

You see the following files and directories in the `/cdrom/cdrom0` directory.

TABLE 2-4 Files in the `/cdrom/cdrom0` Directory

File or Directory	Contents
README	Release information
Sun_Crypto_Acc_1000_1_1	Contains the Sun Crypto Accelerator 1000 Version 1.1 software for Solaris 8 and 9
Sun_Crypto_Acc_1000_2_0	Contains the Sun Crypto Accelerator 1000 Version 2.0 software for Solaris 10 only

Refer to the *Sun Crypto Accelerator 1000 Board Version 1.1 Installation and User's Guide* (816-2450-11) for instructions on how to install the Version 1.1 software.

You see the following files and directories in the `/cdrom/cdrom0` directory.

TABLE 2-5 Files in the `/cdrom/cdrom0/Sun_Crypto_Acc_1000_2_0` Directory

File or Directory	Contents
Copyright	U.S. copyright file
FR_Copyright	French copyright file
Docs	Sun Crypto Accelerator 1000 Board Version 2.0 Installation and User's Guide
Packages	Contains the Sun Crypto Accelerator 1000 software packages: SUNWdcamn – DCA Crypto Accelerator Manual Page SUNWdcar – DCA Crypto Accelerator (Root) SUNWdcau – DCA Crypto Accelerator (Utilities) SUNWdcaf – DCA Crypto Accelerator Supplemental (usr)

3. Install the software packages by typing:

```
# cd /cdrom/cdrom0/Sun_Crypto_Acc_1000_2_0/Packages
# pkgadd -d .
```

At the prompt, enter **all** to install all of the packages.

4. To verify that the software is installed properly, run the `pkginfo` command.

```
# pkginfo SUNWdcamn SUNWdcar SUNWdcau SUNWdcaf
system SUNWdcamn   DCA Crypto Accelerator Manual Page
system SUNWdcar    DCA Crypto Accelerator (Root)
system SUNWdcau    DCA Crypto Accelerator (Utilities)
system SUNWdcaf    DCA Crypto Accelerator Supplemental (usr)
```

5. (Optional) To ensure that the driver attached, run the `prtconf` command. If multiple Sun Crypto Accelerator 1000 boards are installed, multiple lines are displayed as shown in the following example.

```
# prtconf
pci108e,5455, instance #0
pci108e,5455, instance #1
```

6. (Optional) Run the `modinfo` command to see that modules are loaded.

However, until you have actually used the Sun Crypto Accelerator 1000 board to perform cryptographic operations, `kcl` and `cryptio` may not be loaded or appear.

```
# modinfo | grep Crypto
79 7bb80000   adc0 101  1  dca (PCI Crypto Accelerator 2.0)
79 7bb80000   adc0 101  1  dca (PCI Crypto Accelerator Mod 2.0)
```

7. (Optional) Verify that the modules are loaded using the Solaris Cryptographic Framework command.

```
# cryptoadm list
kernel hardware providers:
    dca/0
```

Directories and Files

TABLE 2-6 shows the directories created by the default installation of the Sun Crypto Accelerator 1000 software.

TABLE 2-6 Sun Crypto Accelerator 1000 Directories

Directory	Contents
/opt/SUNWconn/bin	
/opt/SUNWconn/crypto/lib	Soft links to /usr/lib/libpkcs11.so
/opt/SUNWconn/crypto/lib/sparcv9	Soft links to /usr/lib/sparcv9/libpkcs11.so
/opt/SUNWconn/criptov2/bin	Application executables
/opt/SUNWconn/criptov2/man	Manual pages
/opt/SUNWconn/man	Manual pages

FIGURE 2-2 shows the hierarchy of these directories and files.

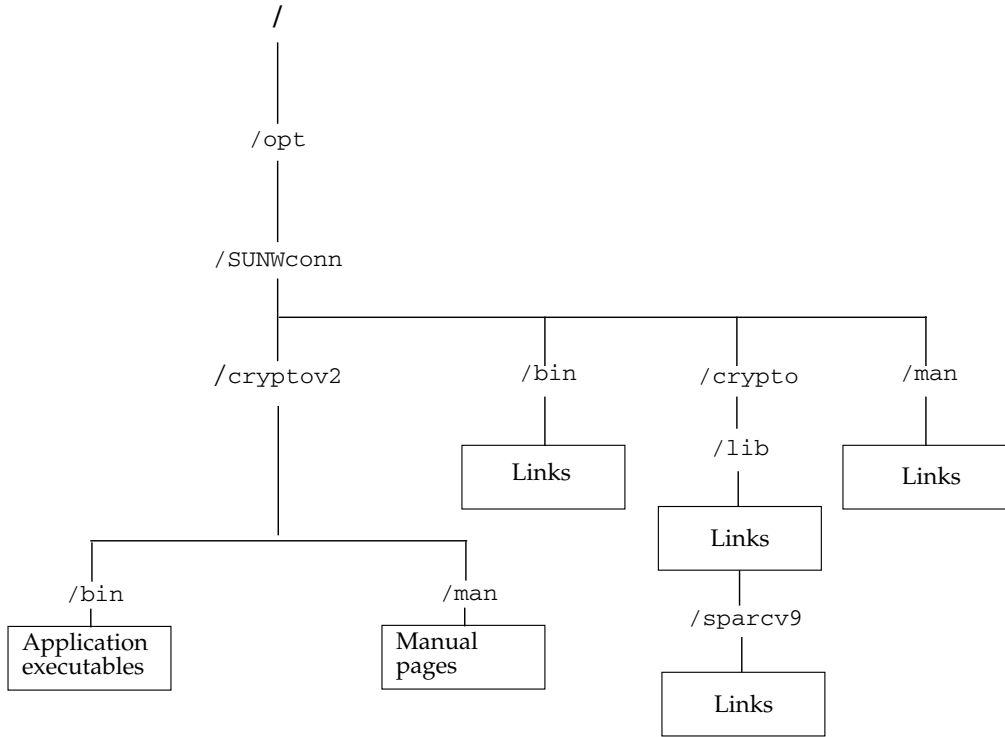


FIGURE 2-2 Sun Crypto Accelerator 1000 Version 2.0 Directories and Files

Removing the Software Without the remove Script



Caution – Before removing the Sun Crypto Accelerator 1000 software you must disable any web servers you have enabled for use with the Sun Crypto Accelerator 1000 board. Failure to do so will leave those web servers nonfunctional.

▼ To Remove the Software Without the `remove` Script

- As superuser, use the `pkgrm` command to remove only the software packages you installed.



Caution – Installed packages must be removed in the order shown. Failure to remove them in this order could result in dependency warnings and leave kernel modules loaded

If you installed all the packages, you would remove them as follows:

```
# pkgrm SUNWdcamn SUNWdcau SUNWdcar SUNWdcf
```

Installing and Configuring Sun ONE Server Software

This chapter describes how to configure the Sun Crypto Accelerator 1000 board for use with Sun ONE servers. This chapter includes the following sections:

- [“Overview of Enabling Sun ONE Web Servers” on page 21](#)
- [“Installing and Configuring Sun ONE Web Server 6.1” on page 22](#)

Note – The Sun ONE servers described in this manual were previously named iPlanet™ Servers.

Note – All Sun ONE server software is supported for use with the board. The example in this section covers configuring the Sun ONE Web Server only. Refer to the Sun ONE documentation for details on how to install and configure Sun ONE server software.

Overview of Enabling Sun ONE Web Servers

To enable Sun ONE Web Servers you must complete the following procedures, that the rest of the chapter explains in detail.

1. **Install the Sun ONE Web Server.**
2. **Create a trust database.**
3. **Request a certificate.**

4. **Install the certificate.**
5. **Configure the Sun ONE Web Server.**



Caution – These procedures must be followed in the order given. Failure to do so could result in an incorrect configuration.

Installing and Configuring Sun ONE Web Server 6.1

This section describes how to install and configure Sun ONE Web Server 6.1 to use the board. You must perform these procedures in order. Refer to the Sun ONE Web Server documentation for more information about installing and using Sun ONE Web Servers. This section includes the following procedures:

- [“To Install Sun ONE Web Server 6.1” on page 22](#)
- [“Configuring Sun ONE Web Server 6.1” on page 23](#)
- [“To Register the Board With the Web Server” on page 24](#)
- [“To Generate a Server Certificate” on page 27](#)
- [“To Install the Server Certificate” on page 30](#)
- [“To Enable the Web Server for SSL” on page 31](#)

▼ To Install Sun ONE Web Server 6.1

1. **Download the Sun ONE Web Server 6.1 software.**

You can find the web server software at the following URL:
<http://www.sun.com/>

2. **Change to the installation directory and extract the web server software.**
3. **Install the web server with the setup script from the command-line.**

The default path name for the server is: `/opt/SUNWwbsvr/`.

This chapter refers to the default paths. If you decide to install the software in a different location, be sure to note where you installed it.

```
# ./setup
```


4. Answer the prompts from the installation script.

Except for the following prompts, you can accept the defaults:

- a. Agree to accept the license terms by typing `yes`.
- b. Enter a fully qualified domain name.
- c. Enter the Sun ONE Web Server 6.1 Administration Server password twice.
- d. Press Return when prompted.

Configuring Sun ONE Web Server 6.1

These procedures create a trust database; register the board with the web server; generate and install a server certificate; and enable the web server for SSL.

▼ To Create a Trust Database

1. Start the administration server.

To start a Sun ONE Web Server, use the following command (instead of running `startconsole` as setup requests):

```
# /opt/SUNWwbsvr/https-admsrv/start
Sun ONE Web Server 6.1 B08/22/2003 12:37
info: CORE3016: daemon is running as super-user
info: CORE5076: Using [Java HotSpot(TM) Server VM, Version 1.4.1_03]
from [Sun Microsystems Inc.]
info: WEB0100: Loading web module in virtual server [vs-admin] at
[/admin-app]
info: HTTP3072: [LS ls1] http://hostname.domain:8888 ready to accept
requests
startup: server started successfully
```

The response provides the URL for connecting to your servers.

2. Start the Sun ONE administration server by opening up a web browser and entering:

```
http://hostname.domain:admin-port
```

In the pop-up window, enter the Sun ONE Web Server administration server username and password you selected while running `setup`.

Note – If you used the default settings during Sun ONE Web Server setup, enter the word `admin` for the User ID or the Sun ONE Web Server administration server username.

3. Click **OK**.

4. **Create the trust database for the web server instance.**

You might want to enable security on more than one web server instance. If so, repeat this process for each web server instance.

Note – If you want to run SSL on the administration server as well, the process of setting up a trust database is similar. Refer to the Sun ONE documentation for more information.

a. Click the **Servers** tab in the administration server.

b. Select a server and click the **Manage** button.

c. Click the **Security** tab near the top of the page and select the **Create Database** link.

d. Enter a password (web server trust database) in the two dialog boxes and click **OK**.

Choose a password of at least eight characters. This will be the password used to start the internal cryptographic modules when the Sun ONE Web Server runs in secure mode.

▼ To Register the Board With the Web Server

1. **Configure Sun Metaslot keystore. Login as the Web Server Administration Server user you chose during Sun ONE Web Server installation (the default is root). Use the following command to setup the Sun Metaslot keystore. The default password is `changeme` if it is prompted. The new password you enter here will be needed**

to start the Sun ONE Web Server. For convenience, you may also use the same password you created in the last section (To Create a Trust Database) for Sun Metaslot.

```
% METASLOT_ENABLED=false
% export METASLOT_ENABLED
% pktool setpin
```

Restore the METASLOT_ENABLED environment variable using the following command.

```
% METASLOT_ENABLED=true
% export METASLOT_ENABLED
```

The `pktool setpin` command creates the `.sunw` directory in the home directory of the Administration Server user. This directory will be used by the System User you chose during Sun ONE Web Server installation (the default user is `webservd`). Change to the home directory of the Administration Server user and use the following command to change the ownership and groupship of `.sunw` directory and all its contents to the System User.

```
% chown -R webservd:webservd .sunw
```

Use the following command to disable the `CKM_SSL3_PRE_MASTER_KEY_GEN`, `CKM_SSL3_MASTER_KEY_DERIVE`, `CKM_SSL3_KEY_AND_MAC_DERIVE`, `CKM_SSL3_MASTER_KEY_DERIVE_DH`, `CKM_SSL3_MD5_MAC`, `CKM_SSL3_SHA1_MAC` mechanisms in the Sun Metaslot.

Determine whether the system is using the non-export or export version of `softtoken` with the following command:

```
% cryptoadm list -p
```

If `pkcs11_softtoken.so` is returned in the output of the previous command, disable the algorithms with the following command.

Note – When executing the `cryptoadm` command, all strings must be entered on one line. You must be superuser to execute this command.

```
% cryptoadm disable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
mechanism=
CKM_SSL3_PRE_MASTER_KEY_GEN,CKM_SSL3_MASTER_KEY_DERIVE,CKM_SSL3_KEY_AND_MAC_DE
RIVE,CKM_SSL3_MASTER_KEY_DERIVE_DH,CKM_SSL3_MD5_MAC,CKM_SSL3_SHA1_MAC
```

Alternately, if `pkcs11_softtoken_extra.so` is returned in the output of the `cryptoadm list -p` command, disable the algorithms with the following command:

```
% cryptoadm disable provider=/usr/lib/security/\$ISA/pkcs11_softtoken_extra.so
mechanism=
CKM_SSL3_PRE_MASTER_KEY_GEN,CKM_SSL3_MASTER_KEY_DERIVE,CKM_SSL3_KEY_AND_MAC_DE
RIVE,CKM_SSL3_MASTER_KEY_DERIVE_DH,CKM_SSL3_MD5_MAC,CKM_SSL3_SHA1_MAC
```

2. Register the Solaris PKCS#11 library in the security module database of the Sun ONE Web Server using `modutil`.

Note – `modutil` is a utility developed by Mozilla and is available with the Sun ONE distribution. By default, the `modutil` is located at `/opt/SUNWwbsvr/bin/https/admin/bin` directory. It uses the NSS libraries located at `/opt/SUNWwbsvr/bin/https/lib`. This directory should be included in the environment variable, `$LD_LIBRARY_PATH`.

```
% modutil -dbdir /opt/SUNWwbsvr/alias -nocertdb -add "Solaris Cryptographic
Framework" -libfile /usr/lib/libpkcs11.so
```

3. Certain Sun ONE applications ask for a password for every known PKCS#11 token. To limit the slots presented to those required to start the web server, disable all slots except for one slot used by the Sun ONE application.

```
% modutil -dbdir /opt/SUNWwbsvr/alias -nocertdb -disable "Solaris Cryptographic
Framework"
% modutil -dbdir /opt/SUNWwbsvr/alias -nocertdb -enable "Solaris Cryptographic
Framework" -slot "Sun Metaslot"
```

▼ To Generate a Server Certificate

1. Restart the Sun ONE Web Server 6.1 Administration Server by typing the following commands. The response provides the URL for connecting to your servers.

```
% /opt/SUNWwbsvr/https-admserv/stop  
% /opt/SUNWwbsvr/https-admserv/start
```

2. Start the Administration GUI by opening up a web browser and typing:

```
http://hostname.domain:admin-port
```

In the authentication dialog box enter the Sun ONE Web Server 6.1 Administration Server user name and password you selected while running setup.

Note – If you used the default settings during Sun ONE Web Server setup, enter **admin** for the user ID or the Sun ONE Web Server 6.1 Administration Server user name.

3. Click **OK**.

The Sun ONE Web Server 6.1 Administration Server window is displayed.

4. To request the server certificate, select the **Servers** tab near the top of Sun ONE Web Server 6.1 Administration Server window. Then select a server from the drop-down menu and click the **Manage** button.

The Sun ONE Web Server 6.1 Server Manager window is displayed.

5. Select the Security tab near the top of the Sun ONE Web Server 6.1 Server Manager window. Then click the Request a Certificate link on the left panel.

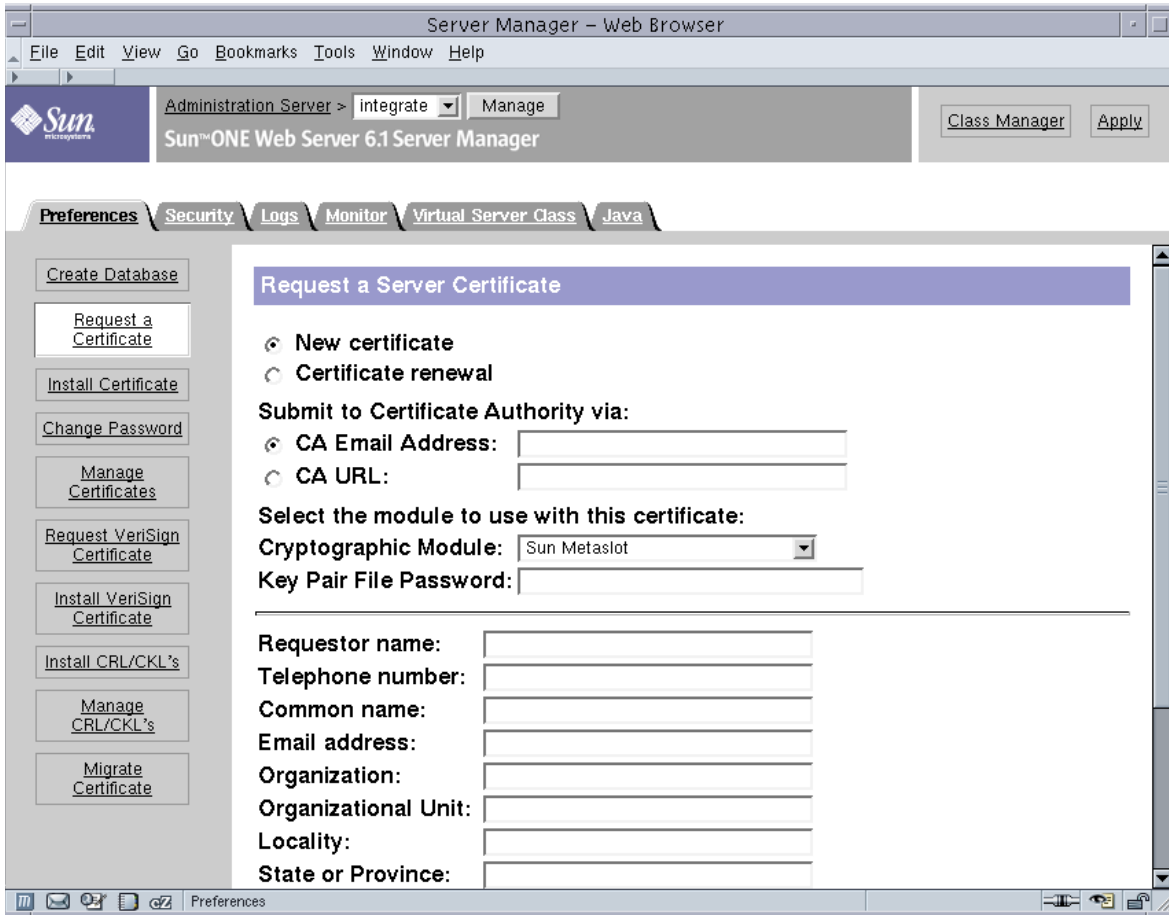


FIGURE 3-1 Sun ONE Web Server 6.1 Administration Server Request a Server Certificate Dialog Box Using Sun Metaslot

6. Fill out the form to generate a certificate request, using the following information:
 - a. Select a New Certificate.

If you can directly post your certificate request to a web-capable certificate authority or registration authority, select the CA URL link. Otherwise, select CA Email Address and enter an email address where you would like the certificate request to be sent.

b. Select the Cryptographic Module you want to use.

Each slot has its own entry in this pull-down menu. For this example, the Sun Metaslot is chosen.

c. In the Key Pair File Password dialog box, provide the password for the user that will own the key.

This password is the one you used to configure the Sun Metaslot.

d. Type the appropriate information for the requestor information fields in [TABLE 3-1](#).

TABLE 3-1 Requestor Information Fields

Field	Description
Requestor Name	Contact information for the requestor
Telephone Number	Contact information for the requestor
Common Name	Web site domain that is typed in a visitor's browser
Email Address	Contact information for the requestor
Organization	Company name
Organizational Unit	(Optional) Department of the company
Locality	(Optional) City, county, principality, or country
State	(Optional) Full name of the state
Country	Two-letter ISO code for the country (for example, the United States is US)

e. Click OK to submit the information.

7. Use a certificate authority to generate the certificate.

- If you choose to post your certificate request to a CA URL, the certificate request is automatically posted there.
- If you choose the CA Email Address, copy the certificate request that was emailed to you with the headers and hand it off to your certificate authority.

8. Once the certificate is generated, copy it, along with the headers, to the clipboard.

Note – The certificate is different from the certificate request and is usually presented to you in text form. Keep this data on the clipboard for [Step 4](#) of “[To Install the Server Certificate](#)” on [page 30](#).

▼ To Install the Server Certificate

1. Click the **Security** tab near the top of the Sun ONE WebServer 6.1 Server Manager window.
2. Select the **Install Certificate** link on the left side of the Sun ONE Web Server 6.1 Administration Server window.

Once your request has been approved by a certificate authority and a certificate has been issued, you must install the certificate in the Sun ONE Web Server.

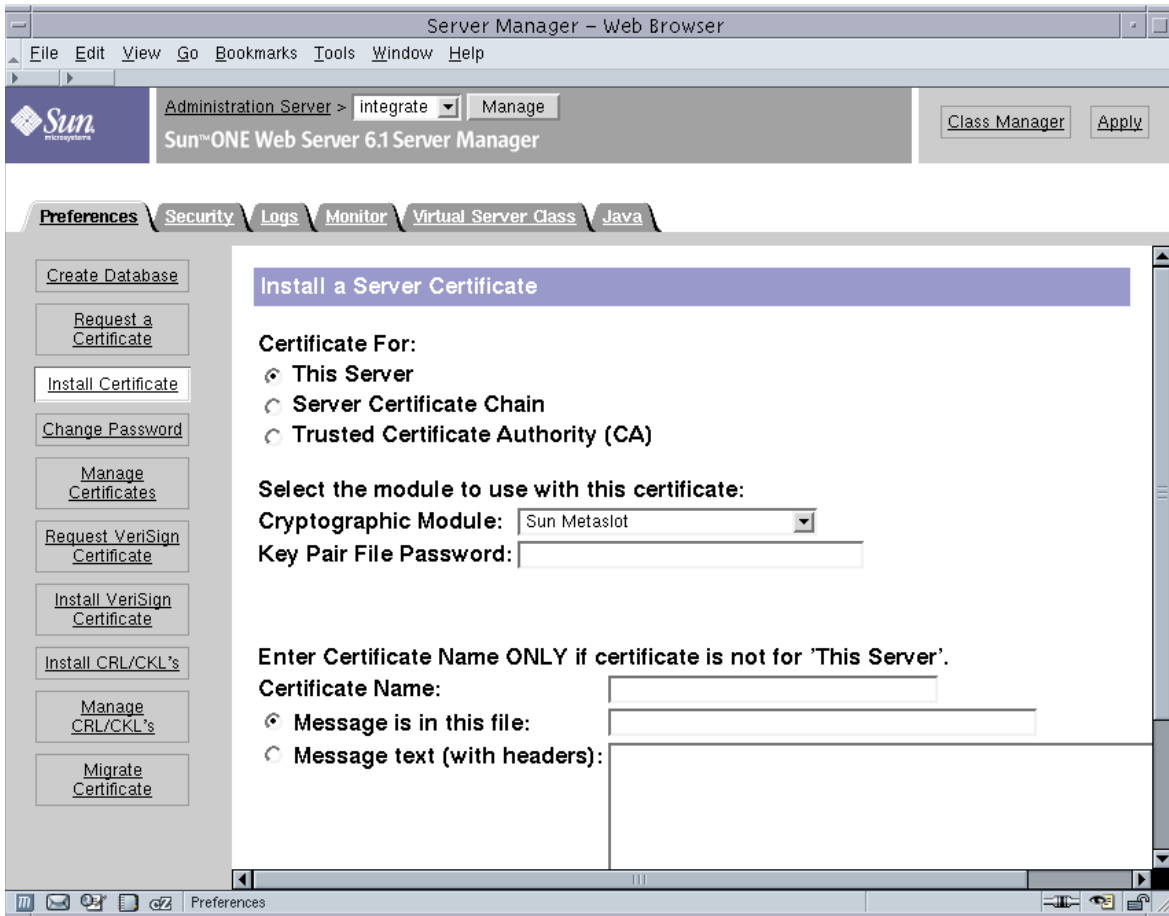


FIGURE 3-2 Sun ONE Web Server 6.1 Administration Server Install a Server Certificate Dialog Box Using Sun Metaslot

3. Fill out the form to install your certificate:

TABLE 3-2 Fields for the Certificate to Install

Fields	Description
Certificate For	This server
Cryptographic Module	Each slot has its own entry in this pull-down menu. Ensure that you select the correct slot name. For this example, use Sun Metaslot
Key Pair File Password	This password is the one you used for configure the Sun Metaslot.
Certificate Name	In most cases, you can leave this blank. If you provide a name, it alters the name the web server uses to access the certificate and key when running with SSL support. The default for this field is <code>Server-Cert</code> .

4. Paste the certificate you copied from the certificate authority (in [Step 8 of the "To Generate a Server Certificate" on page 27](#)) into the Message text box.

You are shown some basic information about the certificate.

5. Click OK.

6. If everything looks correct, click the Add Server Certificate button.

On-screen messages tell you to restart the server. This is not necessary because the web server instance has been shut down the entire time.

You are also notified that in order for the web server to use SSL, the web server must be configured to do so. Use the following procedure to configure the web server.

Now that your web server and the Server Certificate are installed, you must enable the web server for SSL.

7. Use the following command to recursively change permissions of the `.sunw` directory to the System user:

```
% chown -R webservd:webservd .sunw
```

Even though this command was executed previously it needs to be executed again. This step is necessary because the Administration Server user has ownership of the newly imported certificate, and the System user requires ownership.

▼ To Enable the Web Server for SSL

1. Select the Servers tab and make sure the Manage Servers link on the left is selected. Choose a server in the "Select a Server" list and click on the Manage button.

2. **Select the Preferences tab near the top of the page.**

3. **Select the Edit Listen Sockets link on the left panel.**

The main panel lists all the listen sockets set for the web server instance.

a. **Click the link under Listen Socket ID for the listen socket you wish to configure.**

b. **Alter the following fields:**

- **Port:** Set to the port on which you will be running your SSL-enabled web server (usually this is port 443).
- **Security:** Set to Enabled.

c. **Click OK to apply these changes.**

You are back to the list of listen sockets. Make sure the security is enabled.

4. **Click the same listen socket again.**

5. **Enter the password you used for configuring the Sun Metaslot to authenticate to the keystore on the system.**

6. **If you want to change the default set of ciphers, select the cipher suites under the Ciphers heading.**

A dialog box is displayed for changing the cipher settings. You can select either Cipher Default settings, SSL2, or SSL3/TLS. If you select the Cipher Default, you are not shown the default settings. The other two choices require you to select the algorithms you want to enable in a pop-up dialog box. Refer to your Sun ONE documentation on cipher selection.

7. **Select the certificate for the keystore Sun Metaslot: **Server-Cert** (or the name you chose).**

8. **When you have chosen a certificate and confirmed all the security settings, click OK.**

9. **Select the Apply link in the far upper right corner to apply these changes before you start your server.**

10. **Select the Load Configuration Files link to apply the changes.**

You are redirected to a page that allows you to start your web server instance.

If you click the Apply Changes button when the server is off, an authentication dialog box prompts you for the password you used for configuring the Sun Metaslot. This window is not resizable, and you might have a problem submitting the change.

There are two workarounds for this problem:

- Select Load Configuration Files instead.
- Start up the web server first, and click Apply Changes.

11. In the Sun ONE Web Server 6.1 Administration Server window, select the On/Off link on the left side of the window.

12. Enter the passwords for the servers and click Server On.

You are prompted for one or more passwords. At the Module Internal prompt, provide the password for the web server trust database.

At the Module *keystore-name* prompt, enter the password you used for configuring the Sun Metaslot.

Enter the password you entered for configuring other keystores as prompted.

13. Verify the new SSL-enabled web server at the following URL:

`https://hostname.domain:server-port/`

Note – The default *server-port* is 443.

Configuring Sun ONE Web Servers to Start Up Without User Interaction on Reboot

You can enable the Sun ONE Web Servers to perform an unattended startup at reboot with an encrypted key.

▼ To Create an Encrypted Key for Automatic Startup of Sun ONE Web Servers on Reboot

1. Navigate to the **config** subdirectory for your Sun ONE Web Server instance—for example, `/opt/SUNWwbsvr/https-webserver-instance-name/config`.
2. Create a `password.conf` file with only the following lines:

```
internal:trust-db-password  
token-label:password
```

3. Set the file ownership of the password file to the UNIX user ID that the web server runs as, and set the file permissions to be readable only by the owner of the file:

```
# chown web-server-UNIX-user-ID password.conf  
# chmod 400 password.conf
```


Enabling Apache Web Servers

This chapter explains how to configure and enable the Sun Crypto Accelerator 1000 board for use with Apache Web Servers. This chapter includes the following sections:

- [“Creating a Private Key and Certificate” on page 35](#)
- [“Enabling Apache Web Servers” on page 37](#)

Creating a Private Key and Certificate

The following procedure describes how to create the private key and certificate required to enable Apache Web Servers to use the Sun Crypto Accelerator 1000 board. If you already have a private key and certificate, go to [“Enabling Apache Web Servers” on page 37](#).

▼ To Create a Private Key and Certificate

1. Generate an RSA private key in Privacy-Enhanced Mail (PEM) format.

```
% /usr/sfw/bin/openssl genrsa -des3 -out /etc/apache/ssl.key/server.key 1024
```

2. Create your PEM passphrase.

This passphrase protects the key material. Be sure to select a strong passphrase, but one that you can remember. If you forget the passphrase, you will be unable to access your keys.

```
Enter PEM pass phrase:  
Verifying password - Enter PEM pass phrase:
```



Caution – You must remember the passphrase you enter. Without the passphrase, you cannot access your keys. There is no way to retrieve a lost passphrase.

3. Generate the certificate request.

```
% /usr/sfw/bin/openssl req -new -key /etc/apache/ssl.key/server.key  
-out /etc/apache/ssl.csr/certreq.csr
```

4. Create a certificate request using the keys you just created.

You must first enter the passphrase to access your keys. Then provide the appropriate information for the following fields:

- Country Name: The two-letter ISO code for the country, which is asserted on the certificate and is a required field (for example, the United States is US)
- State or Province Name: (Optional) The full name of the state in this field (or type “.” and press Return).
- Locality: (Optional) City, county, principality, or country, which is also asserted on the certificate if provided
- Organization Name: A value for the Organization to be asserted on the certificate
- Organizational Unit Name: (Optional) A value for the Organizational Unit that will be asserted on the certificate
- Common Name: Website Domain that is typed in a visitor’s browser or contact name
- Email Address: Contact information for requestor
- A challenge password: (Optional). You must remember this password if you choose to enter one.

The following is an example of how the certificate fields are entered:

```
Enter PEM pass phrase:
You are about to be asked to enter information that will be incorporated into
your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:US
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) []:Fictional Company, Inc.
Organizational Unit Name (eg, section) []:Online Sales Division
Common Name (eg, YOUR name) []:www.fictional-company.com
Email Address []:admin@fictional-company.com

Please enter the following 'extra' attributes to be sent with your certificate
request
A challenge password []:
An optional company name []: Fictional Comany, Inc.
```

5. **Hand off the `certreq.csr` file to your certificate authority.**
6. **Once the certificate is signed by the certificate authority, go to the next section to setup the Apache Web Server.**

Enabling Apache Web Servers

Apache Web Server and `mod_ssl` are provided with the Solaris 10 Operating System. The following instructions are for these specific releases of Apache Web Server. Refer to the Apache Web Server documentation for more information.

▼ To Enable the Apache Web Server

1. Create an `httpd` configuration file.

For Solaris systems, the `httpd.conf-example` file is usually in `/etc/apache`. You can use this file as a template and copy it as follows:

```
% cp /etc/apache/httpd.conf-example /etc/apache/httpd.conf
```

2. Replace `ServerName` with your server name in the `httpd.conf` file.

- If you have a private key and certificate, go to [Step 5](#).
- If you do not have a private key and certificate, go to “[Creating a Private Key and Certificate](#)” on page 35.

3. Save the issued key as `/etc/apache/ssl.key/`.

4. Save the issued certificate as `/etc/apache/ssl.crt/server.crt`.

Note – When generating the key and copying the certificate, any cert or key with the same filename is overwritten. Other names can be chosen, the names in this example are defaults. If other names are chosen, the administrator must change the `SSLCertificateFile` and `SSLCertificateKeyFile` directives in `httpd.conf` to point to the new filenames.

5. Start the Apache Web Server.

This example assumes the Apache binary directory is `/usr/apache/bin`; if this is not the Apache binary directory, type in the correct directory.

```
% /usr/apache/bin/apachectl startssl
```

6. Enter your PEM passphrase if prompted for it.

7. Verify the SSL enabled web server with a browser pointing to the following URL:

```
https://ServerName:ServerPort/
```

Note – The default port is 443.

8. Verify that the Sun Crypto Accelerator 1000 Board is being used.

```
% kstat -n dca0
```

Verify that the `rsapivate` field is being incremented in the statistics.

Diagnostics and Troubleshooting

This chapter describes diagnostic tests and troubleshooting for the Sun Crypto Accelerator 1000 software. This chapter includes the following sections:

- “SunVTS Diagnostic Software” on page 41
- “Troubleshooting the Sun Crypto Accelerator 1000” on page 42
- “Using kstat to Determine Cryptographic Activity” on page 43
- “Sun’s Predictive Self-Healing” on page 43

SunVTS Diagnostic Software

SunVTS is Sun’s Validation Test Suite software that focuses on testing the system level network and cryptographic functionality of the Sun Crypto Accelerator 1000 subsystem (driver and hardware). The core SunVTS wrapper provides test control and a user interface to a suite of system level tests. These tests are delivered with packages `SUNWvts` and `SUNWvtsts` to make up a bundle that is contained on the Solaris 10 Software DVDs, and also available for download at <http://www.sun.com/oem/vts>.

The Sun Crypto Accelerator 1000 board can be tested by the SunVTS test, `cryptotest`, that is bundled with the core SunVTS software beginning with SunVTS 6.0 Patch Set 1 (PS1) released with Solaris 10. `cryptotest` provides diagnostics of the cryptographic circuitry of the board.

Refer to the *SunVTS 6.0 Patch Set 1 Documentation Supplement* for instructions on how to perform and monitor the diagnostics provided with `cryptotest`. This document is available at: <http://www.sun.com/products-n-solutions/hardware/docs/Software/Diagnostics/index.html>

Installing SunVTS

The SunVTS test `cryptotest` delivered in the `SUNWvts` and `SUNWvtsts` packages on the Solaris Software DVD, provides diagnostics for the Sun Crypto Accelerator 1000 board. `SUNWvts` and `SUNWvtsts` packages from SunVTS 6.0.1 or later must be installed. Refer to the SunVTS user's guide for installation instructions.

Troubleshooting the Sun Crypto Accelerator 1000

To determine whether the Sun Crypto Accelerator 1000 device is listed in the system: from the OpenBoot PROM (OBP) prompt, type `show-devs` to display the list of devices. You should see lines in the list of devices, similar to the examples below, specific to the Sun Crypto Accelerator 1000 board:

```
ok show-devs
. . .
/pci@1f,0/pci@1/pci108e,5455@2
. . .
```

In the above example, the `pci108e,5455` identifies the device path to the Sun Crypto Accelerator 1000 board. There is no firmware on this board, so OBP level diagnostics are not available.

Using `kstat` to Determine Cryptographic Activity

The Sun Crypto Accelerator 1000 board does not contain lights or other indicators to reflect cryptographic activity on the board. In order to determine whether cryptographic work requests are actually being performed on the board, use the `kstat(1M)` command to display the device usage:

```
# kstat -m dca -i 0 -n dca0

module: dca                instance: 0
name:   dca0               class:   misc
       3desbytes           3040
       3desjobs            5
       crtime              65.342725895
       dsasign              0
       dsaverify           0
       rngbytes            10592
       rngjobs             187
       rngshalbytes        16328
       rngshaljobs         327
       rsapivate           9
       rsapublic           0
       snaptime            106956.467004482
```

Displaying the `kstat` information indicates whether cryptographic requests or “jobs” are being sent to the Sun Crypto Accelerator 1000 board. A change in the “jobs” values over time indicates that the board is accelerating cryptographic work requests sent to the Sun Crypto Accelerator 1000 board. If cryptographic work requests are not being sent to the board, verify your web server configuration per the web server specific configuration.

Sun’s Predictive Self-Healing

Solaris 10 introduces a new architecture for building and deploying systems and services capable of Predictive Self-Healing. The `dca` driver delivers an error telemetry for diagnosis of hardware and software problems by the Solaris Fault Manager, `fmd(1M)`.

When problems are detected by the `dca` driver, error reports are sent to the fault manager daemon for diagnosis and logging. The `fmdump(1M)` utility can be used to view the list of problems diagnosed by the fault manager, along with their Universal Unique Identifiers (UUIDs) and knowledge article message identifiers. The `fmadm(1M)` utility can be used to view the resources on the system believed to be faulty. The `fmstat(1M)` utility can be used to report statistics kept by the fault manager. The fault manager is started automatically when Solaris boots, so it is not necessary to use the `fmd` command directly. Refer to the man pages for more details regarding the use of these tools.

The fault manager also sends a message to the `syslogd(1M)` service to notify an administrator that a problem has been detected. The message directs administrators to a knowledge article at <http://www.sun.com/msg/>, which explains more about the problem impact and appropriate responses. A brief description of the problem and the action required by the administrator is also provided in the message.

Migrating Keys From Version 1.x Realms

The `realmparse` command migrates keys from Sun Crypto Accelerator 1000 1.x realms. This command takes realm files from the Sun Crypto Accelerator 1000 1.x product and lists and migrates the key and certificate objects into a PKCS#11 token presented by the Solaris Cryptographic Framework.

In most cases, the full path to a Sun Crypto Accelerator 1000 1.x realm file must be provided with the `realmparse` command. The exception is the `list` subcommand with the `-t / --token` flag which lists available destination tokens for key and certificate objects presented by the Solaris Cryptographic Framework.

The `realmparse` utility has two subcommands that can be used. The `list` subcommand lists available destination PKCS#11 tokens, users that exist within a Sun Crypto Accelerator 1000 1.x realm file, or objects associated with a specific user.

The `migrate` subcommand moves objects from a realm file to a PKCS#11 token chosen by the administrator using the token's label. If no certificate name is specified using the `-c / --certname` option, all objects associated with the realm user are migrated using the same PKCS#11 attributes that were asserted in the realm file.

If the `-c / --certname` option is used, only those objects with the `CKA_LABEL` PKCS#11 attribute matching the value provided is migrated. Additionally the `-n / --newname` option changes the `CKA_LABEL` value supplied for these objects in the destination token. This option is used when two or more realm users have certificates and keys with the same label.

`realmparse` Options

TABLE 6-1 describes the subcommands and options for the `realmparse` command.

Note – Certain shells interpret the ? character when using -? option on the command line. To avoid this, use the escape character (\) directly in front of the ?. For example in the C shell, the command is changed to `realmparse -\?`.

TABLE 6-1 realparse Options

Option	Description
<i>With no Subcommands</i>	
-? / --help	Displays basic help for this command.
-V / --version	Displays version information for this command.
<i>With the list Subcommand</i>	
-p / --passfile file	Takes the full path to a file containing the realm user's password. If this option is not specified then the application prompts for the password. This option must be used with the -u / --user option.
-t / --token	Displays the PKCS#11 tokens available in the system through the Solaris Cryptographic Framework. This option, when used with the list subcommand, should be used by itself, and does not require a realm file to be specified.
-u / --user realmuser	Lists objects in the realm associated with the user realmuser.
-v / --verbose	Provides more detailed information when listing a specific realm user's key and certificate objects. This option must be used with the -u / --user option.
<i>With the migrate Subcommand</i>	
-c / --certname name	Looks for certificates and keys with the label name and migrates them. All other objects owned by that realm user will not be migrated. The name parameter is case-sensitive.
-n / --newname name	For the migrated objects, changes the label from that provided with the -c / --certname option to name. This new name will become the value for the CKA_LABEL attribute for the objects in the destination PKCS#11 token. This option must be used with the -c / --certname option.

TABLE 6-1 realparse Options (Continued)

Option	Description
<i>With no Subcommands</i>	
<code>-p / --passfile file</code>	This option takes the full path to a file containing the realm user's password. If this option is not specified then the application will prompt for the password. This option must be used with the <code>-u / --user</code> option.
<code>-t / --token label</code>	Uses the PKCS#11 token <i>label</i> as the destination for all migrated objects. If a destination PKCS#11 token is not specified on the command line, you are prompted for one.
<code>-u / --user realmuser</code>	Accesses objects in the realm associated with the user <i>realmuser</i> .
<code>-w / --p11passfile file</code>	Takes the full path to a file containing the password for the PKCS#11 token specified with the <code>-t / --token</code> option. If this option is not specified, you are prompted for the password.
<code>-v / --verbose</code>	Provides more detailed information during the migration process.

Examples Using the realmparse Command

This section provides examples of using the `realmparse` command with subcommands and options.

Listing All Available PKCS#11 Tokens

The following command lists all available PKCS#11 tokens.

```
example% /opt/SUNWconn/cryptov2/bin/realmparse list -t
Token Label                               Writeable?
-----
dca/0 Crypto Accel Sym 2.0                No
dca/0 Crypto Accel Asym 2.0              No
Sun Software PKCS#11 Softtoken           Yes
-----
```

Migrating All Objects Associated With a Realm User to the Sun Software PKCS#11 Softtoken

You must execute the `pktool setpin` command before migrating objects with `realmparse`— for example:

```
% pktool setpin
Enter new PIN:
Re-enter new PIN:
```

The following command migrates all objects associated with a realm user `sample-user` to the Sun Software PKCS#11 Softtoken. These objects are retrieved from the realm file `/tmp/oldrealm`.

```
example% realmparse migrate -u "sample-user" -t "Sun Software PKCS#11 Softtoken"
/tmp/oldrealm
Enter realm user password:
Enter PKCS#11 password:
All objects were migrated successfully.
```

Sun Crypto Accelerator 1000 Board Specifications

This appendix outlines the various specifications of the Sun Crypto Accelerator 1000 board. This appendix includes the following sections:

- [“Physical Dimensions” on page 49](#)
- [“Interface Specifications” on page 50](#)
- [“Power Requirements” on page 50](#)
- [“Environmental Specifications” on page 50](#)

Physical Dimensions

TABLE A-1 Physical Dimensions

Dimension	Measurement	Metric Measurement
Length	6.875 inches	174.625 mm
Width	4.2 inches	106.680 mm

Interface Specifications

TABLE A-2 Interface Specifications

Feature	Specification
PCI clock	33 MHz or 66 MHz
Host interface	PCI 2.1 with support for 33 MHz or 66 MHz clock rate and 3.3V or 5V power.
PCI bus width	32-bits or 64-bits

Power Requirements

TABLE A-3 Power Requirements

Specification	Measurement
Maximum power consumption	10W @ 5V 700mW @ 3.3V
Voltage tolerance	5V +/- 5% 3.3V +/- 5%
Operational current	2A @ 1.8V 150mA @ 3.3V

Environmental Specifications

TABLE A-4 Environmental Specifications

Condition	Operating Specification	Storage Specification
Temperature	0° to 70°C, 32° to 160°F	-65°C to +150°C, -85° to 300° F
Relative humidity	5 to 85% non-condensing	0 to 95% non-condensing

Building OpenSSL Applications for Use With the Sun Crypto Accelerator 1000 Board

The Solaris 10 Operating System includes OpenSSL libraries. They are `/usr/sfw/lib/libcrypto.so` and `/usr/sfw/lib/libssl.so` for 32-bit applications and `/usr/sfw/lib/sparcv9/libcrypto.so` and `/usr/sfw/lib/sparcv9/libssl.so` for 64-bit applications. A PKCS#11 OpenSSL engine (with identifier `pkcs11`) is provided in `libcrypto.so`. This engine bridges OpenSSL applications and the Sun Crypto Accelerator 1000 through the PKCS#11 interface provided by the Solaris Cryptographic Framework.

OpenSSL applications should use the PKCS#11 engine through the standard OpenSSL engine interface. The OpenSSL engine interface, along with sample code, is documented in great detail on the OpenSSL web site <http://www.openssl.org/docs/crypto/engine.html>. To use the PKCS#11 engine, the applications are required to use `libcrypto.so` on Solaris 10.

The following command provides simple information on the PKCS#11 OpenSSL engine.

```
% /usr/sfw/bin/openssl engine pkcs11
(pkcs11) PKCS #11 engine support
```

Another example is the OpenSSL speed program which is available also on Solaris 10 Operating System. The following is a sample usage of this program and its output.

```
% /usr/sfw/bin/openssl speed -engine pkcs11 rsa1024
engine "pkcs11" set.
Doing 1024 bit private rsa's for 10s: 5246 1024 bit private RSA's in 0.13s
Doing 1024 bit public rsa's for 10s: 47666 1024 bit public RSA's in 0.90s
OpenSSL 0.9.7d 17 Mar 2004
built on: date not available
options:bn(32,32) md2(int) rc4(ptr,int) des(ptr,risc1,16,long) aes(partial)
blowfish(idx)
compiler: information not available
available timing options: TIMES TIMEB HZ=100 [sysconf value]
timing function used: times
          sign    verify    sign/s  verify/s
rsa 1024 bits  0.0000s  0.0000s  40353.8  52962.2
```

This example tests RSA operations with 1024-bit keys and one process for 10 seconds. Note that for more accurate timing test, the user should use the `-multi` option of the OpenSSL speed program.

The user may check the Sun Crypto Accelerator 1000 usage by using the following command before and after running the OpenSSL speed program.

```
% kstat -n dca0 | grep rsa
```

Building PKCS#11 Applications for Use With the Sun Crypto Accelerator 1000 Board

This appendix describes how to build customized PKCS#11 applications to be used with the board.

The Sun Crypto Accelerator 1000 is registered in the Solaris Cryptographic Framework as a hardware provider. Thus the board can be administered using the system commands. Refer to Solaris Cryptographic Services section in the Solaris 10 *System Administration Guide: Security Services*.

The Solaris Cryptographic Framework provides a PKCS#11 interface. The Sun Crypto Accelerator 1000 is registered with two PKCS#11 slots. The first slot supports CKM_DES_CBC and CKM_DES3_CBC mechanisms and the second supports CKM_DSA, CKM_RSA_PKCS, and CKM_RSA_X_509 mechanisms. Advanced users can develop PKCS#11 applications using this interface to access the Sun Crypto Accelerator 1000 slots to take advantage of hardware accelerations.

The following table summarizes the PKCS#11 mechanisms and the corresponding key ranges:

TABLE C-1

Mechanism	Key Ranges
CKM_DES_CBC	8 bytes
CKM_DES3_CBC	24 bytes
CKM_DSA	512 – 1024 bits
CKM_RSA_PKCS	256 – 2048 bits
CKM_RSA_X_509	256 – 2048 bits

The sample PKCS#11 source code given below prints out the PKCS#11 slots in the system. The following are the sample outputs from this program—3 slots were detected.

- Slot 0 – Sun Metaslot
- Slot 1 – dca/0 Crypto Accel Sym 2.0
- Slot 2 – dca/0 Crypto Accel Asym 2.0

The slots with dca/0 are from the Sun Crypto Accelerator 1000

There are two ways to use the Sun Crypto Accelerator 1000 through the PKCS#11 interface. The first is to use the Sun Metaslot. The Sun Metaslot will use the board for the mechanisms it supports and use its own internal implementations for other mechanisms. The Sun Metaslot also supports load balancing, failover, and so on. For more details, please refer to the Sun Metaslot documentation.

The second is to use the Sun Crypto Accelerator 1000 slots directly. In this way, it is limited to the five mechanisms given above.

The following provides a sample of PKCS#11 source code.

CODE EXAMPLE C-1 Sample PKCS#11 source code

```
#include <stdio.h>
#include <security/cryptoki.h>

int
main(int argc, char **argv)
{
    CK_RV    rv;
    int      i;
    CK_SLOT_ID_PTR pSlotList;
    CK_SLOT_INFO slotInfo;
    CK_ULONG ulSlotCount;

    rv = C_Initialize(NULL);
    if (rv != CKR_OK) {
        printf("C_Initialize failed with code 0x%x\n", rv);
        exit(1);
    }

    rv = C_GetSlotList(1, NULL_PTR, &ulSlotCount);
    if (rv != CKR_OK) {
        printf("C_GetSlotList failed with code 0x%x\n", rv);
        exit(1);
    }

    if (ulSlotCount == 0) {
        printf("No PKCS#11 slots found.\n");
        exit(1);
    }
}
```


CODE EXAMPLE C-1 Sample PKCS#11 source code (*Continued*)

```
}

pSlotList = (CK_SLOT_ID_PTR) malloc(ulSlotCount * sizeof (CK_SLOT_ID));
if (pSlotList == 0) {
    printf("System out of memory.\n");
    exit(1);
}

rv = C_GetSlotList(1, pSlotList, &ulSlotCount);
if (rv) {
    printf("C_GetSlotList failed with code 0x%x\n", rv);
    free(pSlotList);
    exit(1);
}

printf("%d slots were detected\n", ulSlotCount);

for (i = 0; i < ulSlotCount; i++) {
    rv = C_GetSlotInfo(pSlotList[i], &slotInfo);
    if (rv) {
        printf("%d. Could not get Slot Info\n", i);
    } else {
        slotInfo.slotDescription[63] = '\000';
        printf("Slot: %dDescription: %s\n", pSlotList[i],
            slotInfo.slotDescription);
    }
}

free(pSlotList);
}
```

This code can be compiled using the following command in a Solaris 10 system.

```
cc -o test test.c -lpkcs11
```

The pkcs11 libraries are /usr/lib/libpkcs11.so (32-bit mode) and /usr/lib/sparcv9/libpkcs11.so (64-bit mode).

Manual Page

This appendix provides descriptions of the man page included with Sun Crypto Accelerator 1000 software.

The man page can be viewed using the command:

```
man -M /opt/SUNWconn/man page
```

[TABLE D-1](#) lists and describes the available man pages.

TABLE D-1 Sun Crypto Accelerator 1000 Man Pages

man page	Description
dca (7d)	The dca device driver is a leaf driver that provides access control to the underlying hardware cryptographic accelerator. The dca driver requires the presence of layered software for applications and kernel clients to access the provided services.
realmparse (1M)	This command migrates keys from Sun Crypto Accelerator 1000 1.x realms. This command takes realm files from the Sun Crypto Accelerator 1000 1.x product and lists and migrates the key and certificate objects into a PKCS#11 token presented by the Solaris Cryptographic Framework.

Software Licenses

This appendix provides the Sun Binary Code License Agreement and third-party software notices and licenses.

Note – The third-party licenses and notices provided in this appendix are included exactly as they are provided by the owners of the software licenses and notices.

Sun Microsystems, Inc.

Binary Code License Agreement

Sun Microsystems, Inc. ("Sun")

SOFTWARE LICENSE AGREEMENT

READ THE TERMS OF THIS AGREEMENT ("AGREEMENT") CAREFULLY BEFORE OPENING SOFTWARE MEDIA PACKAGE. BY OPENING SOFTWARE MEDIA PACKAGE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCESSING SOFTWARE ELECTRONICALLY, INDICATE YOUR ACCEPTANCE OF THESE TERMS BY SELECTING THE "ACCEPT" BUTTON AT THE END OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS, PROMPTLY RETURN THE UNUSED SOFTWARE TO YOUR PLACE OF PURCHASE FOR A REFUND OR, IF SOFTWARE IS ACCESSED ELECTRONICALLY, SELECT THE "DECLINE" (OR "EXIT") BUTTON AT THE END OF THIS AGREEMENT. IF YOU HAVE SEPARATELY AGREED TO LICENSE TERMS ("MASTER TERMS") FOR YOUR LICENSE TO THIS SOFTWARE, THEN SECTIONS 1-5 OF THIS AGREEMENT ("SUPPLEMENTAL LICENSE TERMS") SHALL SUPPLEMENT AND SUPERSEDE THE MASTER TERMS IN RELATION TO THIS SOFTWARE.

1. Definitions.

(a) "Entitlement" means the collective set of applicable documents authorized by Sun evidencing your obligation to pay associated fees (if any) for the license, associated Services, and the authorized scope

of use of Software under this Agreement.

(b) "Licensed Unit" means the unit of measure by which your use of Software and/or Service is licensed, as described in your Entitlement.

(c) "Permitted Use" means the licensed Software use(s) authorized in this Agreement as specified in your Entitlement. The Permitted Use for any bundled Sun software not specified in your Entitlement will be evaluation use as provided in Section 3.

(d) "Service" means the service(s) that Sun or its delegate will provide, if any, as selected in your Entitlement and as further described in the applicable service listings at www.sun.com/service/servicelist.

(e) "Software" means the Sun software described in your Entitlement. Also, certain software may be included for evaluation use under Section 3.

(f) "You" and "Your" means the individual or legal entity specified in the Entitlement, or for evaluation purposes, the entity performing the evaluation.

2. License Grant and Entitlement.

Subject to the terms of your Entitlement, Sun grants you a nonexclusive, nontransferable limited license to use Software for its Permitted Use for the license term. Your Entitlement will specify (a) Software licensed, (b) the Permitted Use, (c) the license term, and (d) the Licensed Units.

Additionally, if your Entitlement includes Services, then it will also specify the (e) Service and (f) service term.

If your rights to Software or Services are limited in duration and the date such rights begin is other than the purchase date, your Entitlement will provide that beginning date(s).

The Entitlement may be delivered to you in various ways depending on the manner in which you obtain Software and Services, for example, the Entitlement may be provided in your receipt, invoice or your contract with Sun or authorized Sun reseller. It may also be in electronic format if you download Software.

3. Permitted Use.

As selected in your Entitlement, one or more of the following Permitted Uses will apply to your use of Software. Unless you have an Entitlement that expressly permits it, you may not use Software for any of the other Permitted Uses. If you don't have an Entitlement, or if your Entitlement

doesn't cover additional software delivered to you, then such software is for your Evaluation Use.

(a) Evaluation Use. You may evaluate Software internally for a period of 90 days from your first use.

(b) Research and Instructional Use. You may use Software internally to design, develop and test, and also to provide instruction on such uses.

(c) Individual Use. You may use Software internally for personal, individual use.

(d) Commercial Use. You may use Software internally for your own commercial purposes.

(e) Service Provider Use. You may make Software functionality accessible (but not by providing Software itself or through outsourcing services) to your end users in an extranet deployment, but not to your affiliated companies or to government agencies.

4. Licensed Units.

Your Permitted Use is limited to the number of Licensed Units stated in your Entitlement. If you require additional Licensed Units, you will need additional Entitlement(s).

5. Restrictions.

(a) The copies of Software provided to you under this Agreement are licensed, not sold, to you by Sun. Sun reserves all rights not expressly granted. (b) You may make a single archival copy of Software, but otherwise may not copy, modify, or distribute Software. However if the Sun documentation accompanying Software lists specific portions of Software, such as header files, class libraries, reference source code, and/or redistributable files, that may be handled differently, you may do so only as provided in the Sun documentation. (c) You may not rent, lease, lend or encumber Software. (d) Unless enforcement is prohibited by applicable law, you may not decompile, or reverse engineer Software. (e) The terms and conditions of this Agreement will apply to any Software updates, provided to you at Sun's discretion, that replace and/or supplement the original Software, unless such update contains a separate license. (f) You may not publish or provide the results of any benchmark or comparison tests run on Software to any third party without the prior written consent of Sun. (g) Software is confidential and copyrighted. (h) Unless otherwise specified, if Software is delivered with embedded or bundled software that enables functionality of Software, you may not use such software on a stand-alone basis or use any portion of such

software to interoperate with any program(s) other than Software.

(i) Software may contain programs that perform automated collection of system data and/or automated software updating services. System data collected through such programs may be used by Sun, its subcontractors, and its service delivery partners for the purpose of providing you with remote system services and/or improving Sun's software and systems. (j) Software is not designed, licensed or intended for use in the design, construction, operation or maintenance of any nuclear facility and Sun and its licensors disclaim any express or implied warranty of fitness for such uses. (k) No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement.

6. Term and Termination.

The license and service term are set forth in your Entitlement(s). Your rights under this Agreement will terminate immediately without notice from Sun if you materially breach it or take any action in derogation of Sun's and/or its licensors' rights to Software. Sun may terminate this Agreement should any Software become, or in Sun's reasonable opinion likely to become, the subject of a claim of intellectual property infringement or trade secret misappropriation. Upon termination, you will cease use of, and destroy, Software and confirm compliance in writing to Sun. Sections 1, 5, 6, 7, and 9-15 will survive termination of the Agreement.

7. Java Compatibility and Open Source.

Software may contain Java technology. You may not create additional classes to, or modifications of, the Java technology, except under compatibility requirements available under a separate agreement available at www.java.net.

Sun supports and benefits from the global community of open source developers, and thanks the community for its important contributions and open standards-based technology, which Sun has adopted into many of its products.

Please note that portions of Software may be provided with notices and open source licenses from such communities and third parties that govern the use of those portions, and any licenses granted hereunder do not alter any rights and obligations you may have under such open source licenses, however, the disclaimer of warranty and limitation of liability provisions in this Agreement will apply to all Software in this distribution.

8. Limited Warranty.

Sun warrants to you that for a period of 90 days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Some states do not allow limitations on certain implied warranties, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

9. Disclaimer of Warranty.

UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

10. Limitation of Liability.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

11. Export Regulations.

All Software, documents, technical data, and any other materials delivered under this Agreement are subject to U.S. export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with these laws and regulations and acknowledge that you have the responsibility to obtain any licenses to export, re-export, or import as may be required after delivery to you.

12. U.S. Government Restricted Rights.

If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

13. Governing Law.

Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

14. Severability.

If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

15. Integration.

This Agreement, including any terms contained in your Entitlement, is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

Please contact Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054 if you have questions.

Third-Party Licenses

This appendix provides software notices and licenses from other parties that govern the use of such portions.

OPENSSL LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLey License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

```
``Ian Fleming was a UNIX fan!  
How do I know? Well, James Bond  
had the (license to kill) number 007,  
i.e. he could execute anyone."  
-- Unknown
```

MOD_SSL LICENSE

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2000 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."
4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.
5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Index

A

algorithms, 3
Apache Web Servers
 creating a certificate, 35
 enabling, 37

C

commands
 kstat, 43

D

directories
 hierarchy of, 13, 18
Dynamic Reconfiguration, 3

E

enabling
 Apache Web Servers, 37

F

files and directories
 installation, 10, 11, 16

H

High Availability, 3
hot-plug, 3

I

installation
 files and directories, 10, 11, 16

K

kstat command, 43

L

licences
 third party, 65
load sharing, 4

O

OpenBoot PROM, 42
optional packages
 descriptions, 10, 11, 16

P

PKCS#11 interface, 45

R

requirements
 hardware, 4
 software, 4

S

server certificate, 27
software packages, 16
Sun ONE Web Servers
 Sun ONE Web Server 6.0
 generating a server certificate, 27
 installing, 22
 installing a server certificate, 30

T

troubleshooting, 42

trust database

 creating

 iPlanet Web Server 6.0, 23

U

URL

 for Sun ONE software, 22