Sun™ Crypto Accelerator I Board Installation and User's Guide

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303
U.S.A. 650-960-1300

Part No. 806-4575-10
September 2000, Revision A

Send comments about this document to: `docfeedback@sun.com`

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 VCCI 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。

Declaration of Conformity

Compliance Model Number:	Mercury
Product Name:	Crypto Accelerator I

EMC

USA—FCC Class B

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.

European Union

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

EN55022:1995/CISPR22:1997		Class B
EN550024:1998	EN61000-4-2	4 kV (Direct), 8 kV (Air)
	EN61000-4-3	3 V/m
	EN61000-4-4	1.0 kV Power Lines, 0.5 kV Signal Lines
	EN61000-4-5	1 kV Line-Line, 2 kV Line-Gnd Power Lines
	EN61000-4-6	3 V
	EN61000-4-8	3 A/m
	EN61000-4-11	Pass
EN61000-3-2:1995		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:

EN60950:1992, 2nd Edition

Supplementary Information

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

/S/

Dennis P. Symanski DATE
Manager, Compliance Engineering

Sun Microsystems, Inc.
901 San Antonio Road, MPK15-102
Palo Alto, CA 94303-4900, USA

Tel: 650-786-3255
Fax: 650-786-3723

/S/

Peter Arkless DATE
Quality Manager

Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom

Tel: 0506-670000
Fax: 0506 760011

Contents

1. The Sun Crypto Accelerator I Board 1

Installation Requirements 2

Handling the Crypto Accelerator Board 2

Installing the Crypto Accelerator Board 2

▼ To Install the Crypto Accelerator Board 3

▼ To Install the Software 3

▼ To Enable the Board for Netscape 3.6 Enterprise Server 4

▼ To Enable the Board for iPlanet Web Server 4.x 8

▼ To Enable the Board for Other iPlanet Products 13

▼ To Remove the Software 14

Diagnostics and Maintenance 14

Status LED 14

SunVTS Diagnostic Software 14

▼ To Run `cstest` 15

The `cstest` Display 16

Crypto Accelerator Driver Information 17

Crypto Accelerator Board Information 18

Error Codes 19

Error Messages 20

Preface

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

This book assumes that you are a system administrator familiar with the Solaris operating environment.

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*
- AnswerBook2™ online documentation for the Solaris™ operating environment
- 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 `.login` file. Use `ls -a` to list all files. `% You have mail`.

`AaBbCc123`	What you type, when contrasted with on-screen computer output	`%` **`su`**
		`Password:`

AaBbCc123	Book titles, new words or terms, words to be emphasized	Read Chapter 6 in the *User's Guide.* These are called *class* options. You *must* be superuser to do this.
	Command-line variable; replace with a real name or value	To delete a file, type `rm` *filename*.

Shell Prompts

Shell	Prompt
C shell	*machine_name*%
C shell superuser	*machine_name*#
Bourne shell and Korn shell	`$`
Bourne shell and Korn shell superuser	#

Accessing Sun Documentation Online

The `docs.sun.com`^{sm} web site enables you to access a select group of Sun technical documentation on the Web. You can browse the `docs.sun.com` archive or search for a specific book title or subject at:

```
http://docs.sun.com
```

Ordering Sun Documentation

Fatbrain.com, an Internet professional bookstore, stocks select product documentation from Sun Microsystems, Inc.

For a list of documents and how to order them, visit the Sun Documentation Center on Fatbrain.com at:

```
http://www.fatbrain.com/documentation/sun
```

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 (806-4575-10) of your document in the subject line of your email.

The Sun Crypto Accelerator I Board

The Sun Crypto Accelerator I board is a hardware-based, cryptographic security solution that enables a server to sustain maximum performance. It is designed for servers that demand strong cryptographic security yet still need to handle large client loads.

Note – Hereafter in this document, the Sun Crypto Accelerator I board is referred to as the "Crypto Accelerator board."

The Crypto Accelerator board plugs into a server's PCI bus and performs critical cryptographic operations like RSA in hardware. By off-loading cryptographic operations from the server's CPU, the Crypto Accelerator board dramatically decreases the server's response time and increases the number of clients it can support.

The Crypto Accelerator board provides two classes of cryptographic operations in hardware:

- Modular exponentiation functions, including Diffie Hillman, DSA, RSA, and raw modular exponentiation
- Random number generation, which is appropriate for secure key generation

The Crypto Accelerator board executes a 1024-bit RSA private key operation in 5 ms. For greater performance, you can install multiple Crypto Accelerator boards.

Software included with the Crypto Accelerator board implements the PKCS#11 interface used by the Secure Sockets Layer (SSL) library in the iPlanet™ 4.x servers. Libraries are also provided to support the Netscape™ 3.6 Enterprise Server.

Note – The Crypto Accelerator board Public Key product falls under the authority of U.S. export controls policy and requires an export license.

Installation Requirements

The Crypto Accelerator board uses an industry standard PCI bus interface. It supports the Solaris 2.6, 7, and 8 operating environments. It can be installed in any of the following UNIX systems that have an empty PCI bus slot:

- Sun Enterprise™ 250
- Sun Enterprise 450
- Sun Enterprise 220R
- Sun Enterprise 420R
- Sun Enterprise 3000/3500
- Sun Enterprise 4000/4500

Handling the Crypto Accelerator Board

Each Crypto Accelerator 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.

Installing the Crypto Accelerator Board

Installing the Crypto Accelerator board involves inserting the board into the system and loading the software tools.

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).

To Install the Crypto Accelerator Board

1. **Shut down and power off the computer, disconnect the power cord, and remove the computer cover.**
2. **Locate an unused PCI slot.**
3. **Attach an antistatic wrist strap to your wrist, and attach the other end to a grounded metal surface.**
4. **Holding the Crypto Accelerator board by its edges only, take it out of the plastic bag and insert it into the PCI slot, and then secure the screw on the rear bracket.**
5. **Replace the computer cover, reconnect the power cord, and power on the system.**

Note – You *must* install the Crypto Accelerator board before you install the Crypto Accelerator driver software.

To Install the Software

1. **Become superuser.**
2. **Insert the** *Sun Crypto Accelerator I* **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 Volume Manager, mount the CD-ROM as follows:

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

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

File or Directory	Contents
`Copyright`	U.S. copyright file
`FR_Copyright`	French copyright file
`Packages`	Contains the Sun Crypto Accelerator I software packages: • SUNWsecsk—kernel driver • SUNWsecsm—man pages (optional) • SUNWsecsn—Web server support files • SUNWsecsu—SunVTS support files (optional)

3. **Install the software packages by typing at the command line:**

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

4. **Install the Netscape Enterprise Server 3.6 or iPlanet Web Server 4.x software.**

   The default path names for the servers are:
   NES 3.6: `/usr/netscape/suitespot`
   iPlanet 4.x: `/usr/netscape/server4`

   Accept the default path during the Netscape server installation. If you decide to install it in a different location, be sure to note where you installed it.

   Once the installation is complete, the Administration server for the web server you installed in Step 4 is displayed. See the appropriate procedure for your web server:

   - "To Enable the Board for Netscape 3.6 Enterprise Server" on page 4
   - "To Enable the Board for iPlanet Web Server 4.x" on page 8

▼ To Enable the Board for Netscape 3.6 Enterprise Server

1. **Create the actual server process by selecting the Create New Netscape Enterprise Server 3.63 link.**

2. **To accept the defaults on the server installation screen, click the OK button.**

   You can also change the defaults, then click the OK button.

3. **Select the Return to Server Administration link.**

4. **As superuser, execute the following script to enable the Crypto Accelerator board:**

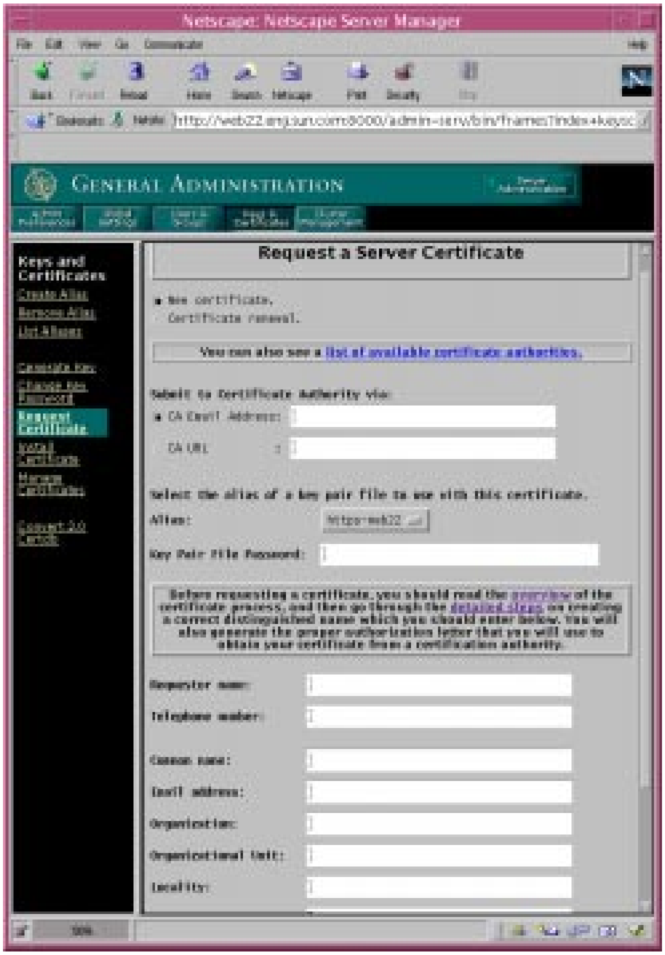
   ```
   # /opt/SUNWconn/sunsecure/bin/NSconfig
   ```

   This script prompts you for the location of the Netscape 3.6 server as well as the specific server instance to configure. It then updates the configuration files to enable the Sun Crypto Accelerator board.

5. **Generate the server certificate. In the Netscape Administration server, click the Keys & Certificates tab near the top of the page.**

   If this is a new installation and you have not created a security database, select the **Generate Key** link on the left side of the page. Click the Help button. Follow the instructions for “Generating a key-pair file on Unix platforms.”

6. **Select the Request Certificate link on the left side of the page.**



Netscape: Netscape Server Manager
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Netsite: http://web22.eng.sun.com:8000/admin-serv/bin/framesTindex+keys
General Administration
Keys and Certificates
Create Alias
Remove Alias
List Aliases
Generate Key
Change Key Password
Request Certificate
Install Certificate
Manage Certificates
Convert 2.0 Certs

Request a Server Certificate

● New certificate.
Certificate renewal.

You can also see a list of available certificate authorities.

Submit to Certificate Authority via:
● CA Email Address:
CA URL :

Select the alias of a key pair file to use with this certificate.
Alias: https-web22
Key Pair File Password:

Before requesting a certificate, you should read the overview of the certificate process, and then go through the detailed steps on creating a correct distinguished name which you should enter below. You will also generate the proper authorization letter that you will use to obtain your certificate from a certification authority.

Requestor name:
Telephone number:
Common name:
Email address:
Organization:
Organizational Unit:
Locality:

7. **Fill in the form and request a Certificate Security Request (CSR).**
   - In the Cryptographic Module field, select the `ISG 2.0 Cryptoki Interface`.
   - Common name is the hostname of your web server.
   - State or Province must be spelled out on this form.
   - Country must be abbreviated.

8. **Copy the certificate request, including the headers.**

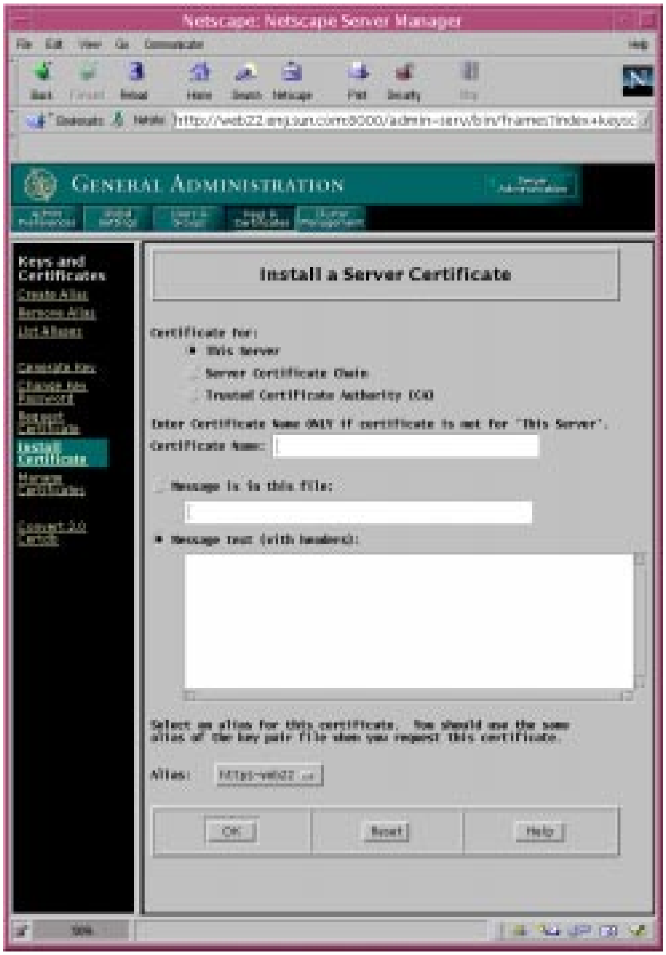
   You will paste this in the next step to generate the certificate.

9. **Use a Certificate Authority to generate the certificate, pasting in the certificate request you copied in Step 8.**

10. **Copy the certificate generated by the Certificate Authority.**

    You will paste this in when you install the certificate.

11. **Select the Install Certificate link on the left side of the page.**



http://web22.eng.sun.com:8000/admin-serv/bin/frame?index+keys

Install a Server Certificate

Certificate for:

● This Server

○ Server Certificate Chain

○ Trusted Certificate Authority (CA)

Enter Certificate Name ONLY if certificate is not for "This Server".

Certificate Name:

○ Message is in this file:

● Message text (with headers):

Select an alias for this certificate. You should use the same alias of the key pair file when you request this certificate.

Alias: https-web22

12. **Fill in the form to install your certificate, pasting the certificate you copied from the Certificate Authority into the Message box.**

13. **Restart the Netscape server process by clicking the On button and then the** *Servername* **button in the Administration server.**

14. **In the Server Preferences panel of the server on which you want to enable encryption, select the Encryption On/Off link. Turn encryption on.**

15. **Click the Save & Apply button. Type the key-pair file password generated in Step 5 “Generating a key-pair file on Unix platforms.”**

16. **For encryption to take effect, restart the Netscape server process again using the On/Off link near the top of the Server Preferences panel.**

17. **Type the key-pair file password again at the prompt, then click the Server On button.**

18. **Select the Access *servername* as a Client link.**

    When the Crypto Accelerator board is installed, the cryptographic functions are automatically performed by the board.

▼ To Enable the Board for iPlanet Web Server 4.x

1. **Run the** `setuser` **program to initialize the Crypto Accelerator key and certificate database and to set the security officer and user passwords.**

```
# /opt/SUNWconn/sunsecure/bin/setuser

Enter Security Officer (SO) password (4 to 128 characters): sopassword
Re-type Security Officer (SO) password (4 to 128 characters): sopassword
Enter User password (4 to 128 characters): userpassword
Re-type User password (4 to 128 characters): userpassword
```

sopassword is the security officer password. The security officer is the administrator of the Crypto Accelerator board. The security officer password is normally required to modify any board parameters. However, the iPlanet Web Server 4.x software does not have any functionality in its administration interface that does this.

userpassword is the password used to control access to the Crypto Accelerator board. For the iPlanet Web Server 4.x software, this password must be supplied to the web server when it is started and whenever new certificates are added to the web server.

Note – If you are using iPlanet 4.0 software, set the *userpassword* to be the same as the password for the web server’s internal key and certificate database. Because the web server only prompts for a single password at startup, its internal database password and the *userpassword* specified when you run `setuser` *must* be the same.

Caution – Run the `setuser` program only once at the beginning of the installation. If you run this program a second time you will reinitialize the database and lose any keys or certificates you have loaded.

---

2. **Start the iPlanet Administration server:**

```
# /usr/netscape/server4/startconsole
```

3. **In the iPlanet Administration server, click the Security tab near the top of the page.**

   The Create Trust Database window is displayed. If you have not previously created a trust database for the iPlanet Administration server, do so now. Later you will create a different trust database for the web server.

4. **To create the trust database, enter a password for the trust database and click OK.**

   Choose a password of at least eight characters.

5. **As superuser, execute the following script to enable the Crypto Accelerator board:**

```
# /opt/SUNWconn/sunsecure/bin/NSconfig
```

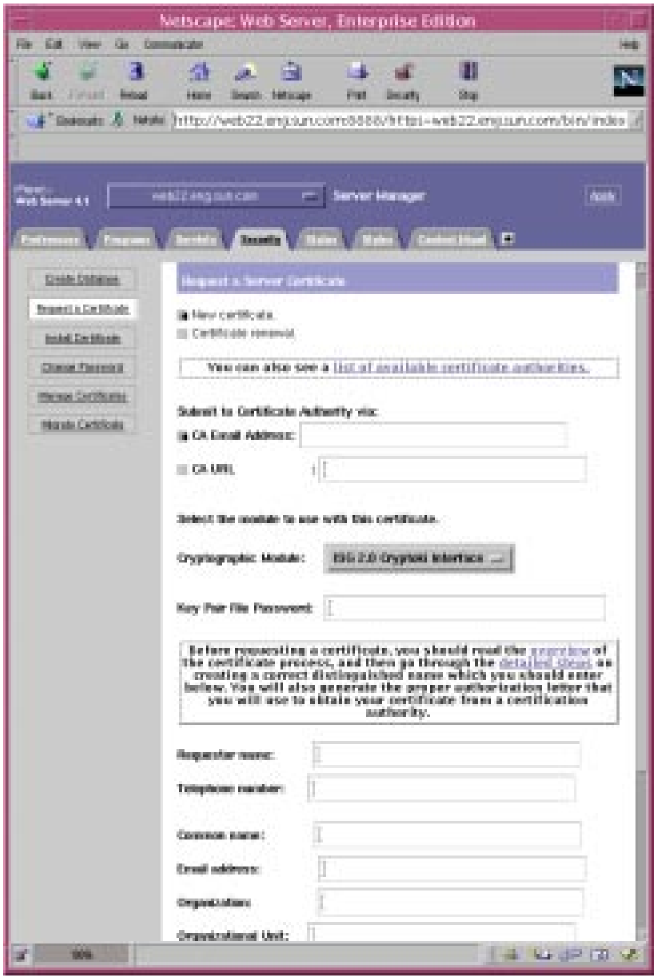
   This script prompts you for the location of the iPlanet 4.x server software. It then updates the configuration files to enable the Crypto Accelerator board.

6. **From the iPlanet Administration server, click the Servers tab near the top of the page. Select a server and click the Manage button.**

7. **To generate the server certificate, click the Security tab near the top of this page.**

   The Create Trust Database window is displayed. If you have not previously created a trust database for the *web server*, do so now. The trust database for the web server is different from that created earlier for the iPlanet Administration server.

8. Select the Request Certificate link on the left side of the page.



Netscape: Web Server, Enterprise Edition

http://web22.eng.sun.com:8888/https-web22.eng.sun.com/bin/index

web22.eng.sun.com

Server Manager

Request a Server Certificate

● New certificate

○ Certificate renewal

You can also see a list of available certificate authorities.

Submit to Certificate Authority via:

● CA Email Address:

○ CA URL

Select the module to use with this certificate.

Cryptographic Module: ISG 2.0 Cryptoki Interface

Key Pair File Password:

Before requesting a certificate, you should read the overview of the certificate process, and then go through the detailed steps on creating a correct distinguished name which you should enter below. You will also generate the proper authorization letter that you will use to obtain your certificate from a certification authority.

Requestor name:

Telephone number:

Common name:

Email address:

Organization:

Organizational Unit:

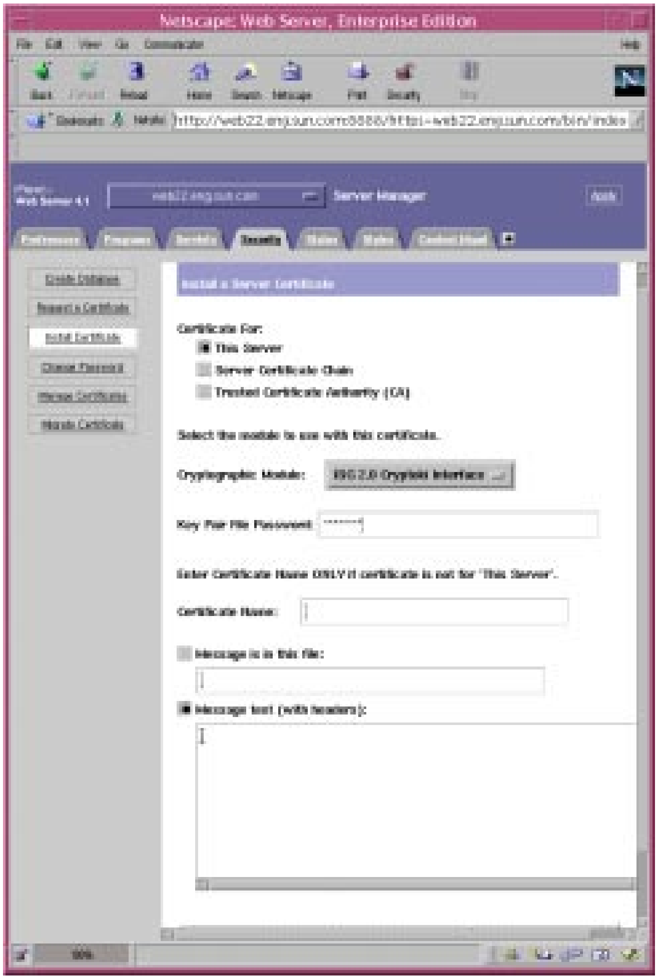
9. Fill out the form to generate a CSR, using the following information:

- In the Cryptographic Module field, select the `ISG 2.0 Cryptoki Interface`.
- Common name is the hostname of your web server.
- State or Province must be spelled out on this form.
- Country must be abbreviated.

10. Use the Certificate Authority to generate the certificate.

11. Copy the certificate generated by the Certificate Authority.

12. **Select the Install Certificate link on the left side of the page.**



Install a Server Certificate

Certificate For:
- ● This Server
- ○ Server Certificate Chain
- ○ Trusted Certificate Authority (CA)

Select the module to use with this certificate.

Cryptographic Module: ISG 2.0 Cryptoki Interface

Key Pair File Password: *******

Enter Certificate Name ONLY if certificate is not for 'This Server'.

Certificate Name:

○ Message is in this file:

● Message text (with headers):

13. **Fill out the form to install your certificate, pasting the certificate you copied from the Certificate Authority into the Message box.**

14. **Edit the** `/usr/netscape/server4/https-`*hostname*`/config/magnus.conf` **file by adding the following line:**

```
CERTDefaultNickname ISG 2.0 Cryptoki Interface:Server-Cert
```

where *hostname* is the name of the web server.

By default, the certificate you generated in Step 7 through Step 13 is named Server-Cert. If for some reason your certificate has a different name, substitute the name of the certificate for Server-Cert.

When the Crypto Accelerator board is installed, the cryptographic functions are automatically performed by the board.

15. **If you plan to use SSL for administration of server traffic, you must also edit the** `/usr/netscape/server4/https-admserv/config/magnus.conf` **file by adding the following line:**

```
CERTDefaultNickname ISG 2.0 Cryptoki Interface:Server-Cert
```

16. **Click the Apply button in the top right corner of the page.**

This loads the latest manual changes made in Step 14 and Step 15.

17. **Click the Preferences tab near the top of the page. Select the Encryption On/Off link on the left side of the page. Set encryption to On.**

18. **Shut down the Administration server. Click the Preferences tab at the top of the page, then click the Shut down the Administration server! button.**

19. **Restart the Administration server:**

```
# /usr/netscape/server4/https-admserv/start
```

20. **On the web server page, select the On/Off link on the left side of the page. Enter the passwords for the module internal software and the** `ISG 2.0 Cryptoki Interface` **module. The password for the** `ISG 2.0 Cryptoki Interface` **module is the user password set in Step 1 in this procedure.**

21. **Click the Server On button to turn on the server.**

This turns on the actual server, not the Administration server.

22. **Test your new SSL server with a browser by going to the URL** `https://`*servername:server_port*`/`.

    The default port for secure sites is 443.

    When the Crypto Accelerator board is installed, the cryptographic functions are automatically performed by the board.

To Enable the Board for Other iPlanet Products

The PKCS#11 module supplied with the Crypto Accelerator board accelerates the Diffie Hellman, RSA, and DSA operations. It also implements a key and certificate database. You can enable the Crypto Accelerator board for these products by using this procedure.

1. **Be sure to initialize any default software key and certificate databases using the administrative GUI for the product.**

2. **Run the** `setuser` **program to initialize the Crypto Accelerator key and certificate database and to set the security officer and user passwords:**

```
# /opt/SUNWconn/sunsecure/bin/setuser

Enter Security Officer (SO) password (4 to 128 characters):
Re-type Security Officer (SO) password (4 to 128 characters):
Enter User password (4 to 128 characters):
Re-type User password (4 to 128 characters):
```

3. **Follow the product's administrative documentation instructions to install a PKCS#11 module. The PCKS#11 jar file for the Crypto Accelerator board is located in the**`/opt/SUNWconn/sunsecure/lib/cryptoki.jar` **file.**

    The name of the Crypto Accelerator board PKCS#11 module is `ISG 2.0 Cryptoki Interface.`

4. **Generate certificates as required. The password for the PKCS#11 module will be the user password set in Step 2.**

    Some products require that you manually edit a configuration file to set the default certificate. Refer to the iPlanet product documentation for more information.

▼ To Remove the Software

1. **Become superuser.**
2. **Remove the Crypto Accelerator driver software:**

```
# pkgrm SUNWsecsm SUNWsecsu SUNWsecsn SUNWsecsk
```

Diagnostics and Maintenance

The status LED and SunVTS diagnostic software provide diagnostic and maintenance tools for the Crypto Accelerator board.

Status LED

The LED on the Crypto Accelerator board indicates the status of the board.

LED Condition	Status
Green	Ready (after firmware is loaded)
Red	Error
Amber	Ongoing math operations

SunVTS Diagnostic Software

Use SunVTS to run `cstest`, which verifies the Crypto Accelerator board functionality.

Note – Version 2.6 of the Solaris operating environment does not include `cstest` functionality. `cstest` also requires SunVTS version 3.0 or a subsequent compatible release.

To use the cstest, you must have the SunVTS software 3.0 or a subsequent compatible release installed on your system. Your system must be running the Solaris 2.7 or Solaris 8 operating environment. Refer to the *Solaris Sun Hardware Platform Guide* for SunVTS installation instructions.

Refer to the SunVTS documentation (listed in TABLE 1) for instructions on how to run and monitor these diagnostic tests. These documents are available on the *Solaris on Sun Hardware AnswerBook*, which is provided on the Solaris Supplement CD for the Solaris release on your system.

TABLE 1 SunVTS Documentation

Title	Description
SunVTS User's Guide	Describes the SunVTS environment
SunVTS Test Reference Manual	Describes each SunVTS test; provides various test options and command-line arguments
SunVTS Quick Reference	Provides an overview of the user interface

▼ To Run cstest

1. **Start SunVTS:**

```
# sunvts
```

2. **Disable all tests by clearing their check boxes except "Other Devices." Then expand "Other Devices."**

   If you see the cstest displayed, then go to Step 4.

3. **If the cstest is not displayed, probe the system to find it. Refer to the SunVTS documentation for the exact procedure, which will depend on your interface.**

   When the probe completes, the cstest is displayed. Clear check boxes for the other tests listed under "Other Devices." (See Error Messages for errors that can occur during this process.)

4. **Click the pop-up Option menu, then click Text Execution.**

   The settings dialog is displayed.

5. **Set the options, such as number of passes, number of instances, and so on.**

   Refer to the SunVTS documentation for more information.

6. **Click Apply, and you will be returned to the SunVTS interface.**

7. **Click Start/Stop to run or stop the test. While the `cstest` is running, the results display in the Test Messages window.**

The `cstest` Display

The `cstest` output appears in the Test Messages window of SunVTS. You will see something similar to the following:

```
API Version: 5.2.2
                   Driver Version: 2.1.3
                     Accelerators: 1
                   Command Bitmap: 7f000000
              Interrupts Serviced: 68
              Interrupts Received: 68
               Requests Attempted: 66
               Requests Completed: 66
         Maximum Pending Requests: 1
         Current Pending Requests: 0

               Accelerator #: 0
                   Last Test: 0
            Self Test Bitmap: 00000000
              Command Bitmap: 7f000000
            Hardware Version: 108e:61.14.7
            Firmware Version: 2.2.1
                   Signature: 907e97d6
         Interrupts Serviced: 36
         Interrupts Received: 36
            Requests Attempted: 35
            Requests Completed: 35
                     Idle Time: 0
                          Name: Sun Crypto Accelerator
                  BIOS Version: 0.0.0
```

Crypto Accelerator Driver Information

The first section of the display contains information on the Crypto Accelerator driver:

TABLE 2 Crypto Accelerator Driver Information

Item	Description
API Version	Version of the Application Programming Interface software loaded
Driver Version	Version of the Crypto Accelerator driver currently loaded
Accelerators	Number of Crypto Accelerator boards detected
Command Bitmap	A bit-mask value indicating which command types are supported by the current Crypto Accelerator hardware/firmware. This is defined by the firmware and is not user selectable.
Interrupts Serviced	Number of interrupts serviced by the board since the driver was started
Interrupts Received	Number of interrupts received by the board since the driver was started
Requests Attempted	Number of operation requests completed since the driver was started
Maximum Pending Size	Maximum number of commands that can be queued
Current Pending Size	Number of commands currently in the queue

Crypto Accelerator Board Information

The next sections of the display contain information on specific Crypto Accelerator boards detected:

TABLE 3 Crypto Accelerator Board Information

Item	Description
Accelerator #	The number of the Crypto Accelerator board based on the order in which the board was detected. The first board detected is Accelerator #0.
Last Test	Status of the last request. This value may be 0 for success or a non-zero number if an error occurred. For information on errors returned, see TABLE 4 for details
Self Test Bitmap	A bit-mask value returned by the diagnostic test. This value is the sum of all error codes returned. See TABLE 4.
Command Bitmap	A bit-mask value indicating which command types are supported by the current Crypto Accelerator hardware/firmware. This is defined by the firmware and is not user selectable.
Hardware Version	Version of the Crypto Accelerator board
Firmware Version	Version of the firmware currently loaded on the board.
Signature	Reserved for future use.
Interrupts Serviced	Number of interrupts serviced by the board during the period since the driver was started.
Interrupts Received	Number of interrupts received by the board during the period since the driver was started.
Requests Attempted	Number of operation requests attempted during the period since the driver was started.
Requests Completed	Number of operation requests completed since the driver was started.
Idle Time	Amount of time the board was not in use.
Name	Name and version assigned to the board.
BIOS Version	Version of the BIOS on the Crypto Accelerator board

Error Codes

The hexadecimal codes shown in TABLE 4 are returned by the diagnostic test in the Self Test Bitmap field. A zero indicates no error occurred. If more than one error occurred, the value returned is the sum of the appropriate error codes. For example, an error of 3F indicates that error 20, 10, 8, 4, 2, and 1 occurred. Each code displayed reflects only one possible combination of errors.

TABLE 4 Error Codes

Code	Description
0x00000000	No error
0x00000001	Exponentiator 1 RAM failure
0x00000002	Exponentiator 2 RAM failure
0x00000004	Multiply and carry test on Exponentiator 1 failed
0x00000008	Multiply and carry test on Exponentiator 2 failed
0x00000010	Exponentiator interrupt disable test failed
0x00000020	Randomizer test 1 failed
0x00000040	Randomizer test 2 failed
0x00000080	Exponentiation on Exponentiator 1 failed
0x00000100	Exponentiation on Exponentiator 2 failed
0x00000200	RSA test failed
0x00000400	DSA test failed
0x00000800	PCI Master test failed
0x00001000	PCI Slave test failed
0x00002000	Interrupt Enable Register test failed
0x00004000	External Control Register test failed
0x00008000	System call exception test failed
0x00010000	RAM test failed
0x00020000	Flash firmware test failed
0x00040000	Firmware RAM cache failed

Error Messages

The diagnostic test reports any errors detected as error codes in the Self Test Bitmap field of the program output. (See TABLE 4 for details.)

Error messages can also be displayed when you are setting up to run the test as you probe for the `cstest`.

If the Crypto Accelerator device driver is not found, you will see the message “Error to find the device cspci.” Install the driver software.

If the Crypto Accelerator device driver is found, but cannot be opened, you will see the message “Error to open the device cspci.” In this case, remove all Crypto Accelerator device driver software packages, following the instructions in “To Remove the Software” on page 14. Then re-install the software.