Sun™ Crypto Accelerator 4000 板 1.1 版安装和用户指南

Sun Microsystems, Inc.
www.sun.com

部件号 817-5927-10
2004 年 1 月，修订版 A

请将有关本文档的意见提交至：http://www.sun.com/hwdocs/feedback

请回收

Adobe PostScript

Declaration of Conformity (Fiber MMF)

Compliance Model Number: Venus-FI
Product Family Name: Sun Crypto Accelerator 4000 - Fiber (X4012A)

EMC

USA - FCC Class B

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

1) This equipment may not cause harmful interference.

2) This equipment must accept any interference that may cause undesired operation.

European Union

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

As Telecommunication Network Equipment (TNE) in both Telecom Centers and Other Than Telecom Centers per (as applicable):

EN300-386 V.1.3.1 (09-2001) Required Limits:

EN55022/CISPR22	Class B
EN61000-3-2	Pass
EN61000-3-3	Pass
EN61000-4-2	6 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m 80-1000MHz, 10 V/m 800-960 MHz and 1400-2000 MHz
EN61000-4-4	1 kV AC and DC Power Lines, 0.5 kV Signal Lines,
EN61000-4-5	2 kV AC Line-Gnd, 1 kV AC Line-Line and Outdoor Signal Lines, 0.5 kV Indoor Signal Lines > 10m.
EN61000-4-6	3 V
EN61000-4-11	Pass

As information Technology Equipment (ITE) Class B per (as applicable):

EN55022:1998/CISPR22:1997	Class B

EN55024:1998 Required Limits:

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 60950:2000, 3rd Edition
Evaluated to all CB Countries
UL 60950, 3rd Edition, CSA C22.2 No. 60950-00

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.
4150 Network Circle, MPK15-102
Santa Clara, CA 95054, USA
Tel: 650-786-3255
Fax: 650-786-3723

/S/

Pamela J Dullaghan
Quality Program Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: +44 1 506 672 395
Fax: +44 1 506 672 855

Declaration of Conformity (Copper UTP)

Compliance Model Number: Venus-CU
Product Family Name: Sun Crypto Accelerator 4000 - Copper (X4011A)

EMC

USA - FCC Class B

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

1) This equipment may not cause harmful interference.

2) This equipment must accept any interference that may cause undesired operation.

European Union

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

As Telecommunication Network Equipment (TNE) in both Telecom Centers and Other Than Telecom Centers per (as applicable):

EN300-386 V.1.3.1 (09-2001) Required Limits:

EN55022/CISPR22	Class B
EN61000-3-2	Pass
EN61000-3-3	Pass

EN61000-4-2	6 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m 80-1000MHz, 10 V/m 800-960 MHz and 1400-2000 MHz
EN61000-4-4	1 kV AC and DC Power Lines, 0.5 kV Signal Lines,
EN61000-4-5	2 kV AC Line-Gnd, 1 kV AC Line-Line and Outdoor Signal Lines, 0.5 kV Indoor Signal Lines > 10m.
EN61000-4-6	3 V
EN61000-4-11	Pass

As information Technology Equipment (ITE) Class B per (as applicable):

EN55022:1998/CISPR22:1997	Class B
EN55024:1998 Required Limits:	
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 60950:2000, 3rd Edition

Evaluated to all CB Countries

UL 60950, 3rd Edition, CSA C22.2 No. 60950-00

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.
4150 Network Circle, MPK15-102
Santa Clara, CA 95054, USA
Tel: 650-786-3255
Fax: 650-786-3723

/S/

Pamela J Dullaghan
Quality Program Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: +44 1 506 672 395
Fax: +44 1 506 672 855

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。

目录

表

序言

本 《*Sun Crypto Accelerator 4000 板 1.1 版安装和用户指南*》介绍了 Sun Crypto Accelerator 4000 板的功能、协议和接口，并说明如何在系统中安装、配置和管理 Sun Crypto Accelerator 4000 板。

本书假定您是一位对下列一项或多项具有丰富配置经验的网络管理员：Solaris 操作环境、带 PCI I/O 卡的 Sun 平台、Sun ONE 和 Apache Web Server、IPsec、SunVTS™ 软件以及获取认证机构证书。

内容编排

本书包括以下内容：

- 第 1 章介绍 Sun Crypto Accelerator 4000 板的产品功能、协议和接口，并说明了板的硬件和软件要求。
- 第 2 章说明如何安装和删除 Sun Crypto Accelerator 4000 的硬件及软件。
- 第 3 章定义 Sun Crypto Accelerator 4000 的可调驱动程序参数，并说明如何使用 `ndd` 实用程序和 `vca.conf` 文件配置这些参数。另外，本章还说明了如何通过 OpenBoot™ PROM 界面为链接参数启用自动协商模式或强制模式，以及如何配置网络 `hosts` 文件。
- 第 4 章介绍如何配置 Sun Crypto Accelerator 4000 板以及使用 `vcaadm` 和 `vcadiag` 实用程序管理密钥库。
- 第 5 章说明如何配置 Sun Crypto Accelerator 4000 板以便与 Sun ONE Web Server 配合使用。
- 第 6 章介绍如何配置 Sun Crypto Accelerator 4000 板以便与 Apache Web Server 配合使用。

- 第 7 章介绍如何使用 SunVTS 诊断应用程序和板载 FCode 自测程序来测试 Sun Crypto Accelerator 4000 板。另外，本章还提供了使用 OpenBoot 命令进行排除故障的技巧。
- 第 8 章介绍如何采用不同的方法配置板以与 PKCS#11 界面配合工作。
- 附录 A 列出了 Sun Crypto Accelerator 4000 板的规格。
- 附录 B 介绍如何在不使用安装脚本的情况下手动安装 Sun Crypto Accelerator 4000 软件。
- 附录 C 列出了使用 Sun Crypto Accelerator 4000 软件为 Apache Web Server 配置 SSL 支持的指令。
- 附录 D 介绍 Sun Crypto Accelerator 4000 板随附的软件，并说明了如何构建 OpenSSL 兼容应用程序以便充分利用板的加密加速功能。
- 附录 E 提供了一些来自其它软件组织的软件声明和许可，用于管理与 Sun Crypto Accelerator 4000 板一起使用的第三方软件。
- 附录 F 说明 Sun Crypto Accelerator 4000 的命令并列出了每个命令的手册页。
- 附录 G 介绍如何将 Sun Crypto Accelerator 4000 板零置为出厂状态，即板的 Failsafe 模式。

使用 UNIX 命令

本文档没有介绍基本 UNIX® 命令和操作过程的有关信息，如关闭系统、启动系统和配置设备等。

有关此类信息的详细情况，请参阅下列文档：

- *Solaris 硬件平台指南*
- `http://docs.sun.com` 网站上提供的关于 Solaris 操作环境的联机文档
- 系统随附的其它软件文档

Shell 提示符

Shell	提示符
C shell	*计算机名* %
C shell 超级用户	*计算机名* #
Bourne shell 和 Korn shell	$
Bourne shell 和 Korn shell 超级用户	#

印刷约定

字样	含义	示例
AaBbCc123	命令、文件和目录的名称；计算机的屏幕输出	编辑 .login 文件。 使用 ls -a 列出所有文件。 % You have mail.
AaBbCc123	键入的内容 （相对于计算机的屏幕输出）	% **su** Password:
AaBbCc123	书的标题、新词或术语、需要强调的词	阅读*用户指南*的第 6 章。 这些称为 *class* 选项。 执行该操作时，您*必须*为超级用户。
	命令行变量；需用真名或实际值替换	若要删除文件，请键入 rm *文件名*。

在线访问 Sun 文档

用户可从以下网站查看、打印或订购 Sun 提供的各类文档，包括本地化版本：

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

联系 Sun 技术支持人员

如果遇到本文档不能解决的产品技术问题，请访问以下网址：

`http://www.sun.com/service/contacting`

Sun 欢迎您提出意见

Sun 十分注重改进自身文档的质量，并欢迎您提出宝贵的意见和建议。您可访问以下网站来提交您的意见：

`http://www.sun.com/hwdocs/feedback`

请在反馈意见中注明本文档的标题和部件号：

Sun Crypto Accelerator 4000 板 1.1 版安装和用户指南，部件号 817-5927-10

第 1 章

产品概述

本章简要介绍 Sun Crypto Accelerator 4000 板的有关信息，包括以下几节：

产品功能

Sun Crypto Accelerator 4000 板是一种基于千兆位以太网的网络接口卡，可为 Sun 服务器上运行的 IPsec 和 SSL （对称和非对称均可）提供加密硬件加速功能。除作为标准千兆位以太网接口卡进行非加密型网络通信之外，该板附带的加密硬件还可以为加密型 IPsec 通信提供高于标准软件方案的吞吐量。

安装后，可用 `vcaadm` 实用程序对该板进行初始化和配置。此实用程序可以管理密钥库和用户信息并确定该板操作的安全等级。配置密钥库和安全主管帐户后，即可使用 `iplsslcfg` 和 `apsslcfg` 脚本配置 Sun ONE Web Server、 Sun ONE Application Server 或 Apache Web Server，以便它们将板用于 SSL 加速。通过使用 Sun ONE 管理控制台和 `modutil` 以及 `certutil` 实用程序配置 Sun ONE Directory Server、Messaging Server 以及 Portal Server，它们也可将板用于 SSL 加速。此外，大多数需用 PKCS#11 界面来获取密钥库和加密服务的应用程序均可使用该板。

主要协议和接口

Sun Crypto Accelerator 4000 板可与现有的以太网设备相互配合操作，前提是这些设备采用标准以太网最小和最大帧大小 （64 至 1518 字节）和帧格式，且与以下标准和协议兼容：

- 全长 PCI 33/66 Mhz， 32/64 位
- IEEE 802.3 CSMA/CD （以太网）
- IEEE 802.2 逻辑链路控制
- SNMP （仅限 MIB）
- 全双工和半双工千兆位以太网接口 (IEEE 802.z)
- 通用双压信号 （3.3V 和 5V）

主要功能

- 带铜或光纤接口的千兆位以太网
- 加速 IPsec 和 SSL 加密功能
- 会话建立速率：高达 4300 次/秒
- 批量加密速率：高达 800 Mbps
- 提供多达 2048 位的 RSA 加密方法
- 加密速度比 3DES 批量数据加密快达 10 倍
- 可为 Sun ONE Web Server 提供能防篡改的集中化安全密钥和证书管理策略，从而实现更高的安全性能和简化的密钥管理
- 符合 FIPS 140-2 Level 3 认证
- 较低的 CPU 利用率 — 释放服务器系统资源和带宽
- 安全可靠的私钥存储和管理
- 在中型和高端服务器上支持动态重配置 (DR) 和冗余/故障接管功能
- 在多个 CPU 之间实现 RX 数据包负载均衡
- 支持全流量控制 (IEEE 802.3x)

Sun Crypto Accelerator 4000 板符合联邦信息处理标准 (FIPS) 140-2 级别 3 中有关加密模块的安全性能要求。

支持的应用程序

- Solaris 8 和 9 操作环境 (IPsec VPN)
- Sun ONE Web Server 4.1 和 6.0
- Sun ONE Application Server 7.0
- Sun ONE Directory Server 5.2
- Sun ONE Messaging Server 5.2
- Sun ONE Portal Server 6.2
- Apache Web Server 1.3.x 和 2.x

支持的加密协议

Sun Crypto Accelerator 4000 板支持以下协议：

- IPsec for IPv4 和 IPsec for IPv6，包括 IKE
- SSLv2、 SSLv3、 TLSv1 （传输层安全性）

Sun Crypto Accelerator 4000 板可加速以下 IPsec 功能：

- ESP （DES 和 3DES）加密
- ESP （SHA1、 MD5）验证 *
- AH （SHA1、 MD5）验证 *

* 当配置用于线内 IPsec 加速时 （参阅第 5 页 “线内 IPsec 硬件加速”）

Sun Crypto Accelerator 4000 板可加速以下 SSL 功能：

- 在客户机和服务器之间安全建立一套加密参数和密钥
- 板上配有安全可靠的密钥库 — 密钥一旦离开板便会加密

诊断支持

- 用户可通过 OpenBoot PROM 执行自测程序
- SunVTS 诊断测试

加密算法加速

该板既可加速硬件中的加密算法，也可加速软件中的加密算法。其复杂性的原因在于加速加密算法的开销对于各种算法并非完全一样。有些加密算法只能通过硬件来实现，而其它一些加密算法则只能通过软件来实现。对于硬件加速而言，数据从用户应用程序移到硬件加速设备中以及将结果移回用户应用程序中均会增加开销。注意：一些加密算法可以由精心调试的软件执行，其速度与在专用硬件中一样。

支持的加密算法

Sun Crypto Accelerator 4000 驱动程序 (vca) 检查每一个加密请求并确定最佳的加密位置 （主机处理器或 Sun Crypto Accelerator 4000），从而获得最大的吞吐量。负载分布取决于加密算法、当前作业量和数据大小。

Sun Crypto Accelerator 4000 板可加速以下 IPsec 算法：

表 1-1 IPsec 加密算法

类型	算法
对称	DES， 3DES
散列 *	MD5， SHA1

* 当配置用于线内 IPsec 硬件加速时。

Sun Crypto Accelerator 4000 板可加速以下 SSL 算法。

表 1-2 SSL 加密算法

类型	算法
对称	DES， 3DES， ARCFOUR
非对称	Diffie-Hellman （只适用于 Apache）和 RSA （多达 2048 位密钥），DSA
散列	MD5， SHA1

IPsec 加速

Sun Crypto Accelerator 4000 板支持两种形式的 IPsec 加速：带外和线内。这两种配置均将 SPARC® 处理器的高开销加密操作转交给 Sun Crypto Accelerator 4000 板处理。有关说明，请参阅第 49 页 “配置 IPsec 硬件加速”。

表 1-3 加速的 IPsec 算法

算法	带外	线内
DES	X	X
3DES	X	X
MD5		X
SHA1		X

带外 IPsec 硬件加速

如果板配置用于带外 IPsec 加速，且安装在 Solaris 9 （或更新版本）系统中，则受支持的加密和解密操作将在硬件中加速。所有特定于 IPsec 处理器的数据包处理过程均由主机 Solaris IPsec 软件执行。有关说明，请参阅第 50 页 “启用带外 IPsec 加速”。

注 – 在 Solaris 9 中，无需配置和调整 IPsec 即可使用板进行带外 IPsec 加速。您只需安装 Sun Crypto Accelerator 4000 软件包然后重新引导。

线内 IPsec 硬件加速

如果板配置用于线内 IPsec 加速，且安装在 Solaris 9 12/03 （或更新版本）系统中，则受支持的加密、解密和验证操作将在硬件中加速。部分特定于 IPsec 的数据包处理过程由板直接执行。有关如何配置板以进行线内 IPsec 加速的说明，请参阅第 50 页 “启用线内 IPsec 加速”。

SSL 加速

表 1-4 列出了可以向 Sun Crypto Accelerator 4000 硬件分配负载的 SSL 加速算法以及为 Sun ONE 和 Apache Web Server 提供的软件算法。

表 1-4 支持的 SSL 算法

	Sun ONE Web Server		**Apache Web Server**	
算法	**硬件**	**软件**	**硬件**	**软件**
RSA	X	X	X	X
DSA	X	X	X	X
ARCFOUR		X		X
Diffie-Hellman			X	X
DES	X	X	X	X
3DES	X	X	X	X
MD5	X	X		
SHA1	X	X		

批量加密

默认情况下，系统已禁用了 Sun Crypto Accelerator 4000 板为 Sun ONE 服务器软件提供的批量加密功能。您必须手动启用此功能，方法是：创建相关文件，然后重新启动 Sun ONE 服务器软件。

要使 Sun ONE 服务器软件可以使用板上的批量加密功能，您只需在 `/etc/opt/SUNWconn/cryptov2/` 目录中创建一个名为 `sslreg` 的空文件，然后重新启动服务器软件。

```
# touch /etc/opt/SUNWconn/cryptov2/sslreg
```

要禁用批量加密功能，您必须删除 `sslreg` 文件，然后重新启动服务器软件。

```
# rm /etc/opt/SUNWconn/cryptov2/sslreg
```

默认情况下，系统已为 Apache Web Server 软件启用了批量加密功能，且不能禁用。

硬件概述

Sun Crypto Accelerator 4000 硬件是一个全长 （4.2 英寸 × 12.283 英寸）的加密加速器 PCI 千兆位以太网适配器，用于提高 Sun 服务器上 IPsec 和 SSL 的性能。

Sun Crypto Accelerator 4000 MMF 适配器

Sun Crypto Accelerator 4000 MMF 适配器是一种单端口的基于光纤的千兆位以太网 PCI 总线卡。它只能在 1000 Mbps 以太网中使用。

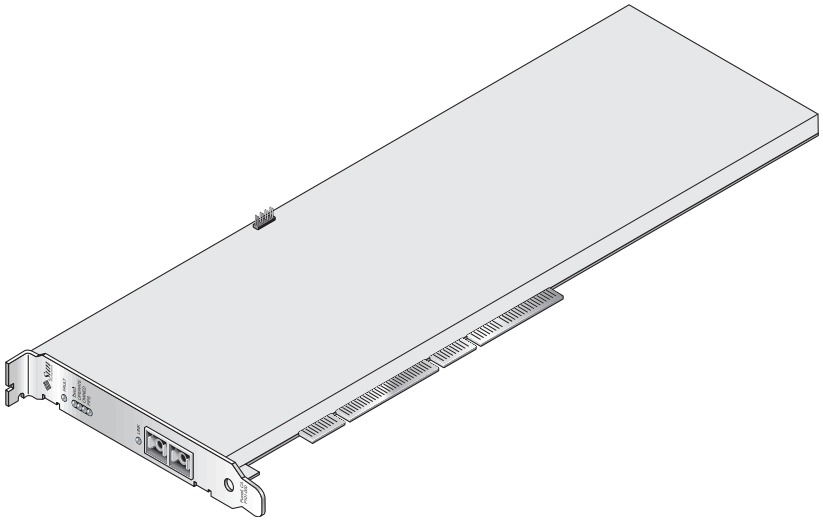

图 1-1 Sun Crypto Accelerator 4000 MMF 适配器

LED 显示

表 1-5 MMF 适配器的前面板显示 LED

标签	亮起时的含义	颜色
FAULT （故障）	当板处于 HALTED （致命错误）状态或低级硬件初始化失败时亮起。 引导期间出现错误时闪烁。	红色
DIAG （诊断）	处于 POST、 DIAGNOSTICS 和 FAILSAFE （固件未升级）状态时亮起。 运行 DIAGNOSTICS 时闪烁。	绿色
OPERATE （操作）	处于 POST、 DIAGNOSTICS 和 DISABLED （未附带驱动程序）状态时亮起。 处于 IDLE、 OPERATIONAL 和 FAILSAFE 状态时闪烁。	绿色
INIT （初始化）	安全主管已使用 `vcaadm` 初始化板时亮起。有关说明，请参阅第 62 页 “通过 `vcaadm` 初始化板”。 存在 ZEROIZE 跳线时闪烁。	绿色
FIPS	在 FIPS 140-2 level 3 认证模式下运行时亮起。在非 FIPS 模式下运行时熄灭。	绿色
LINK （链路）	打开链路时亮起。	绿色

Sun Crypto Accelerator 4000 UTP 适配器

Sun Crypto Accelerator 4000 UTP 适配器是一种单端口的基于铜线的千兆位以太网 PCI 总线卡。经过配置，它可以在 10、 100 或 1000 Mbps 以太网中使用。

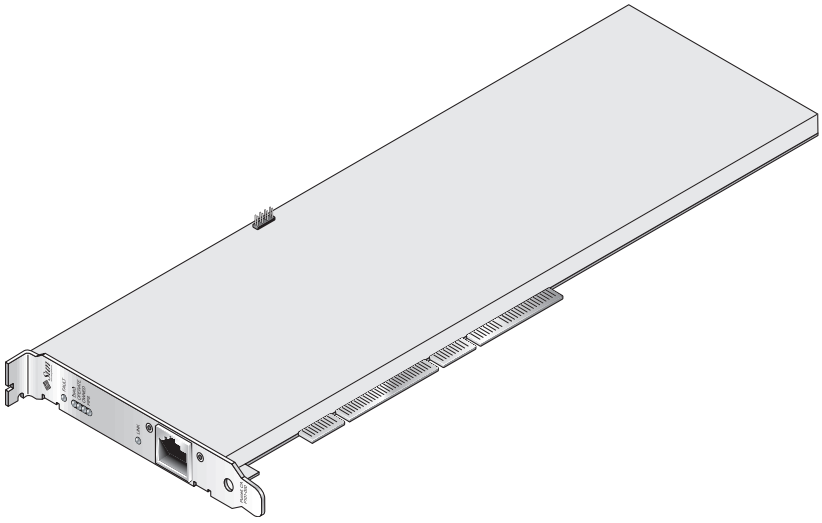

图 1-2 Sun Crypto Accelerator 4000 UTP 适配器

LED 显示

表 1-6 UTP 适配器的前面板显示 LED

标签	亮起时的含义	颜色
FAULT （故障）	当板处于 HALTED （致命错误）状态或低级硬件初始化失败时亮起。 引导期间出现错误时闪烁。	红色
DIAG （诊断）	处于 POST、 DIAGNOSTICS 和 FAILSAFE （固件未升级）状态时亮起。 运行 DIAGNOSTICS 时闪烁。	绿色
OPERATE （操作）	处于 POST、 DIAGNOSTICS 和 DISABLED （未附带驱动程序）状态时亮起。 处于 IDLE、 OPERATIONAL 和 FAILSAFE 状态时闪烁。	绿色

表 1-6 UTP 适配器的前面板显示 LED *（续）*

标签	亮起时的含义	颜色
INIT （初始化）	安全主管已使用 `vcaadm` 初始化板时亮起。有关说明，请参阅第 62 页 “通过 `vcaadm` 初始化板”。 存在 ZEROIZE 跳线时闪烁。	绿色
FIPS	在 FIPS 140-2 level 3 认证模式下运行时亮起。在非 FIPS 模式下运行时熄灭。	绿色
1000	使用千兆位以太网时亮起。	绿色
活动 （无标签）	链路发送或接收数据时亮起。	琥珀色
链路 （无标签）	打开链路时亮起。	绿色

注 – 每次述及 Sun ONE Web Server 4.1 或 6.0 时，均意指服务包号 （SP9 或 SP1）。

动态重配置和高可用性

Sun Crypto Accelerator 4000 硬件和相关软件能够高效地在那些支持动态重配置 (DR) 和热插拔的 Sun 平台上工作。在 DR 或热插拔操作中， Sun Crypto Accelerator 4000 软件层会自动检测板的插拔情况并调节计划算法，以适应硬件资源的变化。

对于高可用性 (HA) 配置，可以在系统或域中安装多块 Sun Crypto Accelerator 4000 板，以确保硬件加速功能连续可用。当 Sun Crypto Accelerator 4000 硬件出现故障时（机率很小），软件层会检测到此故障并从可用的硬件加密加速器列表中删除出现故障的板。Sun Crypto Accelerator 4000 软件会调整计划算法，以适应硬件资源减少的情况。后续的加密请求将会安排给剩余的板。

注意：Sun Crypto Accelerator 4000 硬件为生成长期密钥提供了高质量信息熵 (Entropy) 的来源。如果拆卸某域或系统中的所有 Sun Crypto Accelerator 4000 板，则会生成信息熵质量较低的长期密钥。

负载共享

Sun Crypto Accelerator 4000 软件在 Solaris 域或系统中安装的各个板上分配负载。收到的加密请求依据固定长度的作业队列分配给各个不同的板。也就是说，加密请求首先分配给第一块板，后续请求仍然分配给第一块板，直到该板满荷运行为止。一旦第一块板满荷运行，后续请求会分配给下一块可以接受此类请求的板。排队机制的作用在于疏导那些汇集在板上的请求，从而达到优化吞吐量的目的。

硬件和软件要求

表 1-7 简要列出了 Sun Crypto Accelerator 4000 适配器的硬件及软件要求。

表 1-7 硬件和软件要求

硬件和软件	要求
硬件	Sun Fire™ V120, V210, V240, 280R, V480, V880, 4800, 4810, 6800, 12K, 15K; Netra™ 20 (lw4); Sun Blade™ 100, 150, 1000, 2000
操作环境	Solaris 8 2/02 和以后的兼容版本 （对于 IPsec 加速，需用 Solaris 9 版本。）

必需的修补程序

有关必需修补程序的详细信息，请参阅 《*Sun Crypto Accelerator 4000 板 1.1 版发布说明*》。

要在系统上运行 Sun Crypto Accelerator 4000 板，需要安装以下修补程序。Solaris 更新版本包含以前版本的修补程序。请运行 `showrev -p` 命令来确定是否已安装了下面所列的修补程序。

您可从以下网站下载修补程序：`http://sunsolve.sun.com`。

安装最新版本的修补程序。每发布一个新版本的修补程序，破折号后的数字 （例如 -01）就会增加。如果网站上的版本高于下表中列出的版本，请使用最新的版本。

如果 SunSolve℠ 网站中未提供您所需的修补程序，请与本地销售或服务代表联系。

Apache Web Server 修补程序

如果计划将 Apache Web Server 与 Solaris 8 配合使用，则必须在安装 Sun Crypto Accelerator 4000 软件之前安装修补程序 109234-09。添加 `SUNWkcl2a` 软件包之后，系统将使用 Apache Web Server mod_ssl 1.3.26 进行配置。

Solaris 8 修补程序

表 1-8 列出了 Sun Crypto Accelerator 4000 软件必需的 Solaris 8 修补程序。

表 1-8 必需的 Solaris 8 修补程序

修补程序 ID	说明
110383-01	`libnvpair`
108528-23	`KU-05`（`nvpair` 支持）
112438-01	`/dev/random`
110900-10	`pcifg`、SunFire 15K 支持和 DR
110824-04	DR
110842-11	总线速率和 DR
110839-04	小节点和 DLPI 供应商名称
109234-09	Apache 支持

Solaris 9 修补程序

表 1-9 列出了 Sun Crypto Accelerator 4000 软件必需的 Solaris 9 修补程序。

表 1-9 必需的 Solaris 9 修补程序

修补程序 ID	说明
113068-04	总线速率、Sun Fire 15K 支持和 DR
112838-08	`pcicfg`、DR 和 Sun Fire 15K 支持
113218-08	千兆位性能和 `vca` 内存漏失
112904-08	千兆位性能
114758-01	小节点和 DLPI 供应商名称
112233-08	（只有 Solaris 9 9/04 之前的 Solaris 版本需要安装）

第 2 章

安装 Sun Crypto Accelerator 4000 板

本章介绍如何安装 Sun Crypto Accelerator 4000 硬件以及如何使用自动脚本安装和删除软件。它包括以下几节：

安装板的硬件和软件之后，您需使用配置和密钥库信息来初始化板。有关如何初始化板的信息，请参阅第 62 页 “通过 vcaadm 初始化板”。

板的处理

每块板都采用特制的防静电包进行包装，以确保安全运输和存储。为避免损坏板上的静电敏感组件，请在接触板之前，使用以下其中一种方法消除身上的静电：

- 触摸计算机的金属机箱。
- 戴上防静电腕带，并将其连接到接地的金属表面。

注意 – 为避免损坏板上的静电敏感组件，请在装卸板时戴上防静电腕带，只接触板的边缘，并且始终将板放在防静电的表面上 （如板的包装塑料袋）。

板的安装

Sun Crypto Accelerator 4000 板的安装涉及两个方面，其一是将板插入系统，其二是加载软件工具。硬件安装说明仅包括板的一般安装步骤。有关具体安装说明，请参阅系统随附的文档。

▼ 安装硬件

1. **作为超级用户，按照系统随附文档中的说明关闭系统，关闭计算机，拔掉电源线并卸下计算机外壳。**
2. **找到未用的 PCI 插槽 （最好是 64 位 66 MHz 插槽）。**
3. **将防静电腕带的一端连接到手腕，另一端连接到接地的金属表面。**
4. **使用十字头螺丝刀拧下 PCI 插槽盖板上的螺丝。**
   收好螺丝，以备在步骤 5 中固定支架时使用。
5. **只抓住 Sun Crypto Accelerator 4000 板的边缘，将其从塑料袋中取出，插入 PCI 插槽，然后拧入螺丝以固定后支架。**
6. **装回计算机外壳，接回电源线，然后打开系统电源。**
7. **在 OpenBoot PROM `ok` 提示符下，键入 `show-devs` 命令以检查板的安装是否正确：**

```
ok show-devs
.
/chosen
/packages
/upa@8,480000/SUNW,ffb@0,0
/pci@8,600000/network@1
/pci@8,600000/SUNW,qlc@4
/pci@8,600000/SUNW,qlc@4/fp@0,0
.
```

在上面的示例中，`/pci@8,600000/network@1` 表示 Sun Crypto Accelerator 4000 板的设备路径。系统中的每块板均有类似的设备路径行。

要确定是否正确列出了 Sun Crypto Accelerator 4000 的设备属性，请执行以下操作：在 ok 提示符下，切换至所需的设备路径，然后键入 .properties 命令以显示属性列表。

```
ok cd /pci@8,600000/network@1
ok .properties
assigned-addresses        82000810 00000000 00102000 00000000 00002000
                           81000814 00000000 00000400 00000000 00000100
                           82000818 00000000 00200000 00000000 00200000
                           82000830 00000000 00400000 00000000 00100000
d-fru-len                 00 00 00 00
d-fru-off                 00 00 e8 00
d-fru-dev                 eeprom
s-fru-len                 00 00 08 00
s-fru-off                 00 00 e0 00
s-fru-dev                 eeprom
compatible                70 63 69 38 30 38 36 2c 62 35 35 35 2e 31 30 38
reg                       00000800 00000000 00000000 00000000 00000000
                           02000810 00000000 00000000 00000000 00002000
                           02000814 00000000 00000000 00000000 00000100
                           02000818 00000000 00000000 00000000 00200000
                           02000830 00000000 00000000 00000000 00100000
address-bits              00 00 00 30
max-frame-size            00 00 40 00
network-interface-type    ethernet
device-type               network
name                      network
local-mac-address         00 03 ba 0e 99 ca
version                   Sun PCI Crypto Accelerator 4000 1000Base-T FCode
FCode 2.11.13 03/03/04
phy-type                  mif
board-model               501-6039
model                     SUNW,pci-vca
fcode-rom-offset          00000000
66mhz-capable
fast-back-to-back
devsel-speed              00000001
class-code                00100000
interrupts                00000001
max-latency               00000040
cache-line-size           00000010
max-latency               00000040
min-grant                 00000040
subsystem-vendor-id       0000108e
subsystem-id              00003de8
revision-id               00000002
device-id                 0000b555
vendor-id                 00008086
```

安装 Sun Crypto Accelerator 4000 软件

Sun Crypto Accelerator 4000 CD 中附带了 Sun Crypto Accelerator 4000 软件。您需要从 SunSolve 网站下载修补程序。有关详细信息，请参阅第 10 页 “必需的修补程序”。

可用两种方法安装软件：手动安装或使用 `install` 脚本安装。本节介绍如何使用 `install` 脚本来安装软件。如需手动安装软件，请参阅附录 B。

▼ 安装软件

1. **将 Sun Crypto Accelerator 4000 CD 插入与系统相连的 CD-ROM 驱动器。**
   - 如果系统正在运行 Sun Enterprise Volume Manager™，则它应自动将 CD-ROM 挂装到 `/cdrom/cdrom0` 目录。
   - 如果系统未运行 Sun Enterprise Volume Manager，请按以下方法挂装 CD-ROM：

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

`/cdrom/cdrom0` 目录中具有下列文件和目录。

表 2-1 `/cdrom/cdrom0` 目录中的文件

文件或目录	内容	
`Copyright`	美国版权文件	
`FR_Copyright`	法国版权文件	
`install`	用于安装 Sun Crypto Accelerator 4000 软件的脚本	
`remove`	用于删除 Sun Crypto Accelerator 4000 软件的脚本	
`Docs`	*Sun Crypto Accelerator 4000 板 1.1 版安装和用户指南* *Sun Crypto Accelerator 4000 板发布说明*	
`Packages`	包含以下 Sun Crypto Accelerator 4000 软件包：	
	`SUNWkcl2r`	加密核心组件
	`SUNWkcl2u`	加密管理实用程序和程序库
	`SUNWkcl2a`	用于 Apache 的 SSL 支持 *（可选）*
	`SUNWkcl2m`	加密管理手册页 *（可选）*
	`SUNWvcar`	VCA Crypto Accelerator (root)

表 2-1 /cdrom/cdrom0 目录中的文件 *（续）*

文件或目录	内容	
	SUNWvcau	VCA Crypto Accelerator (usr)
	SUNWvcaa	VCA 管理
	SUNWvcafw	VCA 固件
	SUNWvcamn	VCA Crypto Accelerator 手册页 *（可选）*
	SUNWvcav	VCA Crypto Accelerator 的 SunVTS 测试程序 *（可选）*
	SUNWkcl2o	SSL 开发工具和程序库 *（可选）*
	SUNWkcl2i.u	采用 KCLv2 Crypto 的 IPsec 加速 *（可选）*

此安装脚本以特定的顺序安装必需的软件包，并且这些软件包必须在安装任何可选软件包之前进行安装。安装必需的软件包之后，您可以按任意顺序安装和删除可选软件包。

仅在计划将 Apache 用作您的 Web 服务器时，才有必要安装可选的 SUNWkcl2a 软件包。

仅在计划重新链接到另一版本的 Apache Web Server 时，才有必要安装可选的 SUNWkcl2o 软件包。

仅在计划执行 SunVTS 测试时，才有必要安装可选的 SUNWvcav 软件包。您必须在安装 SunVTS 4.4 或最新 5.x 版本之后才能安装 SUNWvcav 软件包。

注 – Sun Crypto Accelerator 4000 CD 中的可选 SUNWkcl2i.u 软件包只有 .u 扩展名。安装该软件包之后，其名称会更改成为 SUNWkcl2i。该软件包在 CD 中采用 .u 扩展名表示此软件包专用于 sun4u 体系结构。

---

2. **键入以下命令，安装必需的软件：**

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

安装脚本会对系统进行分析，确定必需安装的修补程序，然后安装这些修补程序和主要软件，并根据需要安装可选软件。例如：

注 – 以下示例忽略了版权和许可证信息。有关版权和软件许可证，请参阅附录 E 。

```
# ./install
This program installs the software for the Sun Crypto Accelerator
4000, Version 1.1.

*** Checking if Sun Crypto Accelerator support is already installed...
*** Checking for required OS patch(es):
 113146-01 112838-07 113068-04 113449-02 113453-04 114758-01
*** Checking for incompatible OS patch(es) ...
*** Checking for optional package dependencies...

Do you wish to install the optional Crypto IPsec Acceleration software
(SUNWkcl2i.u)?  [y,n,?,q]

Do you wish to install the optional Crypto Apache Support (SSL) (SUNWkcl2a
SUNWkcl2o)?  [y,n,?,q] y

Do you wish to install the optional Crypto QA Tools (SUNWkcl2q SUNWvcaq)?
[y,n,?,q] n

Do you wish to install the optional VCA Crypto Accelerator/Gigabit Ethernet
SunVTS Diagnostics (SUNWvcav)?  [y,n,?,q] n

This script is about to take the following actions:
- Install Sun Crypto Accelerator 4000 support for Solaris 9
- Install Optional Crypto IPsec Acceleration software
- Install Optional Crypto Apache Support (SSL) software

To cancel installation of this software, press 'q' followed by a Return.
 **OR**
Press Return key to begin installation:

*** Installing Sun Crypto Accelerator 4000 software for Solaris 9...
Installing required packages:
 SUNWkcl2r SUNWkcl2u SUNWkcl2m SUNWvcar SUNWvcau SUNWvcaa SUNWvcamn SUNWvcafw
```

```
Installation of <SUNWkcl2u> was successful.
Installation of <SUNWkcl2m> was successful.
Installation of <SUNWvcar> was successful.
Installation of <SUNWvcau> was successful.
Installation of <SUNWvcaa> was successful.
Installation of <SUNWvcamn> was successful.
Installation of <SUNWvcafw> was successful.
*** Installing selected optional software for Solaris 9...
Installing optional package(s):
 SUNWkcl2i.u SUNWkcl2a SUNWkcl2o
Installation of <SUNWkcl2i> was successful.

Checking operating environment requirements...
Determining package requirements...
Verifying required packages are installed...
All required packages installed.
Determining patch requirements...
Verifying required patches are installed...
Requirement for 113146-01 met by 113146-01.
All required patches installed.

Installation of <SUNWkcl2a> was successful.

Installation of <SUNWkcl2o> was successful.
*** Installation complete.
```

安装可选的软件包

若只安装用于为 Apache Web Server 和 Sun Crypto Accelerator 4000 联机手册页提供 SSL 支持的可选软件包，请选择 `SUNWkcl2a` 和 `SUNWkcl2m`。

若要安装所有的可选软件包，请选择以下选项：`SUNWkcl2a`、`SUNWkcl2m`、`SUNWvcamn`、`SUNWvcav`、`SUNWkcl2o` 和 `SUNWkcl2i.u`。

有关上述示例中可选软件包的内容说明，请参见表 2-1。

目录和文件

表 2-2 列出了 Sun Crypto Accelerator 4000 软件在采用默认方式安装时所创建的目录。

表 2-2 Sun Crypto Accelerator 4000 目录

目录	内容
`/etc/opt/SUNWconn/vca/keydata`	密钥库数据 （已加密）
`/opt/SUNWconn/cryptov2/bin`	实用程序
`/opt/SUNWconn/cryptov2/lib`	支持程序库
`/opt/SUNWconn/cryptov2/sbin`	管理命令

图 2-1 显示了这些目录和文件的层次结构。

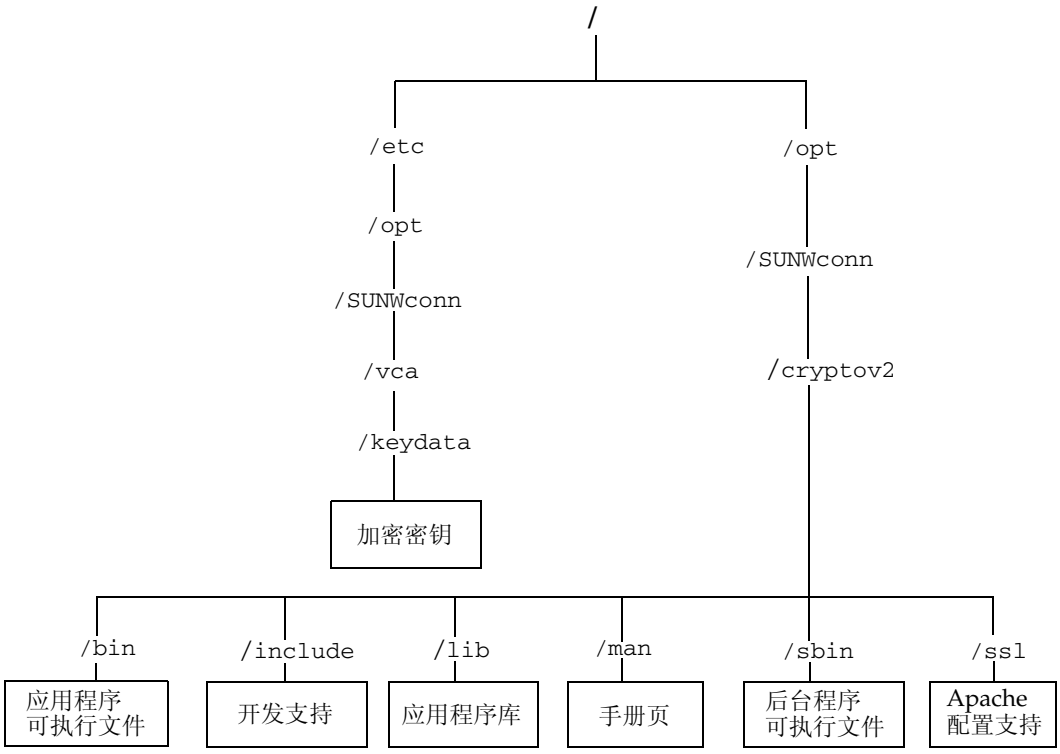

图 2-1 Sun Crypto Accelerator 4000 目录和文件

注 – 安装 Sun Crypto Accelerator 4000 硬件和软件后，需用配置和密钥库信息来初始化板。有关如何初始化板的信息，请参阅第 62 页 “通过 `vcaadm` 初始化板”。

删除 Sun Crypto Accelerator 4000 软件

可用三种方法删除软件：CD-ROM 上的 `remove` 脚本；服务器上的 `/var/tmp/crypto_acc.remove` 脚本；或 `pkgrm` 命令。本节介绍如何使用前两种方法来删除软件。有关使用 `pkgrm` 命令删除软件的说明，请参阅附录 B。

如果软件是使用 `install` 脚本安装的，则用 `remove` 脚本来删除软件。如果软件是手动安装的，则用 `/var/tmp/crypto_acc.remove` 脚本 （附录 B）。

▼ 使用 remove 脚本删除软件

- **插入 Sun Crypto Accelerator 4000 CD-ROM 并键入以下命令：**

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

▼ 使用 /var/tmp/crypto_acc.remove 脚本删除软件

您可在以下目录中找到此安装的日志：

```
/var/tmp/crypto_acc.install.2003.10.13
```

- **键入以下命令：**

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

第 3 章

配置驱动程序参数

本章介绍如何配置 Sun Crypto Accelerator 4000 UTP 和 MMF 以太网适配器所用的 vca 设备驱动程序参数。它包括以下几节：

以太网设备驱动程序 (vca) 参数

vca 设备驱动程序用于控制 Sun Crypto Accelerator 4000 UTP 和 MMF 以太网设备的操作。 vca 驱动程序连接至 Sun Crypto Accelerator 4000 的 UNIX pci 名称属性 pci108e,3de8 （其中 108e 是厂商 ID， 3de8 是 PCI 设备 ID）。

您可以手动配置 vca 设备驱动程序参数，从而自定义系统中的每一个 Sun Crypto Accelerator 4000 设备。本节简要介绍了板中所用的 Sun Crypto Accelerator 4000 以太网设备的性能，并说明了可用的 vca 设备驱动程序参数及其配置方法。

Sun Crypto Accelerator 4000 以太网 UTP 和 MMF PCI 适配器可以按第 37 页 “使用 OpenBoot PROM 为链接参数启用自动协商或强制模式”中列出的速率和模式进行操作。默认情况下， vca 设备以自动协商模式与链接的远端 （链接伙伴）一起操作，以便为 speed、 duplex 和 link-clock 参数选择共同的操作模式。只有板的操作速率为 1000 Mbps 时， link-clock 参数才适用。对于这些参数， vca 设备也可以配置为在强制模式下操作。

注意 – 要建立正常链接，链接伙伴双方的每一个 `speed`、 `duplex` 和 `link-clock`（只适用于 1000 Mbps）参数均应同时在自动协商模式或强制模式下进行操作。如果链接伙伴双方的任何一个参数未在相同的模式下进行操作，将会出现网络错误。有关说明，请参阅第 37 页 “使用 OpenBoot PROM 为链接参数启用自动协商或强制模式”。

驱动程序参数值和定义

表 3-1 列出了 `vca` 设备驱动程序的参数和设置。

表 3-1 `vca` 驱动程序参数、状态和说明

参数	状态	说明
`instance`	读和写	设备例程
`adv-autoneg-cap`	读和写	操作模式参数
`adv-1000fdx-cap`	读和写	操作模式参数 （只适用于 MMF 适配器）
`adv-1000hdx-cap`	读和写	操作模式参数
`adv-100fdx-cap`	读和写	操作模式参数 （只适用于 UTP 适配器）
`adv-100hdx-cap`	读和写	操作模式参数 （只适用于 UTP 适配器）
`adv-10fdx-cap`	读和写	操作模式参数 （只适用于 UTP 适配器）
`adv-10hdx-cap`	读和写	操作模式参数 （只适用于 UTP 适配器）
`adv-asmpause-cap`	读和写	流控制参数
`adv-pause-cap`	读和写	流控制参数
`pause-on-threshold`	读和写	流控制参数
`pause-off-threshold`	读和写	流控制参数
`link-master`	读和写	1 Gbps 速率强制模式参数
`enable-ipg0`	读和写	允许在发送数据包之前使用额外的延迟
`ipg0`	读和写	发送数据包之前的额外延迟
`ipg1`	读和写	数据包收发间隔参数
`ipg2`	读和写	数据包收发间隔参数
`rx-intr-pkts`	读和写	接收中断消隐值
`rx-intr-time`	读和写	接收中断消隐值
`red-dv4to6k`	读和写	随机提前检测和数据包丢弃矢量

表 3-1 vca 驱动程序参数、状态和说明 *（续）*

参数	状态	说明
red-dv6to8k	读和写	随机提前检测和数据包丢弃矢量
red-dv8to10k	读和写	随机提前检测和数据包丢弃矢量
red-dv10to12k	读和写	随机提前检测和数据包丢弃矢量
tx-dma-weight	读和写	PCI 接口参数
rx-dma-weight	读和写	PCI 接口参数
infinit-burst	读和写	PCI 接口参数
disable-64bit	读和写	PCI 接口参数

声明的链接参数

以下参数确定了 vca 驱动程序向其链接伙伴声明的有关发送及接收的 speed 和 duplex 链接参数。表 3-2 介绍了操作模式参数及其默认值。

注 – 如果参数的初始设置是 0，请不要更改该参数。如果尝试更改初始设置为 0 的参数，它仍恢复至 0。默认情况下，这些参数根据 vca 设备的性能进行设置。

Sun Crypto Accelerator 4000 UTP 适配器的声明链接参数不同于表 3-2 中所示的 Sun Crypto Accelerator 4000 MMF 适配器链接参数。

表 3-2 操作模式参数

参数	说明	UTP 适配器	MMF 适配器
adv-autoneg-cap	由硬件声明的本地接口性能 0 = 强制模式 1 = 自动协商模式 （默认）	X	X
adv-1000fdx-cap	由硬件声明的本地接口性能 0 = 不能进行 1000 Mbps 全双工 1 = 能够进行 1000 Mbps 全双工 （默认）		X
adv-1000hdx-cap	由硬件声明的本地接口性能 0 = 不能进行 1000 Mbps 半双工 1 = 能够进行 1000 Mbps 半双工 （默认）	X	X
adv-100fdx-cap	由硬件声明的本地接口性能 0 = 不能进行 100 Mbps 全双工 1 = 能够进行 100 Mbps 全双工 （默认）	X	

表 3-2 操作模式参数 *（续）*

参数	说明	UTP 适配器	MMF 适配器
adv-100hdx-cap	由硬件声明的本地接口性能 0 = 不能进行 100 Mbps 半双工 1 = 能够进行 100 Mbps 半双工 （默认）	X	
adv-10fdx-cap	由硬件声明的本地接口性能 0 = 不能进行 10 Mbps 全双工 1 = 能够进行 10 Mbps 全双工 （默认）	X	
adv-10hdx-cap	由硬件声明的本地接口性能 0 = 不能进行 10 Mbps 半双工 1 = 能够进行 10 Mbps 半双工 （默认）	X	

如果表 3-2 中所有参数均设为 1，则自动协商模式会尽量采用最高的速度。如果您将这些参数均设为 0，则会收到以下错误消息：

```
NOTICE: Last setting will leave vca0 with no link capabilities.
WARNING: vca0: Restoring previous setting.
```

注 – 在上面的示例中，vca0 是 Sun Crypto Accelerator 4000 的设备名称，其中字符串 vca 表示每一个 Sun Crypto Accelerator 4000 板。此字符串后面始终紧跟板的设备例程号。因此， vca0 板的设备例程号为 0。

流控制参数

vca 设备能够产生 （发送）和终止 （接收）符合 EEE 802.3x Frame Based Link Level Flow Control Protocol 要求的暂停帧。回应收到的流控制帧时， vca 设备可以降低其发送速率。此外， vca 设备还可以产生流控制帧以及请求链接伙伴降低其发送速率 （如果链接伙伴支持此项功能）。默认情况下，驱动程序会在自动协商期间声明发送和接收暂停性能。

表 3-3 列出了流控制关键字并说明了它们的作用。

表 3-3 读-写流控制关键字说明

关键字	说明		
adv-asmpause-cap	MMF 适配器和 UTP 适配器都支持非对称暂停；因此， vca 设备只能单向暂停。 0 = 关闭 （默认） 1 = 打开		
adv-pause-cap	此参数有两种含义，具体取决于 adv-asmpause-cap 的值。（默认值 = 0）		
	参数值 +	**参数值 =**	**说明**
	adv-asmpause-cap=	adv-pause-cap=	
	1	1 或 0	adv-pause-cap 确定暂停操作的方向。
	1	1	接收暂停但不发送。
	1	0	发送暂停但不接收。
	0	1	发送和接收暂停。
	0	1 或 0	adv-pause-cap 参数确定是打开还是关闭暂停功能。
pause-on-threshold	定义接收 (RX) FIFO 中的 64 字节块数，可以使板生成 XON-PAUSE 帧。		
pause-off-threshold	定义 RX FIFO 中的 64 字节块数，可以使板生成 XOFF-PAUSE 帧。		

千兆位强制模式参数

对于千兆位链接， link-master 参数用于确定链接主控设备。通常，交换机用作链接主控设备；在这种情况下，此参数可以保持不变。如果交换机没有用作链接主控设备，则可用 link-master 参数指定 vca 设备作为链接主控设备。

表 3-4 千兆位强制模式参数

参数	说明
link-master	设为 1 时，该参数启用主控操作，即假定链接伙伴为从属设备。 设置为 0 时，该参数启用从属操作，即假定链接伙伴为主控设备（默认）。

数据包收发间隔参数

vca 设备支持 enable-ipg0 可编程模式。

当启用 enable-ipg0 （默认）时， vca 设备会在发送数据包之前增加额外的延迟时间。这一延迟 （由 ipg0 参数设定）是对 ipg1 和 ipg2 参数所设定延迟的补充。增加额外的 ipg0 延迟可以降低冲突机率。

当禁用 enable-ipg0 时， ipg0 参数值会被忽略，且不会设定额外的延迟。此时，只使用由 ipg1 和 ipg2 参数设定的延迟。如果其它系统持续发送大量的连续数据包，请禁用 enable-ipg0。系统在启用 enable-ipg0 后，可能在网络上没有充足的时间。此时，您可以通过设置 ipg0 参数 （范围是 0 至 255，这是介质字节延迟时间）来增加额外的延迟。表 3-5 定义了 enable-ipg0 和 ipg0 参数。

表 3-5 定义 enable-ipg0 和 ipg0 参数

参数	值	说明
enable-ipg0	0 1	启用 enable-ipg0 禁用 enable-ipg0 （默认值 = 1）
ipg0	0 至 255	收到数据包与发送数据包之间的额外延迟时间（或间隔）（默认值 = 8）

vca 设备支持可编程的数据包收发间隔 (IPG, Interpacket Gap) 参数 ipg1 和 ipg2。总 IPG 是 ipg1 与 ipg2 之和。链接速率为 1000 Mbps 时，总 IPG 为 0.096 微秒。

表 3-6 列出了 IPG 参数的默认值和允许值。

表 3-6 读-写数据包收发间隔参数值和说明

参数	值 （字节时间）	说明
ipg1	0 至 255	数据包收发间隔 1 （默认值 = 8）
ipg2	0 至 255	数据包收发间隔 2 （默认值 = 4）

默认情况下，驱动程序将 ipg1 设为 8 字节时间， ipg2 设为 4 字节时间，这些都是标准值。（字节时间是指在链接速率为 1000 Mbps 时发送一个字节所用的时间。）

如果在您的网络中，某些系统使用较长的 IPG 时间 （ipg1 与 ipg2 之和），并且它们访问网络的速度似乎较慢，请适当增加 ipg1 和 ipg2 的值，以便与其它系统的较长 IPG 时间一致。

中断参数

表 3-7 介绍了接收中断消隐值。

表 3-7 用于读取别名的 RX 消隐寄存器

字段名称	值	说明
rx-intr-pkts	0 至 511	自处理上一个数据包后，收到此数量的数据包之后即会中断。零值表示无数据包消隐 （默认值 = 3）。
rx-intr-time	0 至 524287	自处理上一个数据包后，等待 4.5 微秒 (Usecs)，然后中断。零值表示无数据包消隐 （默认值 = 3）。

随机提前丢弃参数

这些参数允许依据接收 FIFO 的充满程度来丢弃数据包。默认情况下，此功能禁用。当 FIFO 占用率达到某一范围时，将会根据预定的概率丢弃数据包。当 FIFO 等级增加时，概率也会随之增加。控制数据包永远不会丢弃，且不计入统计数据。

表 3-8 RX 随机提前检测 8 位矢量

字段名称	值	说明
red-dv4to6k	0 至 255	当 FIFO 阈值范围大于 4,096 字节且小于 6,144 字节时，适用的随机提前检测和数据包丢弃矢量。丢弃概率可以按 12.5 百分比的增量进行设定。例如，如果设为 “位 0”，则会丢弃此范围内的每八个数据包中的第一个数据包 （默认值 = 0）。
red-dv6to8k	0 至 255	当 FIFO 阈值范围大于 6,144 字节且小于 8,192 字节时，适用的随机提前检测和数据包丢弃矢量。丢弃概率可以按 12.5 百分比的增量进行设定。例如，如果设为 “位 8”，则会丢弃此范围内的每八个数据包中的第一个数据包 （默认值 = 0）。
red-dv8to10k	0 至 255	当 FIFO 阈值范围大于 8,192 字节且小于 10,240 字节时，适用的随机提前检测和数据包丢弃矢量。丢弃概率可以按 12.5 百分比的增量进行设定。例如，如果设为 “位 16”，则会丢弃此范围内的每八个数据包中的第一个数据包 （默认值 = 0）。
red-dv10to12k	0 至 255	当 FIFO 阈值范围大于 10,240 字节且小于 12,288 字节时，适用的随机提前检测和数据包丢弃矢量。丢弃概率可以按 12.5 百分比的增量进行设定。例如，如果设为 “位 24”，则会丢弃此范围内的每八个数据包中的第一个数据包 （默认值 = 0）。

PCI 总线接口参数

您可使用这些参数来修改 PCI 接口功能，从而使给定的应用程序获得更好的 PCI 互连性能。

表 3-9 PCI 总线接口参数

参数	说明
tx-dma-weight	确定在繁重的循环仲裁过程中为发送 (TX) 端赋予的倍增因数；其值为 0 至 3 （默认值 = 0）。零值表示没有额外的加权。其它值使用 2 次幂来处理繁重的通信。例如，如果 tx-dma-weight = 0 且 rx-dma-weight = 3, 则只要 RX 通信持续到达，RX 通信访问 PCI 的优先级是 TX 通信访问 PCI 优先级的 8 倍 （即 2 的 3 次幂）。
rx-dma-weight	确定在加权循环仲裁过程中为接收 (RX) 端赋予的倍增因数。其值为 0 至 3 （默认值 = 0）。
infinite-burst	当启用此参数且系统支持 infinite burst （无限提速）时，允许使用无限提速功能。在此情况下，适配器不会释放总线，直到数据包通过总线传输完毕为止。其值为 0 或 1 （默认值 = 0）。
disable-64bit	关闭适配器的 64 位功能。 注：对于基于 UltraSPARC® III 的平台，此参数的默认值可能为 1。对于基于 UltraSPARC II 的平台，默认值为 0。其值为 0 或 1（默认值 =0，即启用 64 位功能）。

设置 vca 驱动程序参数

您可采用两种方法来设置 vca 设备驱动程序的参数：

- 使用 ndd 实用程序
- 使用 vca.conf 文件

如果使用 ndd 实用程序，则所设的参数将在重新启动系统后失效。此方法适于测试参数设置。

要使所设置的参数在重新启动系统后仍保持有效，请创建 /kernel/drv/vca.conf 文件，并在其中添加必要的参数值 （如需为系统中的设备设置特殊参数）。有关详情，请参阅第 35 页 “使用 vca.conf 文件设置驱动程序参数”。

使用 ndd 实用程序设置参数

使用 ndd 实用程序配置参数时，所设的参数将在重新启动系统后失效。

以下几节介绍如何使用 vca 驱动程序和 ndd 实用程序修改（使用 -set 选项）或显示（不用 -set 选项）每一个 vca 设备的参数。

▼ 为 ndd 实用程序指定设备例程

使用 ndd 实用程序获取或设置 vca 设备的参数之前，必须为此实用程序指定设备例程。

1. **检查 /etc/path_to_inst 文件，确定与特定设备相关的例程号。参阅 path_to_inst(4) 的联机手册页。**

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
"/pci@8,700000/network@1" 1 "vca"
```

在上面的示例中，有二个 Sun Crypto Accelerator 4000 以太网例程来自已安装的适配器。例程号是 0 和 1。

2. **使用例程号选择设备。**

```
# ndd -set /dev/vcaN
```

注 – 在本用户指南介绍的示例中， *N* 表示设备的例程号。

此设备会一直保持选定状态，直到您更改选择为止。

非交互和交互模式

您可在两种模式下使用 ndd 实用程序：

- 非交互模式
- 交互模式

在非交互模式下，您可以运行实用程序来执行某个特殊命令。执行该命令之后，您将退出实用程序。在交互模式下，您可以使用实用程序来获得或设置多个参数值。有关详细信息，请参阅 ndd(1M) 联机手册页。

在非交互模式下使用 ndd *实用程序*

本节介绍如何修改和显示参数值。

- **要修改参数值，请使用** -set **选项。**

  如果您运行 ndd 实用程序及其 -set 选项，实用程序将传递*值*（该值必须分配给指定的 /dev/vca 驱动程序例程），并将其分配给参数：

```
# ndd -set /dev/vcaN parameter value
```

  更改任何 adv 参数时，屏幕上会显示一则类似于以下的消息：

```
- link up 1000 Mbps half duplex
```

- **要显示参数的值，请指定参数名，但不要输入其值。**

  当忽略 -set 选项时，会出现查询操作，实用程序询问指定的驱动程序例程，检索与指定参数相关的值，然后打印该值：

```
# ndd /dev/vcaN parameter
```

注 – 在上面的示例中， *N* 是 vca 设备的例程号。此号码应反映您正在为其运行 kstat 命令的板的例程号。

在交互模式下使用 ndd *实用程序*

- **要在交互模式下修改参数值，请指定** ndd /dev/vca*N*，**如下所示。**

  ndd 实用程序随后会提示您输入参数名称：

```
# ndd /dev/vcaN
name to get/set? (Enter the parameter name or ? to view all
parameters)
```

注 – 在上面的示例中， *N* 是 vca 设备的例程号。此号码应反映您正在为其运行 kstat 命令的板的例程号。

输入参数名称后， ndd 实用程序会提示您输入参数值 （参见表 3-1 至表 3-9）。

- **要列出** vca **驱动程序支持的所有参数，请键入** ndd /dev/vca*N*。
  （有关参数说明，请参见表 3-1 至表 3-9）。

```
# ndd /dev/vcaN
name to get/set ? ?
?                                (read only)
instance                         (read and write)
adv-autoneg-cap                  (read and write)
adv-1000fdx-cap                  (read and write)
adv-1000hdx-cap                  (read and write)
adv-100fdx-cap                   (read and write)
adv-100hdx-cap                   (read and write)
adv-10fdx-cap                    (read and write)
adv-10hdx-cap                    (read and write)
adv-asmpause-cap                 (read and write)
adv-pause-cap                    (read and write)
pause-on-threshold               (read and write)
pause-off-threshold              (read and write)
link-master                      (read and write)
enable-ipg0                      (read and write)
ipg0                             (read and write)
ipg1                             (read and write)
ipg2                             (read and write)
rx-intr-pkts                     (read and write)
rx-intr-time                     (read and write)
red-p4k-to-6k                    (read and write)
red-p6k-to-8k                    (read and write)
red-p8k-to-10k                   (read and write)
red-p10k-to-12k                  (read and write)
tx-dma-weight                    (read and write)
rx-dma-weight                    (read and write)
infinite-burst                   (read and write)
disable-64bit                    (read and write)
name to get/set ?
#
```

注 – 在上面的示例中，*N* 是 vca 设备的例程号。此号码应反映您正在为其运行 kstat 命令的板的例程号。

设置自动协商或强制模式

下列链接参数可以设为在自动协商或强制模式下进行操作：

- speed
- duplex
- link-clock

默认情况下，系统会为这些链接参数启用自动协商模式。当这些参数均处于自动协商模式下时， vca 设备将与链接伙伴通信，以协商相互兼容的值和流控制性能。当为这些参数设置 auto 之外的值时，链接伙伴双方不会进行协商，并且将链接参数配置为在强制模式下进行操作。在强制模式下，链接伙伴双方的 speed 参数值必须一致。有关说明，请参阅第 37 页 “使用 OpenBoot PROM 为链接参数启用自动协商或强制模式”。

▼ 禁用自动协商模式

如果您的网络设备不支持自动协商模式，或者您想在强制模式下使用网络 speed、duplex 或 link-clock 参数，则可以在 vca 设备上禁用自动协商模式。

1. **将以下驱动程序参数的值设为链接伙伴设备 （例如，交换机）附带文档中所述的值：**
   - adv-1000fdx-cap
   - adv-1000hdx-cap
   - adv-100fdx-cap
   - adv-100hdx-cap
   - adv-10fdx-cap
   - adv-10hdx-cap
   - adv-asmpause-cap
   - adv-pause-cap

   有关这些参数的说明和可能值，请参见表 3-2。

2. **将** adv-autoneg-cap **参数设为** 0。

```
# ndd -set /dev/vcaN adv-autoneg-cap 0
```

更改任何 ndd 参数时，屏幕上均会显示一则类似于以下的消息：

```
link up 1000 Mbps half duplex
```

注 – 如果您禁用了自动协商模式，则必须让 speed、 duplex 和 link-clock （只适用于 1000 Mbps）参数在强制模式下操作。有关说明，请参阅第 37 页 “使用 OpenBoot PROM 为链接参数启用自动协商或强制模式”。

使用 vca.conf 文件设置参数

您也可以通过向 /kernel/drv 目录下的 vca.conf 文件中添加条目来指定驱动程序参数属性。参数名称与第 24 页 “驱动程序参数值和定义”中列出的名称相同。

注意 – 请勿删除 /kernel/drv/vca.conf 文件中的任何默认条目。

有关其它详细资料，请参阅 prtconf(1) 和 driver.conf(4) 联机手册页。下面的过程介绍了在 vca.conf 文件中设置参数的示例。

上一节中定义的变量适用于系统中的已知设备。要通过 vca.conf 文件为 Sun Crypto Accelerator 4000 板设置变量，必须知道以下三条设备信息：设备名称、父设备、设备单元地址。

▼ 使用 vca.conf 文件设置驱动程序参数

1. **获取 vca 设备在设备树中的硬件路径名称。**

   a. **检查 /etc/driver_aliases 文件，确定与特定设备相关的名称。**

```
# grep vca /etc/driver_aliases
vca "pci108e,3de8"
```

   在上面的示例中，与 Sun Crypto Accelerator 4000 软件驱动程序 (vca) 相关的设备名称是 “pci108e,3de8”。

   b. **在 /etc/path_to_inst 文件中找到父设备名称和设备单元地址。**

   参阅 path_to_inst(4) 的联机手册页。

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
"/pci@8,700000/network@1" 1 "vca"
```

在上面的示例中，共有三栏输出值：设备路径名称、例程号和软件驱动程序名称。

上述示例中第一行内的设备路径名称是 “/pci@8,600000/network@1”。设备路径名称由三部分组成：父设备名称、设备节点名称和设备单元地址。有关说明，请参见表 3-10。

表 3-10 设备路径名称

完整设备路径名称	父设备名称部分	节点名称部分	单元地址部分
"/pci@8,600000/network@1"	/pci@8,600000	network	1
"/pci@8,700000/network@1"	/pci@8,700000	network	1

要在 vca.conf 文件中明确标识 PCI 设备，请使用设备的完整设备路径名称（父设备名称、节点名称和单元地址）。有关 PCI 设备规格的详细信息，请参阅 pci(4) 联机手册页。

2. **在 /kernel/drv/vca.conf 文件中为 vca 设备设置参数。**

   在下面的条目中，系统为某个特定 Sun Crypto Accelerator 4000 以太网设备禁用了 adv-autoneg-cap 参数。

```
name="pci108e,3de8" parent="/pci@8,700000" unit-address="1" adv-autoneg-cap=0;
```

3. **保存 vca.conf 文件。**
4. **保存和关闭所有文件及程序，然后退出窗口系统。**
5. **关闭然后重新启动系统。**

使用 vca.conf 文件为所有 Sun Crypto Accelerator 4000 vca 设备设置参数

如果忽略设备路径名称（父设备名称、节点名称和单元地址），则系统会为所有 Sun Crypto Accelerator 4000 以太网设备的每一个例程设置参数。

▼ 使用 vca.conf 文件为所有 Sun Crypto Accelerator 4000 vca 设备设置参数

1. **在 vca.conf 文件中，通过输入*参数* = *值*;添加一行，更改所有例程的参数值。**

   下面的示例将所有 Sun Crypto Accelerator 4000 以太网设备的每一个例程的 adv-autoneg-cap 参数值设为 1：

```
adv-autoneg-cap=1;
```

vca.conf 文件示例

下面是 vca.conf 文件的示例：

```
#
# Copyright 2003 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
#ident  "@(#)vca.conf   1.3     13-3-10 SMI"

#
# Use the new Solaris 9 ddi-no-autodetach property to prevent the
# driver from being unloaded by the cleanup modunload -i 0.
#
ddi-no-autodetach=1;
```

使用 OpenBoot PROM 为链接参数启用自动协商或强制模式

通过 OpenBoot PROM 界面，可将下列参数设置为在自动协商或强制模式下操作：

表 3-11 本地链接网络设备参数

参数	说明
speed	此参数可以设为 auto、1000、100 或 10；语法如下： • speed=auto（默认值） • speed=1000 • speed=100 • speed=10
duplex	此参数可以设为 auto、full 或 half；语法如下： • duplex=auto（默认值） • duplex=full • duplex=half

表 3-11 本地链接网络设备参数 *（续）*

参数	说明
link-clock	只有 speed 参数设为 1000 或使用 1000 Mbps MMF Sun Crypto Accelerator 4000 板时，此参数才适用。此参数的值必须与为链接伙伴设置的值相对应。例如，当本地链接的值为 master 时，则链接伙伴的值必须为 slave。此参数可以设为 master、 slave 或 auto；语法如下： • link-clock=auto（默认值） • link-clock=master • link-clock=slave

要建立正常的链接，必须在本地链接和链接伙伴之间正确配置 speed、 duplex 和 link-clock（只适用于 1000 Mbps）参数。本地链接和链接伙伴的每一个 speed、duplex 和 link-clock（只适用于 1000 Mbps）参数必须在自动协商或强制模式下进行操作。当其中一个参数值设为 auto 时，会使链接在该参数的自动协商模式下进行操作。如果在 OpenBoot PROM ok 提示符下未输入参数，则系统会将参数的值默认设为 auto。当其中一个参数设为 auto 之外的其它值时，会使本地链接在该参数的强制模式下进行操作。

当本地链接在 speed 和 duplex 参数的自动协商模式下操作时，如果其网络速率为 100 Mbps 或更低，并且启用了全双工和半双工模式，则链接伙伴可以采用 100 Mbps 或 10 Mbps 的速度以及任何一种双工模式进行操作。

当 speed 参数在强制模式下操作时，本地链接的 speed 值必须与链接伙伴的 speed 值一致。如果本地链接和链接伙伴之间的 duplex 参数不匹配，虽然可以进行链接；但会出现通信冲突。

当本地链接的 speed 参数设为自动协商模式，链接伙伴的 speed 参数设为强制模式时，也许可以建立链接，具体取决于 speed 的值是否可在本地链接和链接伙伴之间进行协商。默认情况下，自动协商模式下的接口将始终尝试采用半双工模式建立链接（如果速度匹配的话）。由于这两个接口中的其中一个不处于自动协商模式，处于自动协商模式下的接口将只检测 speed 参数；而不检测双工参数。这种方法称为 “并行检测”。

注意 – 在双工不一致时建立的链接总会导致通信冲突。

对于要在强制模式下操作的本地链接参数，其值必须是 auto 之外的值。例如，要建立速度为 100 Mbps 且半双工的强制模式链接，请在 OpenBoot PROM ok 提示符下键入以下命令：

```
ok boot net:speed=100,duplex=half
```

注 – 在本节的示例中，net 是默认的集成网络接口设备路径的别名。您也可以通过指定某个设备路径（而非使用 net）来配置其它网络设备。

要建立速度为 1000 Mbps、半双工且为时钟主控方的强制模式链接，请在 OpenBoot PROM ok 提示符下键入以下命令：

```
ok boot net:speed=1000,duplex=half,link-clock=master
```

注 – 本地链接的 link-clock 参数值必须与链接伙伴的 link-clock 值相对应。例如，当本地链接的 link-clock 值设为 master 时，链接伙伴的 link-clock 值必须设为 slave。

要建立以下链接：速度为 10 Mbps 且采用强制模式；双工且采用自动协商模式，请在 OpenBoot PROM ok 提示符下键入以下命令：

```
ok boot net:speed=10,duplex=auto
```

另外，您也可以在 OpenBoot PROM ok 提示符下键入以下命令，以建立与上一示例相同的本地链接参数：

```
ok boot net:speed=10
```

有关详细信息，请参阅 IEEE 802.3 文档。

加密和以太网驱动程序操作统计

本节介绍由 kstat(1M) 命令提供的统计信息。

加密驱动程序统计

表 3-12 介绍了加密驱动程序的统计信息。

表 3-12 加密驱动程序统计

参数	说明	稳定或不稳定
vs-mode	其值可为 FIPS、 standard 或 unitialized。 FIPS 表示板处于 FIPS 模式。 standard 表示板不处于 FIPS 模式。 unitialized 表示板未初始化。	稳定
vs-status	其值可为 ready、 faulted 或 failsafe。 ready 表示板操作正常。 faulted 表示板未进行操作。 failsafe 表示 failsafe 模式，是板的原始出厂状态。	稳定

以太网驱动程序统计

表 3-13 介绍了以太网驱动程序的统计信息。

表 3-13 以太网驱动程序统计

参数	说明	稳定或不稳定
ipackets	入站数据包的数量。	稳定
ipackets64	64 位版本的 ipackets。	稳定
ierrors	已收到的因包含错误而无法处理的总数据包数（长）。	稳定
opackets	请求通过接口发送的总数据包数。	稳定
opackets64	请求通过接口发送的总数据包数 （64 位）。	稳定
oerrors	因错误而未成功发送的总数据包数 （长）。	稳定
rbytes	通过接口成功接收的总字节数。	稳定
rbytes64	通过接口成功接收的总字节数 （64 位）。	稳定
obytes	请求通过接口发送的总字节数。	稳定
obytes64	请求通过接口发送的总字节数 （64 位）。	稳定
multircv	成功接收的多播数据包数，包括组和功能地址（长）。	稳定
multixmt	请求发送的多播数据包数，包括组和功能地址（长）。	稳定

表 3-13 以太网驱动程序统计 *（续）*

参数	说明	稳定或不稳定
brdcstrcv	成功接收的广播数据包数 （长）。	稳定
brdcstxmt	请求发送的广播数据包数 （长）。	稳定
norcvbuf	由于无法为接收数据包分配缓冲器，而导致输入的有效数据包被丢弃的已知次数 （长）。	稳定
noxmtbuf	由于发送缓冲器繁忙或者没有分配用于发送的缓冲器，而在输出时被丢弃的数据包数 （长）。	稳定

表 3-14 介绍了发送和接收 MAC 计数器。

表 3-14 TX 和 RX MAC 计数器

参数	说明	稳定或不稳定
tx-collisions	对于导致冲突的每一次帧发送尝试，16 位可加载计数器的累计。	稳定
tx-first-collisions	对于符合以下条件的每一次帧发送：第一次尝试时遇到故障，但第二次尝试获得成功， 16 位可加载计数器的累计。	不稳定
tx-excessive-collisions	对于已超出发送限制次数的每一次帧发送， 16 位可加载计数器的累计。	不稳定
tx-late-collisions	对于发生冲突的每一次帧发送， 16 位可加载计数器的累计。此参数表示 TxMAC 在发送至少 Minimum Frame Size （最小帧大小）字节数之后因出现冲突而丢弃的帧数。通常，它表示网络上至少有一个站点违背了网络的最大允许范围。	不稳定
tx-defer-timer	对于以下情况， 16 位可加载计时器的累计：TxMAC 在尝试发送帧期间推迟网络上的通信。计时器的计时单位是介质字节时钟除以 256。	不稳定
tx-peak-attempts	8 位寄存器，表示自上次读取寄存器之后，每个成功发送帧的最大连续冲突数。此寄存器的最大值是 255。如果每个成功发送帧的连续冲突数超过 255，则软件会发生可屏蔽中断。此寄存器会在读取之后自动归零。	不稳定
tx-underrun	通过网络收到有效帧之后， 16 位可加载计数器的累计。	不稳定

表 3-14 TX 和 RX MAC 计数器 *（续）*

参数	说明	稳定或不稳定
rx-length-err	通过网络收到长度大于 Maximum Frame Size Register （最大帧大小寄存器）中设定值的帧之后， 16 位可加载计数器的累计。	不稳定
rx-alignment-err	对于以下情况， 16 位可加载计数器的累计：在接收帧中检测到校准错误。当接收帧未能通过循环冗余校验和 (CRC) 检查算法，*且*帧包含非整数的字节数 （即以位表示的帧大小不能被 8 除尽）时，系统即会报告校准错误。	不稳定
rx-crc-err	对于以下情况， 16 位可加载计数器的累计：当接收帧未能通过 CRC 检测算法，*且*帧包含整数的字节数 （即以位表示的帧大小可被 8 除尽）。	不稳定
rx-code-violations	对于以下情况， 16 位可加载计数器的累计：在接收帧期间，XCVR 通过 MII 生成 Rx_Err 指示。当收发器在收到的数据流中检测到无效代码时，即会生成此指示。接收代码违例不被计为 FCS 或校准错误。	不稳定
rx-overflows	由于缺乏资源而被丢弃的以太网帧数。	不稳定
rx-no-buf	硬件因没有更多的接收缓冲器空间而无法接收数据的次数。	不稳定
rx-no-comp-wb	硬件无法为收到的数据传送完成条目的次数。	不稳定
rx-len-mismatch	帧声明长度与实际帧长度不匹配的已收到帧数。	不稳定

以下以太网属性 （表 3-15）是设备性能和链接伙伴性能的共同部分：

表 3-15 当前以太网链接属性

参数	说明	稳定或不稳定
ifspeed	1000、 100 或 10 Mbps	稳定
link-duplex	0 = 半双工， 1 = 全双工	稳定
link-pause	有关链接的当前暂停设置，请参阅第 26 页 “流控制参数”	稳定
link-asmpause	有关链接的当前暂停设置，请参阅第 26 页 “流控制参数”	稳定

表 3-15 当前以太网链接属性 *（续）*

参数	说明	稳定或不稳定
link-up	1 = 启动， 0 = 关闭	稳定
link-status	1 = 启动， 0 = 关闭	稳定
xcvr-inuse	所用收发器的类型：1 = 内部 MII， 2 = 外部 MII， 3 = 外部 PCS	稳定

表 3-16 介绍了只读介质独立接口 (MII, Media Independent Interface) 的性能。这些参数用于定义硬件的性能。千兆位介质独立接口 (GMII, Gigabit Media Independent Interface) 支持下列所有性能。

表 3-16 只读 vca 设备性能

参数	说明	稳定或不稳定
cap-autoneg	0 = 不能自动协商 1 = 能够自动协商	稳定
cap-1000fdx	本地接口全双工性能 0 = 不能进行 1000 Mbps 全双工 1 = 能够进行 1000 Mbps 全双工	稳定
cap-1000hdx	本地接口半双工性能 0 = 不能进行 1000 Mbps 半双工 1 = 能够进行 1000 Mbps 半双工	稳定
cap-100fdx	本地接口全双工性能 0 = 不能进行 100 Mbps 全双工 1 = 能够进行 100 Mbps 全双工	稳定
cap-100hdx	本地接口半双工性能 0 = 不能进行 100 Mbps 半双工 1 = 能够进行 100 Mbps 半双工	稳定
cap-10fdx	本地接口全双工性能 0 = 不能进行 10 Mbps 全双工 1 = 能够进行 10 Mbps 全双工	稳定
cap-10hdx	本地接口半双工性能 0 = 不能进行 10 Mbps 半双工 1 = 能够进行 10 Mbps 半双工	稳定
cap-asm-pause	本地接口流控制性能 0 = 不能执行非对称暂停 1 = 能够从本地设备执行非对称暂停 （参阅第 26 页“流控制参数”）	稳定
cap-pause	本地接口流控制性能 0 = 不能执行对称暂停 1 = 能够执行对称暂停 （参阅第 26 页 “流控制参数”）	稳定

报告链接伙伴性能

表 3-17 介绍了只读链接伙伴性能。

表 3-17 只读链接伙伴性能

参数	说明	稳定或不稳定
`lp-cap-autoneg`	0 = 无自动协商 1 = 自动协商	稳定
`lp-cap-1000fdx`	0 = 不能进行 1000 Mbps 全双工发送 1 = 1000 Mbps 全双工	稳定
`lp-cap-1000hdx`	0 = 不能进行 1000 Mbps 半双工发送 1 = 1000 Mbps 半双工	稳定
`lp-cap-100fdx`	0 = 不能进行 100 Mbps 全双工发送 1 = 100 Mbps 全双工	稳定
`lp-cap-100hdx`	0 = 不能进行 100 Mbps 半双工发送 1 = 100 Mbps 半双工	稳定
`lp-cap-10fdx`	0 = 不能进行 10 Mbps 全双工发送 1 = 10 Mbps 全双工	稳定
`lp-cap-10hdx`	0 = 不能进行 10 Mbps 半双工发送 1 = 10 Mbps 半双工	稳定
`lp-cap-asm-pause`	0 = 不能执行非对称暂停 1 = 用于链接伙伴性能的非对称暂停 （参阅第 26 页 “流控制参数”）	稳定
`lp-cap-pause`	0 = 不能执行对称暂停 1 = 能够执行对称暂停 （参阅第 26 页 “流控制参数”）	稳定

如果链接伙伴不能进行自动协商 （当 `lp-cap-autoneg` 为 0 时），表 3-17 中的其余信息不适用，并且参数值为 0。

如果链接伙伴能够进行自动协商 （当 `lp-cap-autoneg` 为 1 时），则在使用自动协商和链接伙伴性能时，屏幕上会显示速度和模式信息。

表 3-18 介绍了驱动程序专用的参数。

表 3-18 驱动程序专用参数

参数	说明	稳定或不稳定
lb-mode	设备所处的回送模式（如果有的话）的复件。	不稳定
promisc	当启用该参数时，设备处于混合模式。当禁用该参数时，设备不处于混合模式。	不稳定
以太网发送计数器		
tx-wsrv	发送环充满的次数。	不稳定
tx-msgdup-fail	尝试复制数据包失败。	不稳定
tx-allocb-fail	尝试分配内存失败。	不稳定
tx-queue0	在第一个硬件发送队列中等待发送的数据包的数量。	不稳定
tx-queue1	在第二个硬件发送队列中等待发送的数据包的数量。	不稳定
tx-queue2	在第三个硬件发送队列中等待发送的数据包的数量。	不稳定
tx-queue3	在第四个硬件发送队列中等待发送的数据包的数量。	不稳定
以太网接收计数器		
rx-hdr-pkts	收到的少于 256 字节的数据包数量。	不稳定
rx-mtu-pkts	收到的大于 256 字节且小于 1514 字节的数据包数量。	不稳定
rx-split-pkts	被分割为两页的数据包数量。	不稳定
rx-nocanput	由于发送至 IP 堆栈失败而丢弃的数据包数量。	不稳定
rx-msgdup-fail	不能进行复制的数据包数量。	不稳定
rx-allocb-fail	块分配失败的次数。	不稳定
rx-new-pages	在接收期间被替换的页数。	不稳定
rx-new-hdr-pages	在接收期间被替换的、并且包含小于 256 字节的数据包的页数。	不稳定
rx-new-mtu-pages	在接收期间被替换的、并且包含大于 256 字节且小于 1514 字节的数据包的页数。	不稳定

表 3-18 驱动程序专用参数 *（续）*

参数	说明	稳定或不稳定
rx-new-nxt-pages	在接收期间被替换的、并且包含那些分割在多个页上的数据包的页数。	不稳定
rx-page-alloc-fail	页分配失败的次数。	不稳定
rx-mtu-drops	由于驱动程序无法映射新页来替换一整页大于 256 字节且小于 1514 字节的数据包，而造成此类页被丢弃的次数。	不稳定
rx-hdr-drops	由于驱动程序无法映射新页来替换一整页小于 256 字节的数据包，而造成此类页被丢弃的次数。	不稳定
rx-nxt-drops	由于驱动程序无法映射新页来替换具有分割数据包的页，而造成此类页被丢弃的次数。	不稳定
rx-rel-flow	驱动程序被要求释放流的次数。	不稳定
以太网 PCI 属性		
rev-id	Sun Crypto Accelerator 4000 以太网设备的版本 ID 对于识别域中所用的设备非常有用。	不稳定
pci-err	所有 PCI 错误的总和。	不稳定
pci-rta-err	收到目标中断的次数。	不稳定
pci-rma-err	收到主控中断的数量。	不稳定
pci-parity-err	检测到的 PCI 奇偶校验错误数量。	不稳定
pci-drto-err	已达到延迟发送重试超时的次数。	不稳定
dma-mode	由 Sun Crypto Accelerator 4000 驱动程序 (vca) 使用。	不稳定

▼ 检查链接伙伴设置

- **成为超级用户，键入** `kstat vca:`*N* **命令：**

```
# kstat vca:N
module: vca                             instance: 0
name:   vca0                            class:    misc
```

其中 *N* 为 vca 设备的例程号。此号码应反映您正在为其运行 kstat 命令的板的例程号。

IPsec 线内加速统计

表 3-19 介绍了当板用于线内 IPsec 硬件加速时所累计的核心统计信息。有关如何配置板以使用线内 IPsec 配置的说明，请参阅第 50 页 “启用线内 IPsec 加速”。

表 3-19 线内 IPsec 加速的加密驱动程序统计

参数	说明	稳定或不稳定
ipsec_ierrrors	已收到的因包含错误而无法处理的 IPsec 数据包总数 （长）	稳定
ipsec_ipackets	入站 IPsec 数据包的数量	稳定
ipsec_ipackets64	入站 IPsec 数据包的数量 （64 位）	稳定
ipsec_obytes	请求通过接口发送的 IPsec 字节总数	稳定
ipsec_obytes64	请求通过接口发送的 IPsec 字节总数 （64 位）	稳定
ipsec_oerrors	由于错误而未成功发送的 IPsec 数据包总数 （长）	稳定
ipsec_opackets	请求通过接口发送的 IPsec 数据包总数	稳定
ipsec_opackets64	请求通过接口发送的 IPsec 数据包总数 （64 位）	稳定
ipsec_rbytes	通过接口成功接收的 IPsec 字节总数	稳定
ipsec_rbytes64	通过接口成功接收的 IPsec 字节总数 （64 位）	稳定
sadb_cache_misses	固件高速缓存器缺失数	稳定
sadb_cache_overflows	固件高速缓存器溢出数	稳定
sadb_entries	SADB 驱动程序中的条目数	稳定
sadb_operations	从 Solaris IPsec 发送至驱动程序的 SADB 操作数	稳定

注 – 只有在 IPsec 数据包真正由硬件在线内处理时，才会累计表 3-19 中所列的 IPsec 核心统计。低于 256 字节的接收数据包不会进行线内处理，因此这些数据包不会累计 IPsec 核心统计。此外，这些核心统计还不适用于带外 IPsec 通信（参阅第 49 页“配置 IPsec 硬件加速”）。如果启用 `snoop`，则不会累计这些计数器。带外数据包将累计常规网络核心统计以及任何适用的加密统计，即 `3desbytes` 和 `3desjobs`。

网络配置

本节介绍如何在系统中安装适配器之后编辑网络主机文件。

配置网络主机文件

安装驱动程序软件之后，必须为适配器的以太网接口创建一个 hostname.vca*N* 文件。注意，在文件名 hostname.vca*N* 中， *N* 表示您要使用的 vca 接口的例程号。此外，您还必须在 /etc/hosts 文件中为其以太网接口创建 IP 地址和主机名。

1. **在 /etc/path_to_inst 文件中查找正确的 vca 接口和例程号。**

   参阅 path_to_inst(4) 的联机手册页。

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
```

   上面示例中的例程号为 0。

2. **使用 ifconfig(1M) 命令设置适配器的 vca 接口。**

   使用 ifconfig 命令指定网络接口的 IP 地址。在命令行键入以下命令，并用适配器的 IP 地址替换 *ip_address*：

```
# ifconfig vcaN plumb ip_address up
```

   有关详细信息，请参阅 ifconfig(1M) 手册页和 Solaris 文档。

   - 如果您希望设置在重新引导系统后仍保持有效，请创建 /etc/*hostname*.vca*N* 文件，其中 *N* 是指您要使用的 vca 接口的例程号。

     要使用步骤 1 中所示示例的 vca 接口，请创建 /etc/*hostname*.vca*N* 文件，其中 *N* 是指该示例中设备 0 的例程号。如果设备例程号为 1，则文件应为 /etc/*hostname*.vca1。

   - 不要为您不想使用的 Sun Crypto Accelerator 4000 接口创建 /etc/*hostname*.vca*N* 文件。
   - /etc/*hostname*.vca*N* 文件中必须包含相应 vca 接口的主机名。
   - 主机名必须具有 IP 地址，且必须在 /etc/hosts 文件中列出。
   - 此主机名必须与其它任何接口的主机名不同，例如， /etc/*hostname*.vca0 和 /etc/*hostname*.vca1 不能共用相同的主机名。

对于配有 Sun Crypto Accelerator 4000 板（zardoz-11）的名为 zardoz 的系统而言，需要具有下面示例中的 /etc/*hostname*.vca*N* 文件。

```
# cat /etc/hostname.hme0
zardoz
# cat /etc/hostname.vca0
zardoz-11
```

3. **在 /etc/hosts 文件中为每一个活动的 vca 接口创建相应的条目。**

   例如：

```
# cat /etc/hosts
#
# Internet host table
#
127.0.0.1     localhost
129.144.10.57 zardoz    loghost
129.144.11.83 zardoz-11
```

配置 IPsec 硬件加速

该板有两种 IPsec 硬件加速配置：线内和带外。两种配置均可用于加速 IPsec 加密操作。但是，由于两种配置各自具有不同的优势，因此需对整体系统要求作出估测，以确定合适的配置。

注 – Solaris 9 和更高版本支持 IPsec 加速，Solaris 8 则不支持。只有 Solaris 9 12/03 和更高版本才支持线内 IPsec 加速 （参阅表 3-20）。

表 3-20 IPsec 加速的 Solaris 版本要求

Solaris 版本	带外加速	线内加速
所有 Solaris 8 版本	不支持	不支持
Solaris 9 至 Solaris 9 8/03	支持	不支持
Solaris 9 12/03 和更高版本	支持	支持

带外加速为默认的 IPsec 配置，最适合于在多处理器系统上执行。此配置下， DES 和 3DES 加密功能由板进行处理。对于主机处理能力强大的多处理器系统，这是首选配置。

线内 IPsec 配置通过验证支持 （MD5 和 SHA1）来增强带外功能，并将主机数据包处理负载的一部分分配给板。通过进行额外数据包处理，该板显著地减少了主机 CPU 的使用。

注 – 在只需进行 DES 或 3DES 加密算法的多处理器系统上，带外配置可能比线内配置提供更大的 IPsec 吞吐量。

启用带外 IPsec 加速

需要安装 Solaris 9 或更高版本。带外 IPsec 加速为板的默认配置。在 Solaris 9 中使用板以进行带外 IPsec 加速时，不需要配置或调整 IPsec。您只需安装 Sun Crypto Accelerator 4000 软件包然后重新引导。

启用线内 IPsec 加速

需要安装 Solaris 9 12/03 或更高版本。要配置线内加速，您必须更改 Solaris 软件和 `vca` 驱动程序中的配置文件。

▼ 启用线内 IPsec 硬件加速

1. **将以下条目添加至 `/etc/system` 配置文件，以在 Solaris 软件中启用线内加速：**

```
set ip:ip_use_dl_cap=1
```

要使 `/etc/system` 文件中的更改生效，必须重新启动系统。

2. **将以下条目添加至 `/kernel/drv/vca.conf` 配置文件，以在 `vca` 驱动程序中启用线内加速。**

```
inline-ipsec=1;
```

要使 `/kernel/drv/vca.conf` 文件中的更改生效，必须重新启动系统或重新加载 `vca` 驱动程序。

注 – 如果未在 Solaris 软件中启用线内加速，则不应在驱动程序中启用线内加速，因为这样可能会降低非 IPsec 性能。

启用线内加速后，即可执行标准 IPsec 配置过程为接口配置 Solaris 软件 IPsec 策略。有关在 Solaris 中配置 IPsec 策略的信息，请参阅 `http://docs.sun.com` 网站上的《*IPsec and IKE Administration Guide*》。

线内加速可用于加速 AH 和 ESP 算法；但是不能在板上执行多个嵌套转换 （包括 AH+ESP）。如果应用多个转换，则仅以线内方式执行最外层转换。剩余的转换将由 Solaris IPsec 配置执行。如果 Solaris 9 系统中安装了 KCL IPsec 加速 (`SUNWkcl2i.u`) 软件包，则这些转换还可在硬件中执行 （带外）。

当板配置用于 IPsec 线内加速时，将会累计由 `kstat`(1M) 命令提供的附加统计。有关 IPsec 线内加速 `kstat` 统计的说明，请参见表 3-19。

第 4 章

管理 Sun Crypto Accelerator 4000 板

本章简要介绍了如何使用 vcaadm、vcad、vcadiag 和 pk11export 实用程序来管理板。它包括以下几节：

使用 vcaadm 实用程序

vcaadm 实用程序提供了用于 Sun Crypto Accelerator 4000 板的命令行界面。只有指定为安全主管的用户才允许使用 vcaadm 实用程序。首次通过 vcaadm 连接至 Sun Crypto Accelerator 4000 板时，系统会提示您创建初始安全主管和密码。

为了便于访问 vcaadm 实用程序，请在搜索路径中指定 Sun Crypto Accelerator 4000 工具目录，例如：

```
$ PATH=$PATH:/opt/SUNWconn/bin
$ export PATH
```

vcaadm 命令行语法如下：

- vcaadm [-H]
- vcaadm [-y] [-h *hostname*] [-p *port*] [-d vca*N*] [-f *filename*]
- vcaadm [-y] [-h *hostname*] [-p *port*] [-d vca*N*] [-s *sec-officer*] *command*

注 – 使用 -d 选项时， vca*N* 是指板的设备名称，其中 *N* 表示 Sun Crypto Accelerator 4000 的设备例程号。

表 4-1 列出了 vcaadm 实用程序的选项。

表 4-1 vcaadm 选项

选项	含义
-H	显示 vcaadm 命令的帮助文件并退出。
-d vca*N*	连接至 Sun Crypto Accelerator 4000 板 （其中 *N* 表示板的驱动程序例程号）。例如，键入 -d vca1 命令可连接至设备 vca1，其中 vca 是板设备名称中的字符串， 1 是设备的例程号。该值默认为 vca0，并且必须采用 vca*N* 格式，其中 *N* 表示设备例程号。
-f *filename*	解释 *filename* 中的一个或多个命令并退出。
-h *hostname*	连接到 *hostname* 上的 Sun Crypto Accelerator 4000 板。 *hostname* 的值可以是主机名或 IP 地址，默认值为回送地址。
-p *port*	连接至 *port* 上的 Sun Crypto Accelerator 4000 板。*port* 的默认值为 6870。
-s *sec-officer*	以名为 *sec-officer* 的安全主管身份登录。
-y	对任何正常提示确认的命令强制回答 “是”。

注 – 本用户指南中，采用 *sec-officer* 作为安全主管的名称示例。

操作模式

vcaadm 可按三种模式运行。这些模式的主要差异在于命令传送给 vcaadm 的方式不同。这三种模式分别为单命令模式、文件模式和交互模式。

注 – 要使用 vcaadm，您必须进行安全主管身份验证。安全主管身份验证的频率取决于所用的操作模式。

单命令模式

在单命令模式下，对于每一个命令，您均必须进行安全主管身份验证。执行命令之后，您即会退出 vcaadm。

在单命令模式下输入命令时，您需在指定所有命令行参数之后指定要运行的命令。例如，在单命令模式下，下面的命令将显示指定密钥库中的所有用户，然后向用户返回命令 shell 提示符。

```
$ vcaadm show user
Security Officer Name: sec-officer
Security Officer Password:
```

下面的命令将作为安全主管 *sec-officer* 执行登录，并在密钥库中创建名为 *web_admin* 的用户。

```
$ vcaadm -s sec-officer create user web-admin
Security Officer Password:
Enter new user password:
Confirm password:
User web-admin created successfully.
```

注 – 第一个密码是安全主管密码，随后是新用户 *web-admin* 的密码和确认密码。

单命令模式下的所有输出都转至标准的输出流。使用基于标准 UNIX shell 的方法可以重新指定此类输出的位置。

文件模式

在文件模式下，对于所运行的每一份文件，您均必须进行安全主管身份验证。执行命令文件中的命令之后，您即会退出 vcaadm。

要在文件模式下输入命令，您需指定 vcaadm 可以从中读取一个或多个命令的文件。该文件必须为 ASCII 文本，每行包含一个命令。每条注释均以井字符 (#) 开头。如果设置了文件模式选项，则 vcaadm 会忽略最后一个选项之后的任何命令行参数。下面的示例将运行 deluser.scr 文件中的命令，并对所有提示作肯定回答：

```
$ vcaadm -f deluser.scr -y
```

交互模式

在交互模式下，您必须在每次连接至板时进行安全主管身份验证。这是 vcaadm 的默认操作模式。要在交互模式下退出 vcaadm，请使用 logout 命令。有关说明，请参阅第 56 页 “通过 vcaadm 登录和退出板”。

交互模式向用户提供一个类似于 ftp(1) 的界面。在此界面中，一次可以输入一个命令。交互模式不支持 -y 选项。

通过 vcaadm 登录和退出板

当您在命令行中运行 vcaadm 并分别用 -h、 -p 和 -d 选项指定*主机*、*端口*和*设备*时，系统会立即提示您以安全主管身份登录 （如果已成功建立网络连接）。

vcaadm 实用程序会在 vcaadm 应用程序和特定板上运行的 Sun Crypto Accelerator 4000 固件之间建立加密网络连接 （信道）。

在设置加密信道期间，板通过各自的硬件以太网地址和 RSA 公钥来识别自身。vcaadm 首次连接至板时，会创建一个信任数据库 (`$HOME/.vcaadm/trustdb`)。此文件包含安全主管当前信任的所有板。

通过 vcaadm 登录板

如果安全主管连接至一个新板， vcaadm 会通知安全主管并提示以下选项：

```
1. Abort the connection
2. Trust the connection one time only (no changes to trust
   database)
3. Trust this board forever (adds the hardware ethernet address
   and RSA public key to the trust database)
```

如果安全主管所连接的板的远程访问密钥已发生更改， vcaadm 会通知安全主管并提示以下三种选项：

```
1. Abort the connection
2. Trust the connection one time only (no changes to trust
   database)
3. Replace the old public key bound to this hardware ethernet
   address with the new public key
```

登录新板

注 – 本章以后的示例都是在 vcaadm 的交互模式下创建的。

当连接至新板时， vcaadm 必须在信任数据库中创建一个新条目。下面是登录新板的示例。

```
# vcaadm -h hostname
Warning: MAC ID and Public Key Not Found
-----------------------------------------------------
The MAC ID and public key presented by this board were
not found in your trust database.

MAC ID: 08:00:20:EE:EE:EE
Key Fingerprint: 29FC-7A54-4014-442F-7FD9-5FEA-8411-CFB4
-----------------------------------------------------
Please select an action:

1. Abort this connection
2. Trust the board for this session only
3. Trust the board for all future sessions

Your Choice -->
```

登录已更改远程访问密钥的板

当连接至已更改远程访问密钥的板时， vcaadm 必须更改信任数据库中与该板对应的条目。下面是登录已更改远程访问密钥的板的示例。

```
# vcaadm -h hostname
Warning: Public Key Conflict
-----------------------------------------------------
The public key presented by the board you are connecting
to is different than the public key that is trusted for
this MAC ID.

MAC ID: 08:00:20:EE:EE:EE
New Key Fingerprint: 29FC-7A54-4014-442F-7FD9-5FEA-8411-CFB4
Trusted Key Fingerprint: A508-38D1-FED8-8103-7ACC-0D19-C9C9-11F2
-----------------------------------------------------
Please select an action:

1. Abort this connection
2. Trust the board for this session only
3. Replace the current trusted key with the new key

Your Choice -->
```

vcaadm *提示符*

交互模式下的 vcaadm 提示符如下所示：

```
vcaadm{vcaN@hostname, sec-officer}> command
```

下表介绍了 vcaadm 提示符变量：

表 4-2 vcaadm 提示符变量定义

提示符变量	定义
vca*N*	vca 是一个表示 Sun Crypto Accelerator 4000 板的字符串。 *N* 表示设备例程号 （单元地址），位于板的设备路径名中。有关检索设备例程号的详细说明，请参阅第 35 页 “使用 vca.conf 文件设置驱动程序参数”。
hostname	Sun Crypto Accelerator 4000 板物理连接的主机的名称。*hostname* 可用物理主机的 IP 地址替换。
sec-officer	当前登录板的安全主管名。

通过 vcaadm 退出板

在交互模式下工作时，您可能想断开与一个板的连接并连接到另一个板，而并不完全退出 vcaadm。如果您要断开与一个板的连接并退出，但同时想保持交互模式，请使用 logout 命令：

```
vcaadm{vcaN@hostname, sec-officer}> logout
vcaadm>
```

注意，在上面的示例中， vcaadm> 提示符不再显示设备例程号、主机名或安全主管名。要登录另一个设备，请输入带以下可选参数的 connect 命令。

表 4-3 connect 命令可选参数

参数	含义
dev vca*N*	连接至驱动程序例程号为 *N* 的 Sun Crypto Accelerator 4000 板。例如， -d vca1 表示连接至设备 vca1 ；此参数的默认值是设备 vca0。
host *hostname*	连接至 *hostname* （默认值是回送地址）上的 Sun Crypto Accelerator 4000 板。 *hostname* 可用物理主机的 IP 地址替换。
port *port*	连接至端口 *port* （默认为 6870）上的 Sun Crypto Accelerator 4000 板。

示例：

```
vcaadm{vcaN@hostname, sec-officer}> logout
vcaadm> connect host hostname dev vca2
Security Officer Login: sec-officer
Security Officer Password:
vcaadm{vcaN@hostname, sec-officer}>
```

如果您已连接至一个 Sun Crypto Accelerator 4000 板，则 vcaadm 不允许您输入 connect 命令。您必须首先退出该板，然后才能输入 connect 命令。

每次进行新连接时， vcaadm 和目标 Sun Crypto Accelerator 4000 固件均会重新协商新的会话密钥，从而保护发送的管理数据。

通过 vcaadm 输入命令

vcaadm 实用程序的命令语言只能与 Sun Crypto Accelerator 4000 板配合使用。您可以输入命令的全部，也可以输入命令的一部分 （必须足以与其它任何命令区分开来）。例如，可以输入 sh 来代替 show，但 re 比较含糊，因为它既可以表示 reset，也可以表示 rekey。

下面的示例显示了完整输入命令字符串的情况：

```
vcaadm{vcaN@hostname, sec-officer}> show user
User                                        Status
-----------------------------------------------------
web-admin                                  enabled
Tom                                         enabled
-----------------------------------------------------
```

在上面的示例中，使用命令字符串的一部分，如 sh us，也可以获得同样的信息。

含糊不清的命令会产生解释性的响应：

```
vcaadm{vcaN@hostname, sec-officer}> re
Ambiguous command: re
```

获得命令帮助

vcaadm 内置有帮助功能。要获得帮助，您必须在想要获得更多帮助的命令后面输入问号 (?) 字符。如果已输入完整的命令，并且该命令行中的任意位置存在问号 (?)，则您会得到该命令的语法。例如：

```
vcaadm{vcaN@hostname, sec_officer}> create ?
Sub-Command                    Description
-------------------------------------------------------
so                             Create a new security officer
user                           Create a new user

vcaadm{vcaN@hostname, sec-officer}> create user ?
Usage: create user [<username>]

vcaadm{vcaN@hostname, sec-officer}> set ?
Sub-Command                    Description
-------------------------------------------------------
passreq                        Set password requirements
password                       Change an existing security officer password
timeout                        Set the auto-logout time
```

另外，您还可以在 vcaadm 提示符下输入问号，以查看所有 vcaadm 命令及其说明，例如：

```
vcaadm{vcaN@hostname, sec-officer}> ?
Sub-Command                    Description
-------------------------------------------------------
backup                         Backup master key
connect                        Begin admin session with firmware
create                         Create users and accounts
delete                         Delete users and accounts
diagnostics                    Run diagnostic tests
disable                        Disable a user
enable                         Enable a user
exit                           Exit vcaadm
loadfw                         Load new firmware
logout                         Logout current session
quit                           Exit vcaadm
rekey                          Generate new system keys
reset                          Reset the hardware
set                            Set operating parameters
show                           Show system settings
zeroize                        Delete all keys and reset board
```

不在 vcaadm 交互模式下时，问号 (?) 字符将由您当前所在的 shell 进行解译。在这种情况下，请确保在问号之前使用命令 shell 转义字符。

在交互模式下退出 vcaadm 实用程序

您可使用两个命令从 vcaadm 退出：quit 和 exit。此外，也可使用 Ctrl-D 组合键从 vcaadm 退出。

通过 vcaadm 初始化板

配置 Sun Crypto Accelerator 4000 板的第一个步骤就是对其进行初始化。初始化板时，需要创建密钥库。（参阅第 96 页 “概念和术语”。）首次通过 vcaadm 连接至 Sun Crypto Accelerator 4000 板时，系统会提示您是将板初始化为使用新密钥库，还是使用那些存储在备份文件中的现有密钥库。 vcaadm 会提示您输入任何一种板初始化类型的所有必要信息。

▼ 初始化板以使用新密钥库

1. **在安装板的系统的命令提示符下，输入** vcaadm**，或者输入** vcaadm -h *hostname* **（如果系统为远程系统），然后选择 1 以初始化板：**

```
# vcaadm -h hostname
Please select an action:

1. Abort this connection
2. Trust the board for this session only.
3. Replace the current trusted key with the new key.

Your Choice --> 2
This board is uninitialized.
You will now initialize the board. You may either
completely initialize the board and start with a new
keystore or initialize the board to use an existing
keystore, providing a backup file in the process.

1. Initialize the board with a new keystore
2. Initialize the board to use an existing keystore

Your Choice (0 to exit) --> 1
```

2. **创建密钥库名 （参阅第 65 页 “命名要求”）：**

```
Keystore Name: keystore-name
```

3. **选择 FIPS 140-2 模式或非 FIPS 模式。**

   当处于 FIPS 模式时，板与 FIPS 140-2，level 3 兼容。 FIPS 140-2 是一种联邦信息处理标准，用于防止篡改数据，并实现高级的数据完整性和安全性能。有关说明，请参阅以下网址提供的 FIPS 140-2 文档：
   http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

```
Run in FIPS 140-2 mode? (Y/Yes/N/No) [No]: y
```

4. **创建初始安全主管名和密码 （参阅第 65 页 “命名要求”）：**

```
Initial Security Officer Name: sec_officer
Initial Security Officer Password:
Confirm Password:
```

注 – 更改或删除基本参数之前，或在执行可导致严重后果的命令之前， vcaadm 会提示您输入 Y、 Yes、 N 或 No 进行确认。这些值不区分大小写；默认值为 No。

---

5. **验证配置信息：**

```
Board initialization parameters:
-----------------------------------------------------
Initial Security Officer Name: sec_officer
Keystore Name: keystore-name
Run in FIPS 140-2 Mode: Yes
-----------------------------------------------------

Is this correct? (Y/Yes/N/No) [No]: y
Initializing crypto accelerator board... This may take a few
minutes...Done.
```

初始化板以使用现有的密钥库

如果要将多个板添加至单个密钥库，则可能需要初始化所有板，以便使用相同的密钥库信息。另外，您也可能想将 Sun Crypto Accelerator 4000 板恢复至原来的密钥库配置。本节介绍如何初始化板，以使用保存在备份文件中的现有密钥库。

执行本过程之前，必须先创建一个包含现有板配置信息的备份文件。创建和恢复备份文件时，必须提供密码才能加密和解密备份文件中的数据。（参阅第 70 页“备份主密钥”。）

▼ 初始化板以使用现有的密钥库

1. **从安装 Sun Crypto Accelerator 4000 板的系统的命令提示符下输入** `vcaadm`，**或输入** `vcaadm -h` *hostname*（**如果系统为远程系统），然后选择 2 以使用备份文件中的现有密钥库：**

```
# vcaadm -h hostname
This board is uninitialized.
You will now initialize the board.  You may
either completely initialize the board and
start with a new keystore or restore the board
using a backup file.

1. Initialize the board with a new keystore
2. Initialize the board to use an existing keystore

Your Choice (0 to exit) --> 2
```

2. **输入备份文件的路径和密码：**

```
Enter the path to the backup file: /tmp/board-backup
Password for restore file:
```

3. **验证配置信息：**

```
Board restore parameters:
-----------------------------------------------------
Path to backup file: /tmp/board-backup
Keystore Name: keystore-name
-----------------------------------------------------

Is this correct? (Y/Yes/N/No) [No]: y
Restoring data to crypto accelerator board...
```

通过 vcaadm 管理密钥库

密钥库是密钥资料的储存库。与密钥库信息密切相关的是安全主管和用户。密钥库不但可以存储密钥，而且还是用户帐户拥有密钥对象的一种方式。它可以使那些未通过所有者身份验证的应用程序无法看到密钥。密钥库由三部分组成：

- **密钥对象** – 为应用程序 （如 Sun ONE Web Server）保存的长期密钥。
- **用户帐户** – 这些帐户可使应用程序验证和访问特定的密钥。
- **安全主管帐户** – 这些帐户可通过 vcaadm 访问密钥管理功能。

注 – 每个 Sun Crypto Accelerator 4000 板只能有一个密钥库。不过，多个板可配置为共用同一个密钥库，以便提供额外的性能和容错功能。

命名要求

安全主管名、用户名和密钥库名必须符合以下要求：

表 4-4 安全主管名、用户名和密钥库名要求

名称要求	说明
最小长度	至少一个字符
最大长度	用户名 63 个字符，密钥库名 32 个字符
有效字符	字母数字、下划线 (_)、连字号 (-) 和圆点 (.)
第一个字符	必须是字母

密码要求

密码要求因当前的 set passreq 设置 （low、 med 或 high）而异。

设置密码要求

使用 `set passreq` 命令可设置 Sun Crypto Accelerator 4000 板的密码要求。对于 `vcaadm` 要求输入的任何密码，均可使用此命令来设置这些密码的字符要求。密码要求有三种设置，如下表所示：

表 4-5 密码要求设置

密码设置	要求
`low`	不需要任何密码限制。这是板处于非 FIPS 模式时的默认设置。
`med`	要求最少六个字符：其中三个字符必须是字母字符，一个字符必须是非字母字符。这是板处于 FIPS 140-2 模式时的默认设置，并且也是 FIPS 140-2 模式下所允许的最低密码要求。
`high`	要求最少八个字符：其中三个字符必须是字母字符，一个字符必须是非字母字符。这不是默认设置，必须进行手动配置。

要更改密码要求，请输入 `set passreq` 命令，并在后面附上 `low`、`med` 或 `high` 选项。以下命令用于将 Sun Crypto Accelerator 4000 板的密码要求设为 `high`：

```
vcaadm{vcaN@hostname, sec-officer}> set passreq high

vcaadm{vcaN@hostname, sec-officer}> set passreq
Password security level (low/med/high): high
```

向密钥库中添加安全主管

一个密钥库可能有多个安全主管。安全主管名只能在 Sun Crypto Accelerator 4000 板的域中被识别，且不必与主机系统上的用户名相同。

创建安全主管时，安全主管名是命令行的可选参数。如果未输入安全主管名，`vcaadm` 会提示您输入。（参阅第 65 页 “命名要求”。）

```
vcaadm{vcaN@hostname, sec-officer}> create so Alice
Enter new security officer password:
Confirm password:
Security Officer Alice created successfully.

vcaadm{vcaN@hostname, sec-officer}> create so
New security officer name: Bob
Enter new security officer password:
Confirm password:
Security Officer Bob created successfully.
```

向密钥库中添加用户

这些用户名仅在 Sun Crypto Accelerator 4000 板的域中被识别，而且不必与 Web 服务器进程的 UNIX 用户名相同。

创建用户时，用户名是命令行的可选参数。如果未输入用户名，vcaadm 会提示您输入。（参阅第 65 页 “命名要求”。）

```
vcaadm{vcaN@hostname, sec-officer}> create user web-admin
Enter new user password:
Confirm password:
User web-admin created successfully.

vcaadm{vcaN@hostname, sec-officer}> create user
New user name: Tom
Enter new user password:
Confirm password:
User Tom created successfully.
```

在 Web 服务器启动期间进行验证时，用户必须使用此密码。

注意 – 用户必须记住密码才能访问自己的密钥。丢失的密码无法找回。

注 – 如果在五分钟之内未输入任何命令，用户帐户会被注销。这是一个可调选项。有关详情，请参阅第 71 页 “设置自动注销时间”。

列出用户和安全主管

要列出与密钥库相关的用户或安全主管，请输入 `show user` 或 `show so` 命令。

```
vcaadm{vcaN@hostname, sec-officer}> show user
User                                          Status
------------------------------------------------------
web-admin                                     Enabled
Tom                                           Enabled
------------------------------------------------------


vcaadm{vcaN@hostname, sec-officer}> show so
Security Officer
------------------------------------------------------
sec-officer
Alice
Bob
------------------------------------------------------
```

更改密码

只有安全主管密码才可以通过 `vcaadm` 更改。安全主管可更改自己的密码。使用 `set password` 命令可更改安全主管密码。

```
vcaadm{vcaN@hostname, sec-officer}> set password
Enter new security officer password:
Confirm password:
Security Officer password has been set.
```

通过 PKCS#11 界面，可运行 Sun ONE Web Server `modutil` 实用程序来更改用户密码。有关详细信息，请参阅 Sun ONE Web Server 文档。

启用或禁用用户

注 – 安全主管不能被禁用。一旦创建安全主管，它即会启用，除非将其删除。

默认情况下，创建的每个用户的状态均为 “启用”。用户可以被禁用。用户被禁用后，将不能通过 PKCS#11 界面访问其密钥资料。已禁用的用户在重新启用之后可以重新访问自身的所有密钥资料。

启用或禁用用户时，用户名是命令行的可选参数。如果未输入用户名， vcaadm 会提示您输入。

```
vcaadm{vcaN@hostname, sec-officer}> disable user Tom
User Tom disabled.
vcaadm{vcaN@hostname, sec-officer}> disable user
User name: web-admin
User web-admin disabled.
```

要禁用用户帐户，请输入 disable user 命令。

要启用用户帐户，请输入 enable user 命令。

```
vcaadm{vcaN@hostname, sec-officer}> enable user Tom
User Tom enabled.

vcaadm{vcaN@hostname, sec-officer}> enable user
User name: web-admin
User web-admin enabled.
```

删除用户

输入 delete user 命令并指定要删除的用户。删除用户时，用户名是命令行的可选参数。如果未输入用户名， vcaadm 会提示您输入。

```
vcaadm{vcaN@hostname, sec-officer}> delete user web-admin
Delete user web-admin? (Y/Yes/N/No) [No]: y
User web-admin deleted successfully.

vcaadm{vcaN@hostname, sec-officer}> delete user
User name: Tom
Delete user Tom? (Y/Yes/N/No) [No]: y
User Tom deleted successfully.
```

删除安全主管

输入 `delete so` 命令并指定要删除的安全主管。删除安全主管时，安全主管名是命令行的可选参数。如果未输入安全主管名， `vcaadm` 会提示您输入。

```
vcaadm{vcaN@hostname, sec-officer}> delete so Bob
Delete Security Officer Bob? (Y/Yes/N/No) [No]: y
Security Officer Bob deleted.

vcaadm{vcaN@hostname, sec-officer}> delete so
Security Officer name: Alice
Delete Security Officer Alice? (Y/Yes/N/No) [No]: y
Security Officer Alice deleted.
```

备份主密钥

密钥库保存在磁盘上，并已使用主密钥进行了加密。该主密钥保存在 Sun Crypto Accelerator 4000 固件中，可由安全主管加以备份。

要备份主密钥，请使用 `backup` 命令。 `backup` 命令将要求您输入用于保存备份文件的路径名。该路径名可以在命令行中输入，如果未输入， `vcaadm` 会提示您输入路径名。

您必须为备份数据设置密码。该密码用于加密备份文件中的主密钥。

```
vcaadm{vcaN@hostname, sec-officer}> backup /opt/SUNWconn/vca/backups/bkup.data
Enter a password to protect the data:
Confirm password:
Backup to /opt/SUNWconn/vca/backups/bkup.data successful.
```

注意 – 制作备份文件时，请选择难以猜测的密码，因为此密码用于保护密钥库的主密钥。同时，您必须牢记输入的密码。没有密码，就无法访问主密钥备份文件。一旦遗忘，将无法恢复由密码保护的数据。

锁定密钥库以防止备份

某些站点可能具有严格的安全策略，不允许 Sun Crypto Accelerator 4000 板的主密钥离开硬件。您可以使用 `set lock` 命令来强制实施这一防范措施。

注意 – 输入此命令之后，所有备份主密钥的尝试都将失败。即使主密钥被重新设置，此锁定仍会保持不变。清除此设置的唯一方法是使用 `zeroize` 命令零置化 Sun Crypto Accelerator 4000 板。（参阅第 74 页 “在板上执行软件零置”。）

```
vcaadm{vcaN@hostname, sec-officer}> set lock
WARNING: Issuing this command will lock the
         master key.  You will be unable to back
         up your master key once this command
         is issued.  Once set, the only way to
         remove this lock is to zeroize the board.
Do you wish to lock the master key? (Y/Yes/N/No) [No]: y
The master key is now locked.
```

通过 vcaadm 管理板

本节介绍如何通过 `vcaadm` 实用程序来管理 Sun Crypto Accelerator 4000 板。

设置自动注销时间

`set timeout` 命令用于自定义板注销安全主管的时间。要更改自动注销时间，请输入 `set timeout` 命令，然后输入板在自动注销安全主管之前所等待的分钟数。 0 值表示禁用自动注销功能。最大延迟时间是 1,440 分钟 （即 1 天）。新初始化的板的默认值为 5 分钟。

下面的命令可将安全主管的自动注销时间改为 10 分钟。

```
vcaadm{vcaN@hostname, sec-officer}> set timeout 10
```

显示板状态

要获取 Sun Crypto Accelerator 4000 板的当前状态，请输入 `show status` 命令。此命令可以显示板的硬件和固件版本、网络接口的 MAC 地址、网络接口的状态 （启动或关闭、速度、双工等）以及密钥库名和 ID。

```
vcaadm{vcaN@hostname, sec-officer}> show status
Board Status
----------------------------------------------------------------
Hardware Version: 1.0
Firmware Version: 1.0
Bootstrap Firmware Version: VCA Crypto Accelerator 1.0  March 2003
Current Firmware Version: VCA Crypto Accelerator 1.0  March 2003
MAC Address: 00:03:ba:0e:96:aa
Interface information: Link up, 1000Mbps, Full Duplex
Keystore Name: keystore-name
Keystore ID: 832aece03e654790
Login Session Timeout (in minutes): 10
Password policy security level: HIGH
Number of master key backups: 0
* Device is in FIPS 140-2 Mode
----------------------------------------------------------------
```

确定板是否在 FIPS 140-2 模式下操作

如果 Sun Crypto Accelerator 4000 板正在 FIPS 140-2 模式下操作， `show status` 命令会输出下面的信息行：

```
* Device is in FIPS 140-2 Mode
```

如果板不在 FIPS 140-2 模式下操作，则 `show status` 命令不会输出指示 FIPS 140-2 模式的信息行。

另外，您也可以使用 `kstat`(1M) 实用程序来确定板是否在 FIPS 140-2 模式下操作。如果板正在 FIPS 140-2 模式下操作，`kstat`(1M) 参数 `vs-mode` 的返回值将是 `FIPS`。有关 `kstat`(1M)，请参阅第 39 页 “加密和以太网驱动程序操作统计”和联机手册页。

加载新固件

添加新功能时，可以更新 Sun Crypto Accelerator 4000 板的固件。要加载固件，请输入 `loadfw` 命令并提供固件文件的路径。

为了成功更新固件，必须使用 `reset` 命令对板进行手动重新设置。重新设置板时，当前登录的安全主管会被注销。

```
vcaadm{vcaN@hostname, sec-officer}> loadfw /opt/SUNWconn/cryptov2/firmware/sca4000fw
Security Officer Login: sec-officer
Security Officer Password:
WARNING: This command will load new firmware onto the
          the target device.  You must issue a reset
          command and log back into the target device in
          order to use the new firmware.

Proceed with firmware update? (Y/Yes/N/No) [No]: y
```

重新设置板

某些情况下，可能需要重新设置板。要重新设置板，您必须运行 `reset` 命令。系统会询问您是否确实要重新设置板。重新设置 Sun Crypto Accelerator 4000 板会暂时停止加速系统上的加密过程，除非该板的任务可由其它活动的 Sun Crypto Accelerator 4000 板接管。同时，该命令还会使您自动退出 `vcaadm`。因此，如果您要继续管理板，必须重新登录 `vcaadm` 以重新连接至设备。

```
vcaadm{vcaN@hostname, sec-officer}> reset
WARNING: Issuing this command will reset the
         the board and close this connection.

Proceed with reset? (Y/Yes/N/No) [No]: y
Reset successful.
```

重新设置板的密钥

如果安全策略发生变化，您或许想使用新的密钥作为主密钥或远程访问密钥。 `rekey` 命令用于重新生成其中任何一个密钥，或者重新生成这两个密钥。

重新设置主密钥还会导致在新密钥下重新加密密钥库，且会使旧的备份主密钥文件失效而启用新的密钥库文件。重新设置主密钥时，应制作主密钥的备份。如果多个 Sun Crypto Accelerator 4000 板使用相同的密钥库，则需备份新的主密钥，然后将其恢复至其它板。

重新设置远程访问密钥会注销安全主管，并强制使用新远程访问密钥进行新的连接。

运行 rekey 命令时，您可以指定以下三种密钥类型之一：

表 4-6 密钥类型

密钥类型	操作
master	重新设置主密钥。
remote	重新设置远程访问密钥。注销安全主管。
all	重新设置主密钥和远程访问密钥。

以下是输入 rekey 命令和 all 密钥类型的示例：

```
vcaadm{vcaN@hostname, sec-officer}> rekey

Key type (master/remote/all): all
WARNING: Rekeying the master key will render all old board backups
         useless with the new keystore file. If other boards use this
         keystore, they will need to have this new key backed up and
         restored to those boards. Rekeying the remote access key will
         terminate this session and force you to log in again.

Rekey board? (Y/Yes/N/No) [No]: y
Rekey of master key successful.
Rekey of remote access key successful.  Logging out.
```

在板上执行软件零置

清除板上所有的密钥资料有两种方法。第一种方法是使用硬件跳线 （分路）；这种零置方法可使板恢复至其原始出厂状态 （Failsafe 模式）。（参阅第 237 页 “将 Sun Crypto Accelerator 4000 硬件零置为原始出厂状态”。）第二种方法是使用 zeroize 命令。

注 – zeroize 命令会删除密钥资料，并保持所有更新的固件完好无损。此命令在成功完成时还会注销安全主管。

要使用 zeroize 命令在板上执行软件零置，请输入命令并确认：

```
vcaadm{vcaN@hostname, sec-officer}> zeroize
WARNING: Issuing this command will zeroize all keys
         on the board.  Once zeroized, these keys
         cannot be recovered unless you have
         previously backed up your master key.

Proceed with zeroize? (Y/Yes/N/No) [No]: y
All keys zeroized successfully.
```

使用 vcaadm diagnostics 命令

可通过 vcaadm 实用程序和 SunVTS 软件对板执行诊断。vcaadm 中的 diagnostics 命令涉及 Sun Crypto Accelerator 4000 硬件中的三个主要类别：一般硬件、加密子系统和网络子系统。一般硬件的测试包括 DRAM、闪存、 PCI 总线、 DMA 控制器和其它内部硬件。加密子系统的测试包括随机号码发生器和加密加速器。网络子系统的测试包括 vca 设备。

```
vcaadm{vcaN@hostname, sec-officer}> diagnostics
Performing diagnostic tests...Done.
Diagnostic Results
-----------------------------------------------------
General Hardware:                PASS
Cryptographic Subsystem:         PASS
Network Subsystem:               PASS
-----------------------------------------------------
```

使用 vcad 命令

vcad 命令可配置和启动 vcad 守护程序，以便为 vcaadm(1M) 和其它加密应用程序提供加密密钥库服务。此外，vcad 守护程序还可为驱动程序和硬件读取/写入密钥库数据。

为了便于访问 vcad 命令，请在搜索路径中指定 Sun Crypto Accelerator 4000 工具目录，例如：

```
$ PATH=$PATH:/opt/SUNWconn/cryptov2/sbin/
$ export PATH
```

vcad 命令的命令行语法如下所示：

```
/opt/SUNWconn/cryptov2/sbin/vcad [-dFlV] [-f config-file]
[-h host-address] [-k keystore-dir] [-L logfile] [-p port] [-s max-size]
[-t seconds][-u username]
```

表 4-7 介绍了 vcad 命令支持的选项。

表 4-7 vcad 命令选项

选项	说明
-d	启动调试。每则消息除了包含自身的实际消息外，还包含 vcad 的进程 ID、当前线程 ID 和消息类别。多个 -d 选项会增加详细程度 （最高为 2）。使用多个 -d 选项时，单个 -d 相当于将配置文件中的 DebugLevel 参数设为 “INFO”， -dd 则相当于将该参数设为 “DEBUG”。
-f *config-file*	指定配置文件的位置。此配置文件的默认位置为：/etc/opt/SUNWconn/vca/vcad.conf。如果使用此选项但不能打开文件，则 vcad 不会启动。
-F	在前台执行 vcad 并将日志输出发送至 stderr。此操作会覆盖通过 -L 标志选定的 *logfile* （日志文件）。
-h *host-address*	为 vcad 指定要连接的主机 IPv4 或 IPv6 地址，并监听进入的连接。可以用附加的 -h 选项来指定多个主机或 IP 地址。如果不使用此选项，则 vcad 的默认操作为：监听用于进入连接的所有可用接口。当指定特定主机或 IP 地址以进行连接时，只能在回应这些地址和 localhost 的接口上建立连接。通过 -h 标志指定的任何地址或主机将由 -l 选项覆盖。
-k *keystore-dir*	将 *keystore-dir* 用作所有密钥库数据的目录。如果守护程序作为非超级用户运行，则该用户必须能够读写此目录，犹如读写密钥库数据文件一样。密钥库数据的默认目录为：/etc/opt/SUNWconn/vca/keydata。
-l	只接受源自本地主机的管理客户机发出的进入连接。此选项会覆盖任何使守护程序监听其它任何接口的命令行或 .conf 文件指令。
-L *logfile*	将日志输出发送到 *logfile*，而不是系统日志的标准位置。
-p *port*	指定用于接收进入连接的 *port*。默认端口为 6870。
-s *max-size*	使向下传送至 Sun Crypto Accelerator 的命令的最大数据长度为 *max-size* 字节。使用此选项，管理员可防止在单命令中通过内核向下传送大量数据。单命令的默认最大值为 4 MB （4194304 字节）。

表 4-7 vcad 命令选项 *（续）*

选项	说明
-t *seconds*	设定秒数，作为 vcad 停止接受来自客户机的数据之前要等待的*秒*数。如果此计时器到期，则 vcad 与客户机之间的连接会关闭。
-u *username*	以 *username* 身份执行 vcad。如果未指定用户名，则 vcad 尝试作为启动 vcad 的用户运行。如果已指定用户名，但在系统上找不到该用户名，则 vcad 不会启动。如果 vcad 作为超级用户或用户 ID 为 0 的任何其它帐户运行，则 vcad 会发出警告。有关以非超级用户身份运行 vacd 的建议，请参阅第 78 页 “vcad 守护程序的安全性能”。
-V	显示 vcad 的版本信息。

vcad 配置文件

vcad 守护程序从配置文件中获取操作参数。默认情况下，守护程序在 /etc/opt/SUNWconn/vca/vcad.conf 目录下寻找此配置文件，尽管在调用 vcad 守护程序时，可能以 vcad 命令的 -f 标志指定了其它文件。如果未使用 -f 标志，或者无法找到或读取默认的配置文件，则 vcad 守护程序会尝试使用所有默认值进行启动。在此情况下，一则警告消息会发送至标准错误输出文件中。

在配置文件中，每行包含一个指令。每个指令必须附有值。可以使用注释，但必须以井字符 (#) 开头。指令名不区分大小写，但其值可能区分大小写。有关更多详情，请参阅表 4-8 中各个指令的说明。

使用同一操作参数的命令行选项可替代配置文件中的指令。例如，您可以用 -p 选项替代配置文件中的 “Port” 指令。未使用命令行选项或配置文件指令指定的操作参数将使用内置的默认值。表 4-8 介绍了 vcad 命令支持的命令行指令。

表 4-8 vcad 命令的命令行指令

指令	说明
DebugLevel *level*	可使用户在配置文件中设定三种调试级别之一。这三种级别按详细程度从低到高分别为 Notice、 Info 和 Debug。 Notice 级别为默认值。
HostBind *host/IP*	告知 vcad 连接并监听指定的 IPv4 或 IPv6 地址，或主机解析的 IP 地址。使用多个 HostBind 指令可使 vcad 监听多个地址。如果配置文件中无 HostBind 条目，则默认操作为监听所有用于连接的接口。请注意， -l 命令行标志可替代所有 HostBind 条目。
KeyStoreDir *directory*	可使管理员选择另一目录以存储密钥库文件。运行 vcad 的用户必须对此目录具有读写权限 （参阅 User 指令）。密钥库目录的默认位置为：/etc/opt/SUNWconn/vca/keydata。

表 4-8 vcad 命令的命令行指令 *（续）*

指令	说明
`LogFile` *logfile*	使用 *logfile* 作为所有日志数据的写入位置。默认情况下，日志数据写入 syslog 文件中。如果已使用 `-F`（前台运行）命令行标志，则会忽略此指令并将 vcad 日志数据发送至标准错误输出设备。
`MaxData` *size*	设置允许在单命令中发送的最大数据量，即 size 字节。默认情况下，此值为 4 MB（4194304 字节）。如果所发送的数据超过此值，则 vcad 会向客户机返回错误并关闭连接。
`Port` *port*	设置监听端口。 vcad 监听的默认端口为 6870。如果管理员想让 vcad 监听特权端口（通常为低于 1024 的端口），则 vcad 必须作为具有超级用户权限的用户运行。有关安全的注意事项，请参阅第 78 页 “vcad 守护程序的安全性能”。
`Timeout` *seconds*	允许管理员设置命令数据在被接收首个字节之后的超时值。此超时值可防止延迟的读取操作锁定对特定卡的访问。如果 vcad 正在等待某一连接的客户机发送新命令，则此超时对其不适用。固件超时值包含此情况。（参阅第 71 页 “设置自动注销时间”。）默认超时值为 300 秒（即五分钟）。
`User` *username*	设置 vcad 使其作为 username（用户名）运行。守护程序会尝试将其真正的用户 ID 设为与此用户名关联的 UID。此指令的默认值为启动 vcad 进程的用户。

vcad 守护程序的安全性能

由于 vcad 守护程序需要监听 TCP 端口，因此应考虑采用某些安全措施。

运行 vcad 时，应以不具备超级用户权限的用户 ID 身份（即非 `UID0` 帐户）来运行此进程。您不可直接从网络上登录此用户帐户。此帐户不应设密码或锁定密码和登录 shell。在 `/etc/shadow` 文件中，此帐户的条目应具有 `NP` 或 `*LK*`。

默认情况下， vcad 守护程序将尝试作为守护程序用户帐户启动。即使禁用该帐户，vcad 守护程序仍将正常启动，但该帐户必须存在于系统中。执行以下步骤，手动配置 vcad，可使其以不同的用户名来运行。

▼ 配置 vcad 守护程序使其以不同的用户名运行

1. **配置对 /dev/vcactl 的读/写访问。**

   vcad 守护程序直接与 /dev/vcactl 进行通信，以传递命令数据并从 Sun Crypto Accelerator 4000 固件获取密钥库 I/O 命令。您应设置访问权限和所有权，使得只有 vcad 采用其身份运行的用户帐户可读写 /dev/vcactl。默认情况下，会添加 vcactl 模块，从而只允许具有所有者读写许可权限的守护程序拥有小节点。更改这些许可权限最安全的方法是使用 rem_drv(1m) 和 add_drv(1m) 重新注册 vcactl 模块：

```
rem_drvvcactl
add_drv-m '* MODE USERGROUP' vcactl
```

   USER 和 GROUP 占位符应包含设备小节点所需的用户和组所有权。 MODE 为设备小节点的文件模式。 0600 为 vcactl 模块的建议模式。有关详情，请参阅 add_drv(1m) 手册页。

2. **配置对密钥库的读/写访问权限。**

   要使 vcad 守护程序能够执行密钥库 I/O 操作，它必须能够访问在其配置中指定的密钥库目录。只有 vcad 采用其身份运行的用户帐户才应具有对密钥库目录的读写和执行权限。此目录中密钥库文件的读写权限应仅授予该用户。

3. **在非特权 TCP 端口上运行 vcad 守护程序。**

   如果 vcad 守护程序在没有超级用户权限的情况下运行，则它不能绑定到特权端口。通常，非特权端口的值为 1024 和更高。如果给定系统上的端口值不是 1024，可用 ndd 来确定 tcp_smallest_nonpriv_port 参数的值。默认情况下， vcad 守护程序使用端口 6870。

示例

示例 1：启动 vcad 守护程序以监听端口 5525。

```
# /opt/SUNWconn/cryptov2/sbin/vcad -p 5525
```

示例 2：启动 vcad 守护程序，使其显示详细调试信息并将信息发送至屏幕。

```
# /opt/SUNWconn/cryptov2/sbin/vcad -Fdd
```

此启动方法在启动时生成下列输出：

```
vcad[1679/1]: [debug] got exclusive lock
vcad[1679/1]: [info] Security daemon starting up
vcad[1679/1]: [debug] Starting file handling thread
vcad[1679/1]: [debug] Starting TCPserver
vcad[1679/1]: [debug] TCP socket bound on port 6870
vcad[1679/1]: [debug] fd is 6
```

在启用两个级别调试输出的情况下运行时，vcad 守护程序还会提供有关何时打开和关闭新连接的通知。

示例 3：启动 vcad 守护程序并使用另一配置文件。

```
# /opt/SUNWconn/cryptov2/sbin/vcad -f /etc/opt/SUNWconn/vca/alt-vcad.conf
```

使用 vcadiag 实用程序

vcadiag 实用程序提供了用于 Sun Crypto Accelerator 4000 板的命令行界面。通过此界面，超级用户无需进行安全主管身份验证即可执行管理任务。命令行选项决定 vcadiag 所执行的操作。

为了便于访问 vcadiag 实用程序，请在搜索路径中指定 Sun Crypto Accelerator 4000 工具目录，例如：

```
$ PATH=$PATH:/opt/SUNWconn/bin
$ export PATH
```

vcadiag 命令行语法如下：

- vcadiag [-D] vca*N*
- vcadiag [-F] vca*N*
- vcadiag [-K] vca*N*
- vcadiag [-Q]
- vcadiag [-R] vca*N*
- vcadiag [-Z] vca*N*

注 – 当使用 [-DFKRZ] 选项时， vca*N* 表示板的设备名称，其中 *N* 表示 Sun Crypto Accelerator 4000 的设备例程号。

表 4-9 介绍了 vcadiag 实用程序支持的选项。

表 4-9 vcadiag 选项

选项	含义
-D vca*N*	在 Sun Crypto Accelerator 4000 板上执行诊断程序。
-F vca*N*	显示 Sun Crypto Accelerator 4000 板为保证管理会话的安全而采用的公钥指纹。
-K vca*N*	显示 Sun Crypto Accelerator 4000 板为保证管理会话的安全而采用的公钥和公钥指纹。
-Q	提供 Sun Crypto Accelerator 4000 设备和软件组件的有关信息。输出是由冒号隔开的一组信息： • 设备 • 内部功能 • 密钥库名 • 密钥库序列号 • 密钥库参考计数 您可以使用此选项确定设备和密钥库之间的关联。
-R vca*N*	重新设置板。
-Z vca*N*	将板置零。

下面是使用 -D 选项的示例：

```
# vcadiag -D vca0
Running vca0 on-board diagnostics.
Diagnostics on vca0 PASSED.
```

下面是使用 -F 选项的示例：

```
# vcadiag -F vca0
5f26-b516-83b4-d254-a75f-c70d-0544-4de6
```

下面是使用 -K 选项的示例：

```
# vcadiag -K vca0
Device: vca0
Key Length: 1024 bits
Key Fingerprint: 5f26-b516-83b4-d254-a75f-c70d-0544-4de6
Modulus:
        b7215a99 8bb0dfe9 389363a0 44dac2b0 7c884161
        20ee8c8b d751437d 4e6a5cdb 76fdcb2a ad353c0b
        248edc1d 3c76591d dbca5997 f6ee8022 e8bb5a6d
        465a4f8c 601d46be 573e8681 506e5d8d f240a0db
        11d5c095 2d237061 df27b2de c353900f f531092b
        7d9a755b c5d79782 95a1180b e17303bb aca939ef
        006c73f7 74469031
Public Exponent:
        00010001
```

下面是使用 -Q 选项的示例：

```
# vcadiag -Q
vca0:cb
vca0:cb:keystore-name:83097c2b3e35ef5b:1
vca0:ca
vca0:ca:keystore-name:83097c2b3e35ef5b:1
kcl2pseudo
vca0:om
vca0:om:keystore-name:83097c2b3e35ef5b:1
libkcl
```

下面是使用 -R 选项的示例：

```
# vcadiag -R vca0
Resetting device vca0, this may take a minute.
Please be patient.
Device vca0 reset ok.
```

下面是使用 -Z 选项的示例：

```
# vcadiag -Z vca0
Zeroizing device vca0, this may take a few minutes.
Please be patient.
Device vca0 zeroized.
```

使用 pk11export 实用程序

pk11export 实用程序用于从密钥数据库中抽取密钥和证书，并将它们变成 PKCS#12 可导入格式。此实用程序要求使用 PKCS#11 界面来抽取对象，并将密钥和证书置于 PKCS#12 文件中。一次只可抽取一个密钥和证书对。

如果此界面包含在动态程序库中，则此实用程序将使用不同的 PKCS#11 提供程序。当满足以下要求， pk11export 实用程序通过 PKCS#11 提供程序导出密钥：

- PKCS#11 界面必须实施 C_WrapKey PKCS#11 功能。
- PKCS#11 界面必须实施 CKM_DES3_CBC_PAD 和 CKM_SHA_1 PKCS#11 机制。
- 要导出的密钥必须设置了 CKA_EXTRACTABLE 属性。

pk11export 的命令行语法如下：

- /opt/SUNWconn/cryptov2/bin/pk11export -V
- /opt/SUNWconn/cryptov2/bin/pk11export -l [-p *pkcs11-lib*]
- /opt/SUNWconn/cryptov2/bin/pk11export [-n *friendly-name*] [-o *filename*] [-p *pkcs11-lib*] *token-name*

表 4-10 介绍了 pk11export 实用程序支持的选项。

表 4-10 pk11export 选项

选项	说明
-l	列出给定 PKCS#11 程序库可识别的所有可用令牌。
-n *friendly-name*	指定要导出的密钥和证书对。*friendly-name* 为字符串值。
-o *filename*	将生成的 PKCS#12 文件放入 *filename* 文件中。如果未指定输出 *filename*，则 PKCS#12 文件将放入当前目录中，并命名为 pkcs12file。
-p *pkcs11-lib*	指定要从中抽取密钥和证书的 PKCS#11 程序库。此选项要求在 *pkcs11-lib* 变量中提供动态程序库的完整路径。默认情况下，pk11export 使用 Sun Crypto Accelerator 1000 PKCS#11 程序库 (/opt/SUNWconn/crypto/lib/libpkcs11.so)。不过，您可以使用此选项中的 *pkcs11-lib* 变量来指定任何 PKCS#11 程序库。
-V	显示 pk11export 的版本信息。

示例

示例 1：列出用于执行 PKCS#11 的令牌。

```
# pk11export -l -p /opt/SUNWconn/cryptov2/bin/libvpkcs11.so
0. SUNW acceleration only
1. arf
```

示例 2：从 PKCS#11 令牌 `nobody@webserv` 中导出 `Server-Cert` 证书并放入 `/tmp/webserv-export.p12` 文件中。

```
example% pk11export -o /tmp/webserv-export.p12 nobody@webserv
Enter password for nobody@webserv:
Enter password for PKCS12 file:
Enter password for PKCS12 file:
/tmp/webserv-export.p12 was created successfully
```

使用 iplssl cfg 脚本

`iplssl cfg` 脚本的选项 1 和 2 用于安装模块，以便配置板并将其注册到 Sun ONE Web 和 Application Server 软件。脚本的选项 3 和 4 分别用于将 Sun ONE Web Server 密钥导出为 PKCS#12 格式，或从 PKCS#12 格式导入 Sun ONE Web Server。

▼ 为 Sun ONE Web Server 4.1 选择 iplssl cfg 脚本的选项 1

- **有关说明，请参阅第 104 页 “配置 Sun ONE Web Server 4.1”。**

▼ 为 Sun ONE Web Server 6.0 选择 iplssl cfg 脚本的选项 1

- **有关说明，请参阅第 114 页 “配置 Sun ONE Web Server 6.0”。**

▼ 使用 iplsslcfg 脚本的选项 2

1. **键入以下命令执行 iplsslcfg 脚本：**

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

2. **键入 2 以选择 Sun ONE Application Server 并输入二进制文件路径和域路径。**

```
Sun Crypto Accelerator Sun ONE Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

Your selection (0 to quit): 2

You will now be prompted for four pieces of information:
 1. The location of the Sun ONE Application Server binaries
 2. The location where Sun ONE Server domains are stored
 3. The Application Server domain (e.g. domain1)
 4. The Application Server server name (e.g. server1)

Full path to Application Server binaries: [/opt/SUNWappserver7]:
/opt/SUNWappserver7
Full path to Application Server domains: [/var/opt/SUNWappserver7]:
/var/opt/SUNWappserver7
Application Server domain: domain1
Application Server server name: server1
This script will update your Sun ONE Application Server installation
in /opt/SUNWappserver7 to use the Sun Crypto Accelerator.
You will need to restart your admin server after this has completed.
Ok to proceed? [Y/N]: y
Using database directory
/var/opt/SUNWappserver7/domains/domain1/server1/config...
Module "Sun Crypto Accelerator 4000" added to database.
/opt/SUNWappserver7 has been configured to use
the Sun Crypto Accelerator.

<Press ENTER to continue>
```

3. **键入 0 退出。**

▼ 使用 iplsslcfg 脚本的选项 3

此选项用于将 Sun ONE Web Server 内部数据库中的 SSL 证书和密钥导出为 PKCS#12 格式。之后，这些证书可重新导入至 Sun Crypto Accelerator 4000 模块。

1. **键入以下命令执行 iplsslcfg 脚本：**

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

2. **键入 3 以将 Sun ONE Web Server 密钥导出为 PKCS#12 格式并按回车键。**

```
Sun Crypto Accelerator Sun ONE Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

Your selection (0 to quit): 3
```

3. **键入 Sun ONE 服务器目录的路径。**

iplsslcfg 实用程序将搜索任何潜在的证书和密钥数据库，以便从中导出密钥。

```
Please enter the full path of the web server
root directory [/usr/iplanet/servers]: /usr/iplanet/servers
```

4. **键入所提供列表中的某一名称。**

```
The following certificate databases were found:
https-machine.domain.com-webserv1-
https-machine.domain.com-webserv2-
Which certificate database do you wish to export from?
https-machine.domain.com-webserv1-
```

5. **为要导出的服务器证书指定容易记忆的名称。**

   默认情况下，此名称为 Server-Cert。

```
Please provide the name for the certificate you wish to export.
If you wish to export from a hardware device, you will need to
provide the token name followed by a ":" and the certificate name.
Not all external tokens will allow keys to be exported.
Certificate Name [Server-Cert]: Server-Cert
```

6. **指定 PKCS#12 文件的路径和文件名。**

```
Please specify the path where the PKCS#12 file will be stored:
/tmp/export.p12
```

7. **输入密码。**

   成功验证后，系统将要求您设置 PKCS#12 文件的密码。密码创建后， PKCS#12 文件会写入至您在步骤 6 中所选的文件名。

```
Enter Password or Pin for "NSS Certificate DB":
Enter password for PKCS12 file:
Re-enter password:
pk12util: PKCS12 EXPORT SUCCESSFUL
Successfully created the PKCS#12 file.
<Press ENTER to continue>
```

8. **键入** 0 **退出。**

▼ 使用 iplsslcfg 脚本的选项 4

此选项用于将 PKCS#12 格式的密钥和证书导入至板。

1. **键入以下命令执行** iplsslcfg **脚本：**

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

2. **键入 4 从 SUN ONE Web Server 的 PKCS#12 格式文件中导入密钥并按回车键。**

```
Sun Crypto Accelerator Sun ONE Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

Your selection (0 to quit): 4
```

3. **键入 Sun ONE 服务器目录的路径。**

```
Please enter the full path of the web server
root directory [/usr/iplanet/servers]: /usr/iplanet/servers
```

4. **键入要导入至 PKCS#12 文件的路径。**

```
Enter the path to the PKCS#12 file: /tmp/export.p12
```

5. **对以下问题回答 “是”。**

```
Will you be importing to a hardware device? [Y/N]: Y
```

6. **键入您在初始化期间为板配置的密钥库名。**

```
Enter the token name: vca0
```

7. **键入 *username:password* 字符串，以成功通过验证。参见**表 5-1。

```
Enter Password or Pin for "vca0":
```

8. **键入用于保护 PKCS#12 文件的密码。**

```
Enter password for PKCS12 file:
Import successful.

<Press ENTER to continue>
```

使用 apssl cfg 脚本

apssl cfg 脚本的选项 1 用于配置 Apache Web Server 以使用 SSL。选项 2 用于为 Apache Web Server 配置密钥。

注 – apssl cfg 脚本只支持 Apache Web Server 1.3.26。

▼ 使用 apssl cfg 脚本的选项 1

- **有关说明，请参阅第 164 页 “配置 Apache Web Server 1.3x”。**

使用 apssl cfg 脚本的选项 2

选项 2 具有以下 3 个子选项：

1. 生成密钥对并申请 Apache 证书
2. 将 Apache （PEM 编码 X.509）密钥导出为 PKCS#12 格式
3. 将 PKCS#12 格式的密钥导入 Apache （PEM 编码 X.509）

▼ 生成密钥对并申请 Apache 证书

此选项用于生成 RSA 密钥和可提交至认证机构的证书申请。

1. **键入 `1` 以选择此选项。**

2. **键入二进制文件和 Apache 模块的路径，以及配置文件的路径。**

```
Please enter the directory where the Apache
binaries and libraries exist [/usr/apache]: /usr/apache

Please enter the directory where the Apache
configuration files exist [/etc/apache]: /etc/apache
```

3. **键入用于存储密钥的路径。**

```
Where would you like the keys stored? [/etc/apache/keys]: /etc/apache/keys
```

4. **键入密钥和证书申请文件的库名。**

   此名称位于文件名之前。例如：如果您选择 `cert1`，则密钥文件名为 `cert1-key.pem`，证书申请文件名则为 `cert1-certreq.pem`。

```
Please choose a base name for the key and request file: cert1
```

5. **选择要生成的 RSA 密钥的大小。**

   选择大小（单位：位）后，将会生成 RSA 密钥。

```
What size would you like the RSA key to be [1024]? 1024
```

6. **键入用于加密密钥文件的密码。**

   使用难以猜测的密码，并且不要忘记。

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

7. **为您的申请键入证书名称组件。**

证书申请会写入可提交至认证机构的文件。

```
-----
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]: California
Locality Name (eg, city) []: San Diego
Organization Name (eg, company) []: Company
Organizational Unit Name (eg, section) []: Department
SSL Server Name (eg, www.company.com) []: www.company.com
Email Address []: admin@domain.com

The keyfile is stored in /etc/apache/keys/cert1-key.pem.
The certificate request is in /etc/apache/keys/cert1-certreq.pem.

<Press ENTER to continue>
```

▼ 将 Apache (PEM 编码 X.509) 密钥导出为 PKCS#12 格式

此选项允许您将 Apache Web Server 密钥和证书放入 PKCS#12 文件。

1. **键入 2 以选择此选项。**
2. **键入密钥文件和证书文件的路径。**

如果密钥文件和证书文件为同一文件，则键入相同的路径两次。

注 – 密钥和证书数据可以保存在相同文件或独立文件中。但是，保存在独立文件中时，文件名必须相同。

```
Enter the path to the key file:
Enter the path to the certificate file:
```

3. **键入输出 PKCS#12 文件的路径。**

```
Please specify the path where the PKCS#12
file will be stored:
```

4. **键入证书的容易记忆的名称。**

   此名称可唯一地识别证书和密钥对。

```
Please provide a friendly name for the PKCS#12 being
built.  This friendly name is necessary when
importing your PKCS#12 file for use by other web servers.
Friendly Name [Server-Cert]:
```

5. **键入密码以保护将要存入 PCKS#12 文件的密钥。**

```
Enter pass phrase for /etc/apache/keys/ap1-key.pem:
```

6. **键入密码以保护 PKCS#12 文件中的密钥数据。**

   PKCS#12 文件会写入到上述指定的文件。

```
Enter Export Password:
Verifying - Enter Export Password:
Your PKCS#12 file has been created successfully and is in
/tmp/exp.p12

<Press ENTER to continue>
```

▼ 将 PKCS#12 格式的密钥导入 Apache （PEM 编码 X.509）

此选项允许您从 PKCS#12 文件中抽取密钥和证书并用于 Apache Web Server。

1. **键入 3 以选择此选项。**
2. **键入 PKCS#12 文件的路径和文件名。**

```
Enter the path to the PKCS#12 file:
```

3. **键入用于保存所抽取密钥和证书的路径。**

```
Enter the directory where keys and certificates
will be stored:
```

4. **键入密钥和证书文件的文件名。**

   加密密钥和证书将包含在相同的文件中。

```
Please choose a name for the key and
Certificate file. This file will contain
both the encrypted key and the certificate:
```

5. **键入用于保护 PKCS#12 文件的密码。**

```
Enter Import Password:
MAC verified OK
```

6. **键入新密码以保护可供 Apache 读取的密钥文件。**

   密钥和证书数据会写入至步骤 4 中指定的文件。

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

The keys have been successfully extracted to the file
/etc/apache/key2/yakstuff.pem.

<Press ENTER to continue>
```

为安装在同一服务器中的多块板分配不同的 MAC 地址

您可采用两种方法来为单个服务器中的多块板分配不同的 MAC 地址。第一种方法在操作系统级别下执行，第二种方法在 OpenBoot PROM 级别下执行。

▼ 从终端窗口分配不同的 MAC 地址

1. **键入以下命令：**

```
# eeprom "local-mac-address?"=true
```

注 – 当“local-mac-address?”参数设为 true 时，所有非集成网络接口设备均使用产品在工厂中制造时分配的本地 MAC 地址。

---

2. **重新引导系统。**

▼ 在 OpenBoot PROM 级别下分配不同的 MAC 地址

1. **在 OpenBoot PROM** ok **提示符下，输入以下命令：**

```
ok setenv local-mac-address? true
```

注 – 当“local-mac-address?”参数设为 true 时，所有非集成网络接口设备均使用产品在工厂中制造时分配的本地 MAC 地址。

---

2. **引导操作系统。**

第 5 章

安装和配置 Sun ONE 服务器软件

本章介绍如何配置 Sun Crypto Accelerator 4000 板以便与 Sun ONE 服务器配合使用。它包括以下几节：

注 – 本手册中所述的 Sun ONE 服务器此前称为 iPlanet™ 服务器。

Sun ONE Web Server 的安全管理性能

本节概述了 Sun Crypto Accelerator 4000 板由 Sun ONE Web Server 管理时的安全性能。

注 – 要管理密钥库，您必须对系统拥有系统管理员帐户的访问权限。

概念和术语

必须为通过 PKCS#11 界面与 Sun Crypto Accelerator 4000 板通信的应用程序 （如 Sun ONE Web Server）创建密钥库和用户。

注 – Apache Web Server （第 6 章）不使用本章中介绍的密钥库或用户帐户功能。

在与 Sun Crypto Accelerator 4000 板相关的上下文中，用户是指加密密钥资料的所有者。一个密钥只能由单个用户拥有，但每个用户可以拥有多个密钥。用户可能需要拥有多个密钥来支持不同的配置，如生产密钥和开发密钥 （用以反映用户所支持的部门）。

注 – 术语*用户*或*用户帐户*是指在 `vcaadm` 中创建的 Sun Crypto Accelerator 4000 用户，而非传统的 UNIX 用户帐户。UNIX 用户名与 Sun Crypto Accelerator 4000 用户名之间没有固定的一一对应关系。

密钥库是密钥资料的储存库。与密钥库信息密切相关的是安全主管和用户。密钥库不但可以存储密钥，而且还是用户帐户拥有密钥对象的一种方式。它可以使那些未通过所有者身份验证的应用程序无法看到密钥。密钥库由三部分组成：

- **密钥对象** – 为应用程序 （如 Sun ONE Web Server）保存的长期密钥。
- **用户帐户** – 可使应用程序验证和访问特定密钥的帐户。
- **安全主管帐户** – 可通过 `vcaadm` 访问密钥管理功能的帐户。

注 – 每个 Sun Crypto Accelerator 4000 板只能有一个密钥库。不过，多个 Sun Crypto Accelerator 4000 板可以共用同一个密钥库，以便提供额外的性能和容错功能。

典型安装包含一个密钥库，该库中具有三个用户。例如，此配置可能包含一个密钥库 *sca4000-ks-1*，该密钥库中具有三个用户：*webserv*、*dirserv* 和 *mailserv*。这允许三个用户有权访问和维护各自在该单个密钥库中的服务器密钥。图 5-1 显示了典型安装概述。

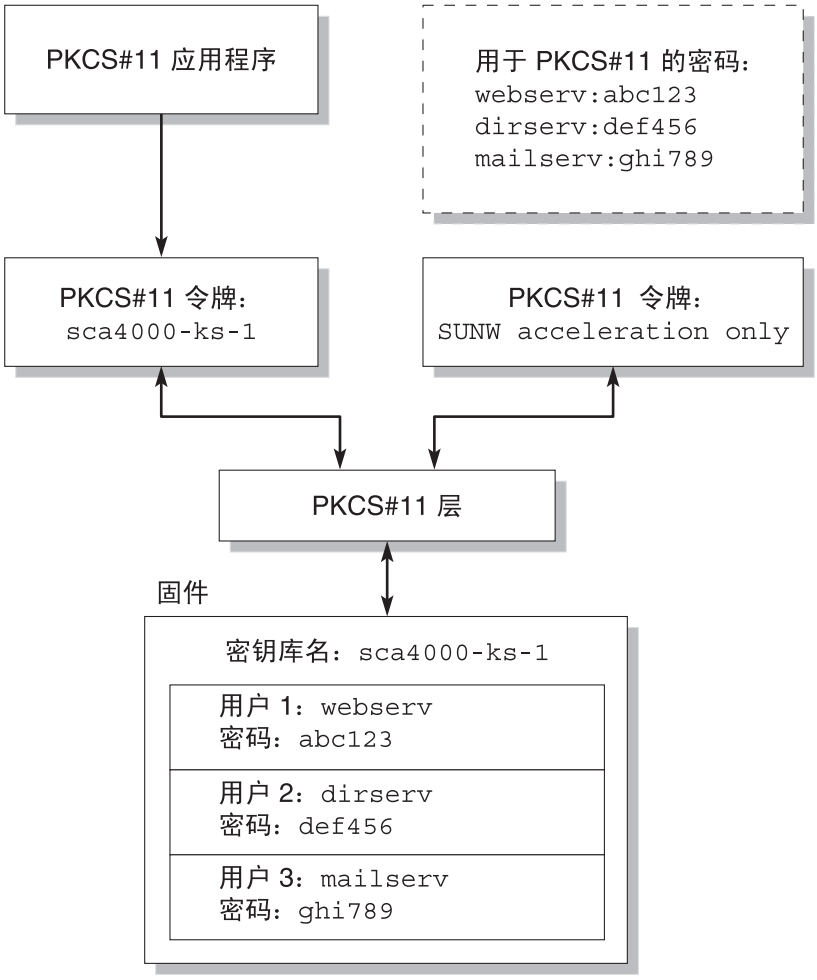

图 5-1 密钥库和用户概述

管理工具 vcaadm 用于管理 Sun Crypto Accelerator 4000 的密钥库和用户。有关说明，请参阅第 65 页 “通过 vcaadm 管理密钥库”。

令牌和令牌文件

*密钥库*以*令牌*的形式呈现给 Sun ONE Web Server。令牌文件使 Sun Crypto Accelerator 4000 管理员可以选择性地仅向给定的应用程序提供特定的令牌。

示例

如果创建了三个密钥库 （*engineering*、 *finance* 和 *legal*），则默认情况下会向 Sun ONE Web Server 提供以下三个令牌：

- `engineering`
- `finance`
- `legal`

令牌文件

要改写默认情况，必须要有令牌文件。某些应用程序无法处理多个令牌。令牌文件是包含一个或多个令牌名 （每行一个）的文本文件。

注 – 令牌名与密钥库名相同。

Sun ONE Web Server 仅提供令牌文件中列出的令牌。指定令牌文件的方法如下 （按优先顺序排列）：

1. 由环境变量 `SUNW_PKCS11_TOKEN_FILE` 命名的文件

   某些应用程序软件禁止使用环境变量。此情况下，不能采用这种方法。

2. 文件 `$HOME/.SUNWconn_cryptov2/tokens`

   此文件必须位于 Sun ONE Web Server 以其身份运行的 UNIX 用户的主目录下。如果 Sun ONE Web Server 以其身份运行的 UNIX 用户没有主目录时，则不能使用这种方法。

3. 文件 `/etc/opt/SUNWconn/cryptov2/tokens`

如果不存在任何令牌文件，Sun Crypto Accelerator 4000 软件会向 Sun ONE Web Server 提供所有令牌。

下面是令牌文件示例：

```
================================
# This is an example token file

engineering # Comments are acceptable on the same line

legal

# Because the finance keystore is not listed, the Sun Crypto
# Accelerator will not present it to the Sun ONE Web Server.

...
================================
```

注 – 注释以井字符 (#) 开头。允许存在空行。

如果找不到本节介绍的任何文件，则采用第 98 页 “令牌和令牌文件”中所述的默认方法。

启用和禁用批量加密

默认情况下，系统已禁用了 SunONE 服务器软件的批量加密功能。您可能需要启用此功能以便安全地传送较大的文件。

要使 Sun ONE 服务器软件可以使用 Sun Crypto Accelerator 4000 板上的批量加密功能，您只需在 `/etc/opt/SUNWconn/cryptov2/` 目录中创建一个名为 `sslreg` 的空文件，然后重新启动服务器软件。

```
# touch /etc/opt/SUNWconn/cryptov2/sslreg
```

要禁用批量加密功能，您必须删除 `sslreg` 文件，然后重新启动服务器软件。

```
# rm /etc/opt/SUNWconn/cryptov2/sslreg
```

配置 Sun ONE Web Server

本部分介绍以下主题：

密码

在启用 Sun ONE Web Server 的过程中，系统会要求您提供几个密码。表 5-1 对每个密码进行了说明。本章介绍的各个过程会用到这些密码。

表 5-1 Sun ONE Web Server 所需的密码

密码类型	说明
Sun ONE Web Server 管理服务器	启动 Sun ONE Web Server 管理服务器时需要提供此密码。此密码在设置 Sun ONE Web Server 期间指定。
Web 服务器信任数据库	在安全模式下启动内部加密模块时需要提供此密码。此密码是在通过 Sun ONE Web Server 管理服务器创建信任数据库时指定的。此外，在申请证书并将其安装到内部加密模块时也要求提供该密码。
安全主管	执行 `vcaadm` 权限操作时需要提供此密码。
username:password	在安全模式下启动 Sun Crypto Accelerator 4000 模块时需要提供此密码。此外，在申请证书并将其安装到内部加密模块 (*keystore_name*) 时也需提供此密码。此密码包括在 `vcaadm` 中创建的密钥库用户的 *username （用户名）*和 *password （密码）*。密钥库 *username （用户名）*和 *password （密码）*以冒号 (:) 隔开。

填充密钥库

启用板以便与 Sun ONE Web Server 配合使用之前，您必须先初始化板，然后向此板的密钥库中添加至少一位用户。板的密钥库是在初始化过程中创建的。另外，您也可以对 Sun Crypto Accelerator 4000 板进行初始化，使之使用现有的密钥库。有关说明，请参阅第 62 页 “通过 `vcaadm` 初始化板”。

注 – 每个 Sun Crypto Accelerator 4000 板仅能配置一个密钥库，因此，您必须为每个板配置一个密钥库。不过，多个 Sun Crypto Accelerator 4000 板可以配置为共用同一个密钥库，以便提供其它性能和容错功能。

▼ 填充密钥库

1. **在搜索路径中指定 Sun Crypto Accelerator 4000 工具目录（如果尚未这样做），例如：**

```
$ PATH=$PATH:/opt/SUNWconn/bin
$ export PATH
```

2. **使用** `vcaadm` **命令访问** `vcaadm` **实用程序，或输入** `vcaadm -h` *hostname* **将** `vcaadm` **连接至远程主机上的板。**

   有关说明，请参阅第 53 页 “使用 vcaadm 实用程序”。

```
$ vcaadm -h hostname
```

3. **向板的密钥库中添加用户。**

   这些用户名仅在 Sun Crypto Accelerator 4000 板的域中被识别，而且不必与 Web 服务器进程所用的 UNIX 用户名相同。请注意，在尝试创建用户之前，必须先以 `vcaadm` 安全主管的身份登录。

4. **运行** `create user` **命令创建用户。**

```
vcaadm{vcaN@hostname, sec-officer}> create user username
Initial password:
Confirm password:
User username created successfully.
```

   此处创建的 *username*（*用户名*）和 *password*（*密码*）共同组成了 *username:password*（参见表 5-1）。在 Web 服务器启动期间进行验证时，必须使用此密码。这是单个用户的密钥库密码。

注意 – 用户必须记住此 *username:password*。没有密码，用户将无法访问自己的密钥。丢失的密码无法找回。

5. **退出** `vcaadm`。

```
vcaadm{vcaN@hostname, sec-officer}> exit
```

启用 Sun ONE Web Server 概述

要启用 Sun ONE Web Server，必须完成以下步骤。接下来的两节将对这些步骤进行详细说明。

1. 安装 Sun ONE Web Server。
2. 创建信任数据库。
3. 申请证书。
4. 安装证书。
5. 配置 Sun ONE Web Server。

注意 – 这些步骤必须按指定的顺序进行。否则，则可能导致配置错误。

- 如果您使用 Sun ONE Web Server 4.1，请转至第 103 页“安装和配置 Sun ONE Web Server 4.1”。
- 如果您使用 Sun ONE Web Server 6.0，请转至第 113 页“安装和配置 Sun ONE Web Server 6.0”。

配置 Sun ONE Web Server，使其在重新引导期间启动但不进行用户交互操作

使用加密密钥，您可以使 Sun ONE Web Server 在重新引导期间自动启动。

▼ 创建加密密钥以使 Sun ONE Web Server 在重新引导期间自动启动

1. **浏览至 Sun ONE Web Server 例程的** `config` **子目录 — 例如，** `/usr/iplanet/servers/https-`*webserver_instance_name*`/config`。
2. **创建只包含以下行的** `password.conf` **文件 （有关密码定义，请参见**表 5-1**）：**

```
internal:trust-db-password
keystore-name:username:password
```

3. **将密码文件的所有权设置为 Web 服务器以其身份运行的 UNIX 用户 ID，并将密码文件的访问权限设置为只供密码文件的所有者读取：**

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

安装和配置 Sun ONE Web Server 4.1

本部分介绍如何安装和配置 Sun ONE Web Server 4.1 以使用板。您必须按顺序执行这些步骤。有关安装和使用 Sun ONE Web Server 的详细信息，请参阅 Sun ONE Web Server 文档。本部分包括以下过程：

▼ 安装 Sun ONE Web Server 4.1

1. **下载 Sun ONE Web Server 4.1 软件。**

   以下 URL 提供了该 Web 服务器软件：`http://www.sun.com/`

2. **切换至安装目录并解压 Web 服务器软件。**

3. **从命令行中使用 `setup` 脚本安装 Web 服务器。**

   服务器的默认路径名为：`/usr/netscape/server4`。

   本章中使用默认路径。如果您想将 Web 服务器软件安装在不同的位置，请记住其安装位置。

```
# ./setup
```

4. **回答安装脚本中的提示。**

   除以下提示之外，可以接受默认设置。

   a. 通过键入 `yes` 同意接受许可条款。

   b. 输入完整的域名。

   c. 输入两次 Sun ONE Web Server 4.1 管理服务器的密码。

   d. 提示时，按回车键。

配置 Sun ONE Web Server 4.1

本节介绍以下过程：为 Web 服务器例程创建信任数据库；向 Web 服务器注册板；生成并安装服务器证书；以及启用 Web 服务器以使用 SSL。

在配置过程中， Sun ONE Web Server 管理服务器必须开启并运行。

▼ 创建信任数据库

1. **启动 Sun ONE Web Server 4.1 管理服务器。**

   通过键入以下命令来启动 Sun ONE Web Server 4.1 管理服务器（而不是在 `setup` 请求时运行 `startconsole`）：

```
# /usr/netscape/server4/https-admserv/start
SunONE-WebServer-Enterprise/4.1SP9 BB1-08/23/2001 05:50
startup: listening to http://hostname.domain, port 8888 as root
```

   此响应提供用于连接到管理服务器的 URL。

2. **打开 Web 浏览器并输入以下内容来启动管理图形用户界面 (GUI)：**

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

   在验证对话框中，输入您在运行 `setup` 时选择的 Sun ONE Web Server 4.1 管理服务器用户名及密码。

注 – 如果您在设置 Sun ONE Web Server 期间使用的是默认设置，请键入 **`admin`** 作为用户 ID 或 Sun ONE Web Server 4.1 管理服务器用户名。

---

3. **选择 “OK”。**

   屏幕上会显示 Sun ONE Web Server 4.1 管理服务器窗口。

4. **创建 Web 服务器例程的信任数据库。**

   a. **在 Sun ONE Web Server 4.1 管理服务器窗口中单击 “Servers” 选项卡。**

   b. **选择服务器，然后单击 “Manage” 按钮。**

   c. **单击页面顶部附近的 “Security” 选项卡，然后选择 “Create Database” 链接。**

   d. **在两个对话框中输入密码（Web 服务器信任数据库；参见**表 5-1**），然后选择 “OK”。**

      选择一个至少包含 8 个字符的密码。当 Sun ONE Web Server 在安全模式下运行时，此密码用于启动内部加密模块。

      您可能想对多个 Web 服务器例程启用安全保护功能。如果是这样，请对每一个 Web 服务器例程重复步骤 1 至步骤 4。

注 – 如果您还想在 Sun ONE Web Server 4.1 管理服务器上运行安全套接层 (SSL) 功能，则此过程与设置信任数据库的过程类似。有关详情，请参阅 `http://docs.sun.com` 网站上的 《*iPlanet Web Server, Enterprise Edition Administrator's Guide*》。

▼ 向 Web 服务器注册板

1. **执行以下脚本以向 Web 服务器注册板：**

```
# /opt/SUNWconn/bin/iplsslcfg
```

此脚本会提示您选择服务器并为所选的 Sun ONE 服务器安装 Sun Crypto Accelerator 4000 加密模块。然后，脚本会更新配置文件以启用板。

2. **键入 1，配置 Sun ONE Web Server 以使用 SSL，然后按回车键。**

注 – 本过程假定您在此提示下选择选项 1。如果希望选择选项 2、 3 或 4，请参阅第 84 页 “使用 iplsslcfg 脚本”。

```
Sun Crypto Accelerator Sun ONE Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

Your selection (0 to quit): 1
```

3. **提示时，输入 Web 服务器根目录的路径，然后按回车键。**

```
Please enter the full path of the web server
root directory [/usr/netscape/server4]: /usr/netscape/server4
```

4. **提示时，键入 y 然后按回车键。**

```
This script will update your Sun ONE Web Server installation
in /usr/netscape/server4 to use the Sun Crypto Accelerator
You will need to restart your admin server after this has
completed.
Ok to proceed? [Y/N]: y

Using database directory /usr/netscape/server4/alias...
Module "Sun Crypto Accelerator 4000" added to database.
/usr/netscape/server4 has been configured to use
the Sun Crypto Accelerator.


<Press ENTER to continue>
```

5. **键入 0 退出。**

▼ 生成服务器证书

1. **键入以下命令，重新启动 Sun ONE Web Server 4.1 管理服务器：**

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

此响应提供用于连接到管理服务器的 URL。

2. **打开 Web 浏览器并输入以下地址来启动管理 GUI：**

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

在验证对话框中，输入您在运行 `setup` 命令时选择的 Sun ONE Web Server 4.1 管理服务器用户名及密码。

注 – 如果您在设置 Sun ONE Web Server 期间使用的是默认设置，则键入 `admin` 作为用户 ID 或 Sun ONE Web Server 4.1 管理服务器用户名。

---

3. **选择 “OK”。**

屏幕上会显示 Sun ONE Web Server 4.1 管理服务器窗口。

4. **要申请服务器证书，请选择 Sun ONE Web Server 4.1 管理服务器窗口顶部附近的 “Security” 选项卡** （图 5-2）。

屏幕上会显示 “Create Trust Database” 页面。

5. **选择左窗格中的 “Request a Certificate” 链接** （图 5-2）。

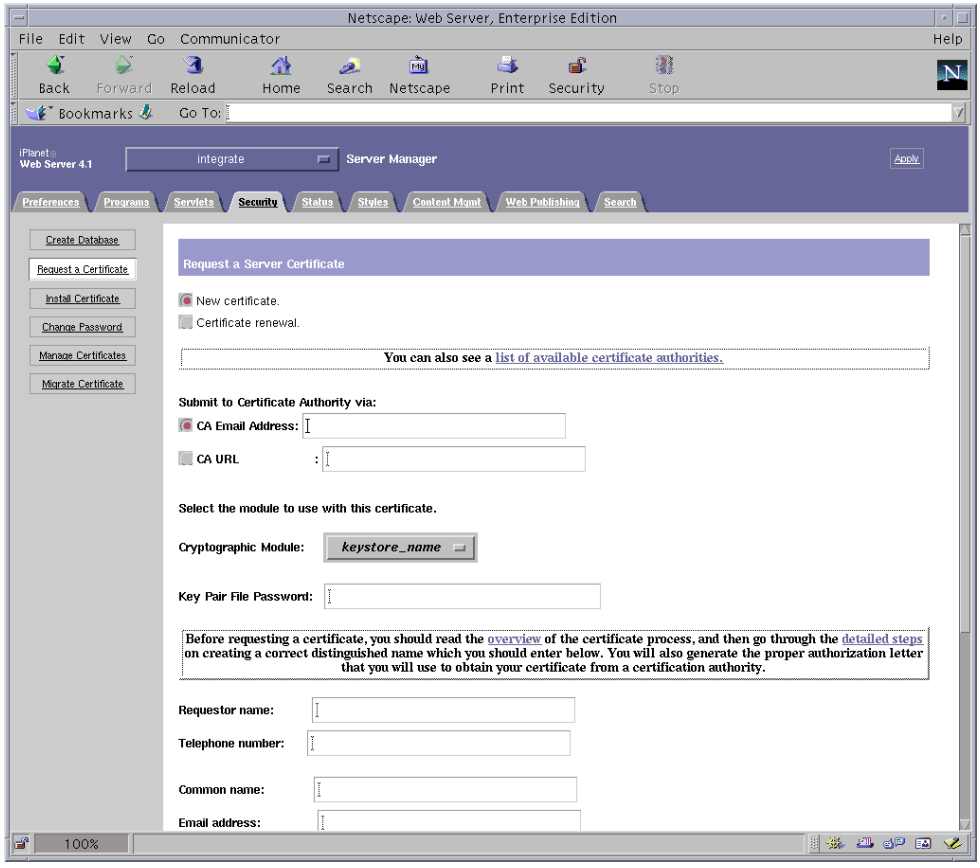

图 5-2 Sun ONE Web Server 4.1 管理服务器的申请服务器证书对话框

6. **使用以下信息填写表单以生成证书申请：**

   a. **选择 “New Certificate”**。

   如果您可以直接将证书申请发送到可通过 Web 访问的认证机构或注册机构，请选择 CA URL （认证机构 URL）链接。否则，请选择 “CA Email Address”，然后输入要将证书申请发送到的电子邮件地址。

   b. **选择要使用的 “Cryptographic Module”**。

   此下拉菜单中包含每一个密钥库的条目。务必选择正确的密钥库。不要选择 “SUNW acceleration only”。

   c. **在 “Key Pair File Password” 对话框中，为将要拥有密钥的用户输入密码。**

   此密码为 *username:password* （表 5-1）。

d. 在表 5-2 **列出的申请人信息字段中输入正确的信息。**

表 5-2 申请人信息字段

字段	说明
Requestor Name	申请人的联系信息
Telephone Number	申请人的联系信息
Common Name	在来访者的浏览器中键入的 Web 站点域
Email Address	申请人的联系信息
Organization	公司名称
Organizational Unit	（可选）公司部门
Locality	（可选）城市、郡县、公国或国家/地区
State	（可选）省/州的全称
Country	由两个字母组成的国家/地区 ISO 代码 （例如，中国为 CN）

e. 单击 “OK” 提交信息。

7. 利用认证机构生成证书。

- 如果已选择将证书申请发送给 CA URL，则证书申请会自动发送到该处。
- 如果已选择 “CA Email Address”，请复制通过电子邮件发送给您的证书申请及标题，然后将其交给认证机构。

8. 一旦生成证书，请将证书及标题一起复制到剪贴板上。

注 – 证书通常以文本格式向您提供，这与证书申请不同。请将此数据保留在剪贴板上，以便在以下过程的步骤 5 中使用。

▼ 安装服务器证书

1. 选择 Sun ONE Web Server 4.1 管理服务器窗口左侧的 “Install Certificate” 链接。

一旦认证机构批准您的申请并签发证书，您必须将证书安装在 Sun ONE Web Server 中。

2. 单击 “Security” 选项卡。

3. 在左窗格中，选择 “Install Certificate”链接。

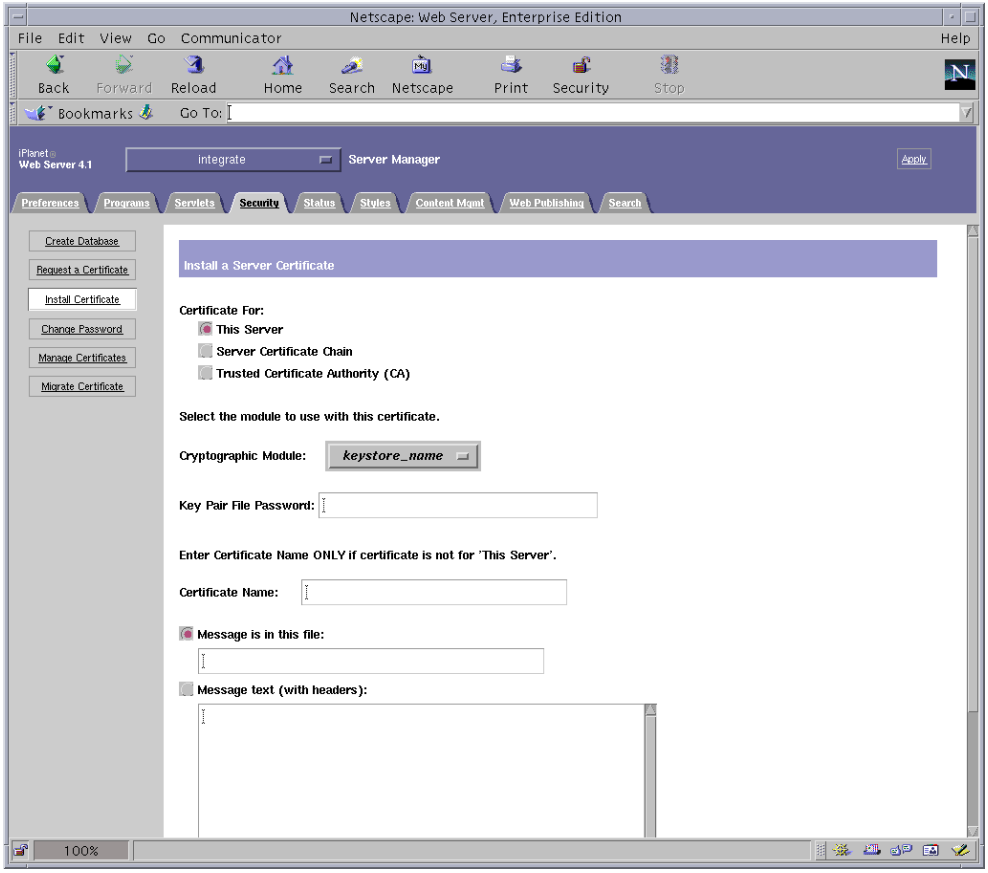

图 5-3 Sun ONE Web Server 4.1 管理服务器的安装服务器证书对话框

4. **填写表单，安装证书：**

表 5-3 要安装证书的字段

字段	说明
Certificate For	本服务器。
Cryptographic Module	此下拉菜单中包含每一个密钥库的条目。请务必选择正确的密钥库名称。要使用板，必须选择与密钥库名称相同的模块。
Key Pair File Password	此密码为 *username:password* （表 5-1）。
Certificate Name	多数情况下，您可以将此字段留空。如果提供一个名称，该名称将会改变 Web 服务器在运行 SSL 支持时用来访问证书和密钥的名称。此字段的默认值为 `Server-Cert`。

5. **将从认证机构复制的证书（第 107 页“生成服务器证书”的步骤 8）粘贴到“Message”框内。**

   屏幕上会显示证书的一些基本信息。

6. **单击 “OK”。**

7. **如果输入的内容正确无误，请选择 “Add Server Certificate”按钮。**

   屏幕上会显示一则消息，通知您重新启动服务器。由于 Web 服务器例程一直处于关闭状态，因此不必重新启动。

   另外，系统还会通知您，为使 Web 服务器使用 SSL，必须对 Web 服务器进行相应配置。请执行下面的过程来配置 Web 服务器。

注 – 有关如何自签用于测试的证书，请参阅 mod_SSL 和 OpenSSL 文档。

现在，您已安装了 Web 服务器和服务器证书，不过，您必须启用 Web 服务器以使用 SSL。

▼ 启用 Web 服务器以使用 SSL

1. **在 Sun ONE Web Server 4.1 管理服务器主页上，选择您要与 SSL 一起使用的 Web 服务器例程，然后选择 “Manage”。**

2. **单击页面顶部的 “Preferences”选项卡 （如果尚未选定）。**

3. **选择页面左侧的 “Encryption On/Off”链接。**

4. **将加密设为 “On”。**

   对话框中的 “Port”字段应更新为默认的 SSL 端口号 443。如果需要，请更改端口号。

5. **单击 “OK”按钮。**

6. **单击 “Save”按钮，应用这些更改。**

   现在， Web 服务器即可在安全模式下运行。

7. **打开** `/usr/netscape/server4/https-`*hostname*`/config/magnus.conf` **文件（***hostname* **是 Web 服务器的名称），在其中添加下面的行：**

   ```
   CERTDefaultNickname keystore-name:Server-Cert
   ```

   默认情况下，您生成的证书名为 `Server-Cert`。如果您的证书采用其它名称，请务必用您选择的名称代替 `Server-Cert`。

8. **选择您要管理的服务器，然后单击页面右上角的 “Apply”按钮。**

   此选项会将更改应用于整个 Sun ONE Web Server 4.1 管理服务器。

9. **单击 “Load Configuration Files”按钮，以应用对** `magnus.conf` **文件所做的更改。**

   屏幕上会显示一个允许您启动 Web 服务器例程的页面。

   如果您在服务器关闭时选择 “Apply Changes”按钮，则会出现一个验证对话框，提示您输入 *username:password*。此窗口不可以调整大小，因此在提交更改时可能会遇到问题。

   该问题有两种解决方法：

   - 改选 “Load Configuration Files”。
   - 先启动 Web 服务器，然后单击 “Apply Changes”按钮。

10. **在 Sun ONE Web Server 4.1 管理服务器窗口中，选择窗口左侧的 “On/Off”链接。**

11. **输入服务器密码，然后选择 “OK”按钮。**

    系统会提示您输入一个或多个密码。出现 “Module Internal”提示时，请输入 Web 服务器信任数据库的密码。

    出现模块 *keystore_name* 提示时，请输入该密钥库的 *username:password*。

    出现其它密钥库的提示时，请输入相应的 *username:password*。

12. **在下面的 URL 上验证已启用 SSL 的新 Web 服务器：**

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

注 – 默认的 *server-port* 为 443。

安装和配置 Sun ONE Web Server 6.0

本部分介绍如何安装和配置 Sun ONE Web Server 6.0 以使用板。您必须按顺序执行这些步骤。有关安装和使用 Sun ONE Web Server 的详细信息，请参阅 Sun ONE Web Server 文档。本节包括以下过程：

▼ 安装 Sun ONE Web Server 6.0

1. **下载 Sun ONE Web Server 6.0 软件。**

   以下 URL 提供了该 Web 服务器软件：`http://www.sun.com/`

2. **切换至安装目录并解压 Web 服务器软件。**

3. **从命令行中使用 setup 脚本安装 Web 服务器。**

   服务器的默认路径名为：`/usr/iplanet/servers`。

   本章中使用默认路径。如果您想将软件安装在不同的位置，请记住其安装位置。

   ```
   # ./setup
   ```

4. **回答安装脚本中的提示。**

   除了以下提示，可以接受默认选项：

   a. **通过键入 `yes` 同意接受许可条款。**

   b. **输入完整的域名。**

   c. **输入两次 Sun ONE Web Server 6.0 管理服务器的密码。**

   d. **提示时，按回车键。**

配置 Sun ONE Web Server 6.0

本节包括以下过程：为 Web 服务器例程创建信任数据库；向 Web 服务器注册板；生成并安装服务器证书；以及启用 Web 服务器以使用 SSL。

在配置过程中， Sun ONE Web Server 管理服务器必须开启并运行。

▼ 创建信任数据库

1. **启动 Sun ONE Web Server 6.0 管理服务器。**

   要启动 Sun ONE Web Server 6.0 管理服务器，请使用以下命令（而不是在 `setup` 请求时运行 `startconsole`）：

```
# /usr/iplanet/servers/https-admserv/start
SunONE-WebServer-Enterprise/6.0SP1 B08/20/2001 00:58
warning: daemon is running as super-user
[LS ls1] http://hostname.domain/port 8888 ready to accept requests
startup: server started successfully
```

   此响应提供用于连接到管理服务器的 URL。

2. **打开 Web 浏览器并输入以下地址来启动管理 GUI：**

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

   在验证对话框中，输入您在运行 `setup` 时选择的 Sun ONE Web Server 6.0 管理服务器用户名及密码。

注 – 如果您在设置 Sun ONE Web Server 期间使用的是默认设置，则在用户 ID 或 Sun ONE Web Server 6.0 管理服务器用户名字段中键入 `admin`。

---

3. **单击 “OK”。**

   屏幕上会显示 Sun ONE Web Server 6.0 管理服务器窗口。

4. **创建 Web 服务器例程的信任数据库。**

   您可能想对多个 Web 服务器例程启用安全保护功能。如果是这样，请对每一个 Web 服务器例程重复步骤 1 至步骤 4。

注 – 如果您还想在 Sun ONE Web Server 6.0 管理服务器上运行 SSL 功能，则此过程与设置信任数据库的过程类似。有关详情，请参阅 `http://docs.sun.com` 网站上的《*iPlanet Web Server, Enterprise Edition Administrator's Guide*》。

---

a. 在 Sun ONE Web Server 6.0 管理服务器对话框中单击 “Servers”选项卡。

b. 选择服务器，然后单击 “Manage”按钮。

c. 单击页面顶部附近的 “Security”选项卡，然后选择 “Create Database”链接。

d. 在两个对话框中输入密码 （Web 服务器信任数据库的密码；参阅表 5-1**），然后单击 “OK”。**

选择一个至少包含 8 个字符的密码。 Sun ONE Web Server 在安全模式下运行时，将使用此密码来启动内部加密模块。

▼ 向 Web 服务器注册板

1. 运行以下脚本，向 Web 服务器注册板：

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

此脚本会提示您选择服务器并为所选的 Sun ONE 服务器安装 Sun Crypto Accelerator 4000 加密模块。然后，脚本会更新配置文件以启用板。

2. 键入 1**，配置 Sun ONE Web Server 以使用 SSL，然后按回车键。**

注 – 本过程假定您在此提示下选择选项 1。如果希望选择选项 2、 3 或 4，请参阅第 84 页 “使用 iplsslcfg 脚本”。

```
Sun Crypto Accelerator Sun ONE Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

Your selection (0 to quit): 1
```

3. 提示时，输入 Web 服务器根目录的路径，然后按回车键。

```
Please enter the full path of the web server
root directory [/usr/iplanet/servers]: /usr/iplanet/servers
```

4. **如果要继续操作，请在提示时键入** `y` **并按回车键。**

```
This script will update your Sun ONE Web Server installation
in /usr/iplanet/servers to use the Sun Crypto Accelerator
You will need to restart your admin server after this has
completed.
Ok to proceed? [Y/N]: y

Using database directory /usr/iplanet/servers/alias...
Module "Sun Crypto Accelerator 4000" added to database.
/usr/iplanet/servers has been configured to use
the Sun Crypto Accelerator.


<Press ENTER to continue>
```

5. **键入** `0` **退出。**

▼ 生成服务器证书

1. **键入以下命令，重新启动 Sun ONE Web Server 6.0 管理服务器：**

```
# /usr/iplanet/servers/https-admserv/stop
# /usr/iplanet/servers/https-admserv/start
```

此响应提供用于连接到管理服务器的 URL。

2. **打开 Web 浏览器并输入以下地址来启动管理 GUI：**

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

在验证对话框中，输入您在运行 `setup` 时选择的 Sun ONE Web Server 6.0 管理服务器用户名及密码。

注 – 如果您在设置 Sun ONE Web Server 期间使用的是默认设置，则在用户 ID 或 Sun ONE Web Server 6.0 管理服务器用户名字段中键入 **admin**。

---

3. **单击 “OK”。**

屏幕上会显示 Sun ONE Web Server 6.0 管理服务器窗口。

4. **要申请服务器证书，请选择 Sun ONE Web Server 6.0 管理服务器窗口顶部附近的“Security”选项卡。**

   屏幕上会显示“Create Trust Database”窗口。

5. **单击 Sun ONE Web Server 6.0 管理服务器窗口左窗格中的 “Request a Certificate” 链接。**

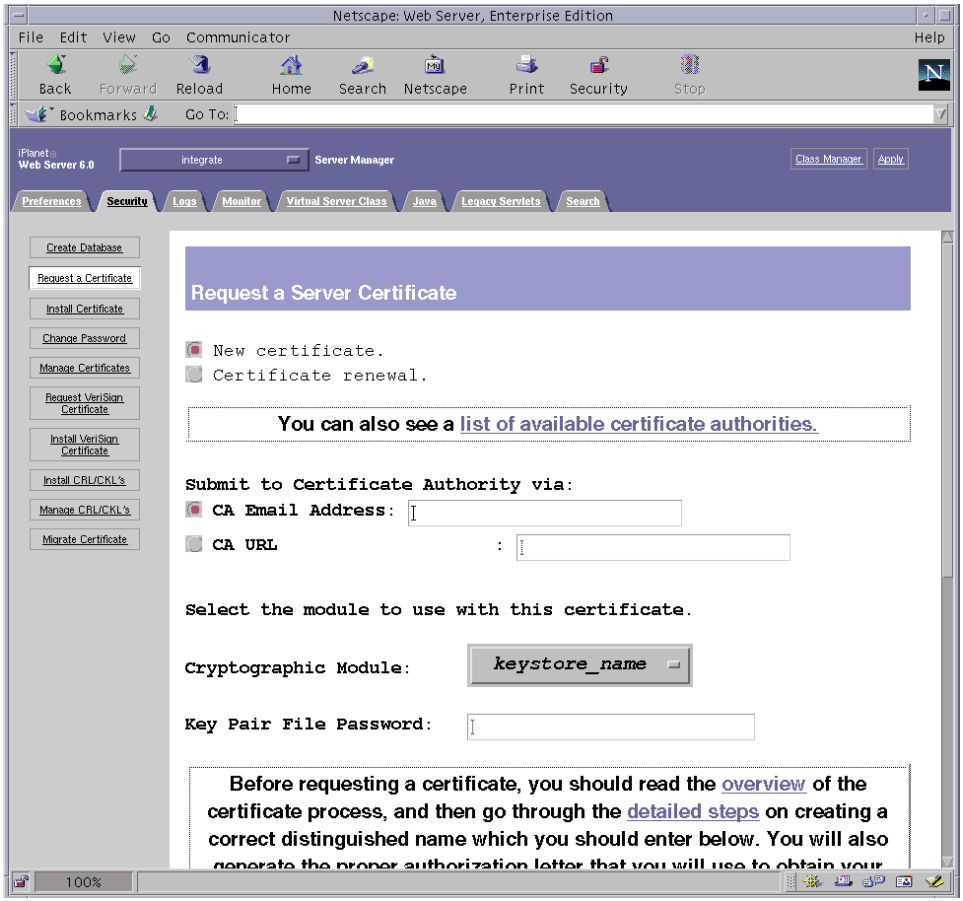

图 5-4 Sun ONE Web Server 6.0 管理服务器的申请服务器证书对话框

6. **使用以下信息填写表单以生成证书申请：**

   a. **选择 “New Certificate”。**

      如果您可以直接将证书申请发送到可通过 Web 访问的证书机构或注册机构，请选择“CA URL”链接。否则，请选择 “CA Email Address”，然后输入您要将证书申请发送至的电子邮件地址。

b. 选择要使用的 “Cryptographic Module”。

此下拉菜单中包含每一个密钥库的条目。务必选择正确的密钥库。不要选择“SUNW acceleration only”。

c. 在 “Key Pair File Password” 对话框中，为将要拥有密钥的用户输入密码。

此密码为 *username:password* （表 5-1）。

d. 在表 5-4 **列出的申请人信息字段中输入正确的信息。**

表 5-4 申请人信息字段

字段	说明
Requestor Name	申请人的联系信息
Telephone Number	申请人的联系信息
Common Name	在来访者的浏览器中键入的 Web 站点域
Email Address	申请人的联系信息
Organization	公司名称
Organizational Unit	（可选）公司部门
Locality	（可选）城市、郡县、公国或国家/地区
State	（可选）省/州的全称
Country	由两个字母组成的国家/地区 ISO 代码 （例如，中国为 CN）

e. 单击 “OK” 提交信息。

7. 利用认证机构生成证书。

- 如果已选择将证书申请发送给 CA URL，则证书申请会自动发送到该处。
- 如果已选择 “CA Email Address”，请复制通过电子邮件发给您的证书申请及标题，然后将其交给认证机构。

8. 一旦生成证书，请将证书及标题一起复制到剪贴板上。

注 – 证书通常以文本格式向您提供，这与证书申请不同。请将此数据保留在剪贴板上，以便在第 119 页 “安装服务器证书”的步骤 5 中使用。

▼ 安装服务器证书

1. **选择 Sun ONE Web Server 6.0 管理服务器窗口左侧的 “Install Certificate” 链接。**
   一旦认证机构批准您的申请并签发证书，您必须将证书安装在 Sun ONE Web Server 中。
2. **单击 “Security” 选项卡。**
3. **在左窗格中，单击 “Install Certificate” 链接。**

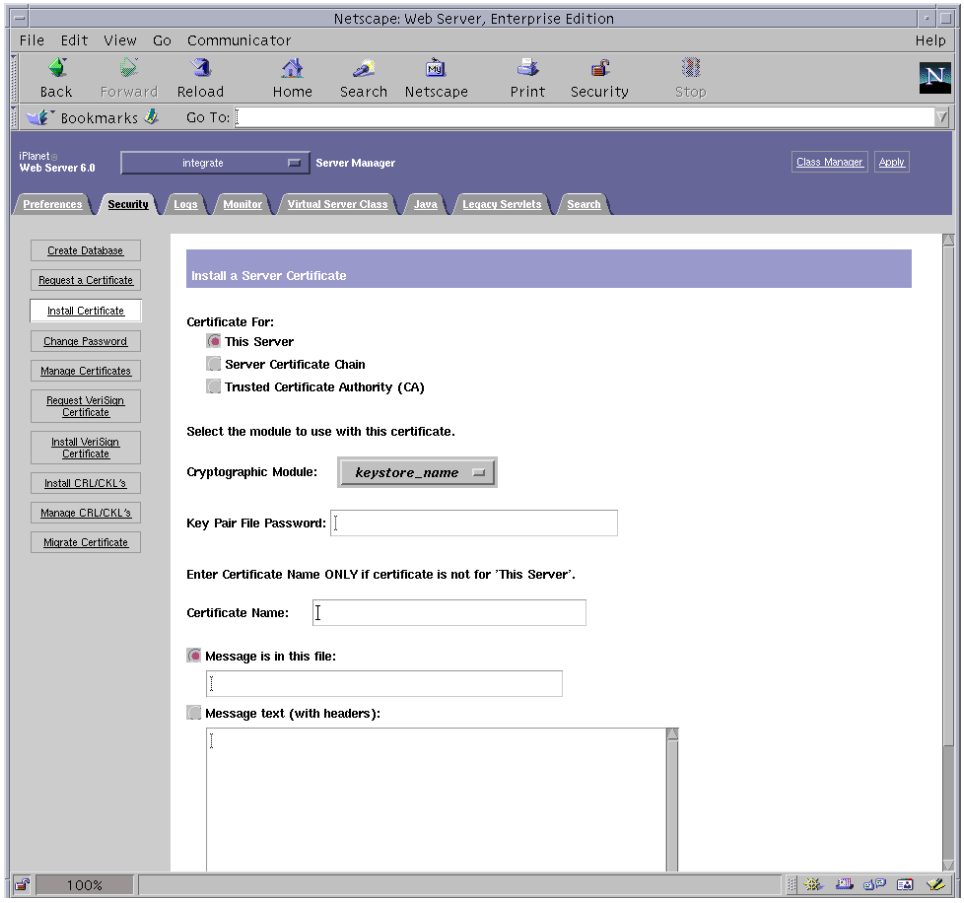

图 5-5 Sun ONE Web Server 6.0 管理服务器的安装服务器证书对话框

4. **填写表单，安装证书：**

表 5-5 要安装证书的字段

字段	说明
Certificate For	本服务器。
Cryptographic Module	此下拉菜单中包含每一个密钥库的条目。务必选择正确的密钥库名称。要使用板，必须选择一个格式为 *keystore_name* 的模块。
Key Pair File Password	此密码为 *username:password* （表 5-1）。
Certificate Name	多数情况下，您可以将此字段留空。如果提供一个名称，该名称将会改变 Web 服务器在运行 SSL 支持时用来访问证书和密钥的名称。此字段的默认值为 `Server-Cert`。

5. **将从证书机构复制的证书（第 116 页“生成服务器证书”的步骤 8）粘贴到“Message”文本框内。**

   屏幕上会显示证书的一些基本信息。

6. **单击 “OK”。**

7. **如果输入的内容正确无误，请单击 “Add Server Certificate”按钮。**

   屏幕上会显示一则消息，通知您重新启动服务器。由于 Web 服务器例程一直处于关闭状态，因此不必重新启动。

   另外，系统还会通知您，为使 Web 服务器使用 SSL，必须对 Web 服务器进行相应配置。请执行下面的过程来配置 Web 服务器。

注 – 有关如何自签用于测试的证书，请参阅 mod_SSL 和 OpenSSL 文档。

现在，您已安装了 Web 服务器和服务器证书，不过，您必须启用 Web 服务器以使用 SSL。

▼ 启用 Web 服务器以使用 SSL

1. **选择页面顶部附近的 “Preferences”选项卡。**

2. **在左窗格中选择 “Edit Listen Sockets”链接。**

   主窗格中将会列出已为 Web 服务器例程设置的所有监听套接口。

   a. **更改以下字段：**

   - **Port：**设置为您要运行已启用 SSL 的 Web 服务器的端口 （通常为端口 443）。
   - **Security：**设置为 On。

b. 单击 “OK” 应用这些更改。

现在，“Edit Listen Sockets”页面的安全字段中应显示了一个 “Attributes”链接。

3. **选择 “Attributes”链接。**
4. **输入 *username:password*，以在系统上验证密钥库。**
5. **如果您想更改一组默认密码，请在 “Ciphers”标题下面选择所需的密码组。**

   屏幕上会显示用于更改密码设置的对话框。您可以选择 “Cipher Default”设置、“SSL2”或 “SSL3/TLS”。如果选择 “Cipher Default”，则不会显示默认设置。其它两个选项需要您在弹出式对话框中选择要启用的算法。有关密码选项，请参阅 Sun ONE 文档。

6. **为密钥库选择后跟：`Server-Cert` 的证书 （或者使用您选择的名称）。**

   “Certificate Name”字段中仅显示相应密钥库用户所拥有的密钥。此密钥库用户是指使用 *username:password* 验证的用户。

7. **选择证书并确认所有安全设置之后，单击 “OK”。**
8. **选择右上角的 “Apply”链接，以便在启动服务器之前应用这些更改。**
9. **选择 “Load Configuration Files”链接以应用更改。**

   屏幕上会显示一个允许您启动 Web 服务器例程的页面。

   如果您在服务器关闭时选择 “Apply Changes”按钮，则会出现一个验证对话框，提示您输入 *username:password*。此窗口不可以调整大小，因此在提交更改时可能会遇到问题。

   该问题有两种解决方法：

   - 改选 “Load Configuration Files”。
   - 先启动 Web 服务器，然后单击 “Apply Changes”。

10. **在 Sun ONE Web Server 6.0 管理服务器窗口中，选择窗口左侧的 “On/Off”链接。**
11. **输入服务器密码，然后单击 “OK”。**

    系统会提示您输入一个或多个密码。出现 “Module Internal”提示时，请输入 Web 服务器信任数据库的密码。

    出现模块 *keystore-name* 提示时，请输入 *username:password*。

    出现其它密钥库的提示时，请输入相应的 *username:password*。

12. **在下面的 URL 上验证已启用 SSL 的新 Web 服务器：**

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

注 – 默认的 *server-port* 为 443。

安装和配置 Sun ONE Application Server 7

本部分介绍如何安装和配置 Sun ONE Application Server 7 以使用板。除安装应用程序服务器软件之外，还必须安装应用程序服务器插件软件。您必须按顺序执行这些步骤。有关安装和使用 Sun ONE Application Server 的详细信息，请参阅 Sun ONE Application Server 文档。本部分包括以下过程：

▼ 安装 Sun ONE Application Server 7

1. **下载 Sun ONE Application Server 7 软件。**

   以下 URL 提供了该应用程序服务器软件：`http://www.sun.com/`

   Sun ONE Application Server 7 有多个版本，分别具有不同的功能。

2. **切换至安装目录并解压应用程序服务器软件。**

   对于各版本的 Sun ONE Application Server 7 软件，其安装目录的默认路径有所不同。

3. **运行 `setup` 程序以启动基于 GUI（图形用户界面）的安装。**

注 – 此外，还可以从终端窗口运行 `setup -console` 程序以启动基于命令行的安装。本过程中的示例假定您使用基于 GUI 的安装。

```
# ./setup
```

4. **回答安装脚本中的提示。**

   除以下提示之外，可以接受默认设置：

   a. **通过键入 yes 同意接受许可条款。**

   b. **当提示输入 JDK (Java™ Development Kit) 的位置时，您可选择：使用现有的安装（如果支持），或者从 Appserver Build 中安装。**

   c. **输入 Sun ONE Application Server 管理服务器用户名（可以选择任何名称）。**

   d. **输入两次 Sun ONE Application Server 管理服务器密码。**

注 – 以下步骤仅适用于 Solaris 8 OE。

---

5. **如果您使用 Solaris 8，则应安装 Solaris 8 Sun ONE Application Server 修补程序 (109326-08)。**

   Solaris 9 不需要此修补程序。从 SunSolve Web 站点下载 Solaris 8 Sun ONE Application Server 修补程序：`http://sunsolve.sun.com`

   添加修补程序，方法如下：

```
# cd patch-location/SUNWappserver7/patches
# cd patches/109326-08
# ./patchadd .
```

6. **重新引导系统。**

▼ 安装 Sun ONE Application Server 插件软件

1. **下载 Sun ONE Application Server 7 插件软件。**

   以下 URL 提供了该应用程序服务器软件：`http://www.sun.com/`

2. **解压应用程序服务器插件软件。**

3. **切换至 `./AddOns/SSLUtils` 目录**

4. **创建一个目录，以便 `iplsslcfg` 脚本在此目录中调用 `modutil` 安全工具。**

```
# mkdir /usr/bin/mps
```

   这是 `iplsslcfg` 脚本希望找到 `modutil` 安全工具的路径。

5. **将** `modutil`、`certutil` **和** `pk12util` **二进制文件复制到** `/usr/bin/mps/` **路径中。**

```
# cp modutil /usr/bin/mps/
# cp certutil /usr/bin/mps/
# cp pk12util /usr/bin/mps/
```

6. **为** `/usr/bin/mps/` **目录中的二进制文件启用执行权限。**

```
# chmod 544 /usr/bin/mps/*
```

配置 Sun ONE Application Server 7

本节介绍以下过程：为应用程序服务器例程创建信任数据库；向应用程序服务器注册板；生成并安装服务器证书；启用应用程序服务器以使用 SSL 和 TLS。

在配置过程中， Sun ONE Application Server 管理服务器必须开启并运行。

▼ 创建信任数据库

1. **启动 Sun ONE Application Server 和 Sun ONE Application Server 管理服务器。**

```
# installation-directory/bin/asadmin start-appserv
```

注 – 显示的消息将表明应用程序服务器正在运行。

2. **打开 Web 浏览器并输入以下 URL 来启动管理 GUI:**

```
http://hostname:4848
```

在验证对话框中，输入您在运行 `setup` 程序时创建的 Sun ONE Application Server 用户名和密码。

注 – 如果您在设置 Sun ONE Application Server 期间使用的是默认设置，请键入 `admin` 作为用户 ID 或 Sun ONE Application Server 管理服务器用户名。

3. **单击 “OK”。**

4. **创建应用程序服务器例程的信任数据库。**

   您可能想为多个应用程序服务器例程启用安全保护功能。如果是这样，请对每一个应用程序服务器例程重复步骤 1 至步骤 4。

注 – 如果您还想在 Sun ONE 应用程序服务器管理服务器上运行 SSL 功能，则此过程与设置信任数据库的过程类似。有关详细信息，请访问 `http://docs.sun.com/source/816-7158-10/` 处提供的 《*Sun ONE Application Server 7 Administrator's Guide*》

---

   a. **浏览至 “管理 GUI” 的 “Manage Database” 部分。**

      在左窗格中选择“Security”链接，并在右窗格中单击“Manage Database”选项卡。

   b. **在两个文本框中键入至少八个字符的密码，然后单击 “OK”。**

      此密码是 Sun ONE Application Server 的信任数据库密码。当应用程序服务器在安全模式下运行时，此密码用于启动内部加密模块。

▼ 向应用程序服务器注册板

1. **运行 `iplsslcfg` 脚本，以向应用程序服务器注册板。**

```
# /opt/SUNWconn/cryptov2/bin/iplsslcfg
```

   此脚本会提示您选择服务器并为所选的 Sun ONE 服务器安装 Sun Crypto Accelerator 4000 加密模块。然后，脚本会更新配置文件以启用板。

2. **键入 2 以选择 Sun ONE Application Server，然后输入二进制文件路径和域路径。**

注 – 本节中的过程假定您在此提示时选择选项 2。如果希望选择选项 3 或 4，请参阅第 84 页 “使用 iplsslcfg 脚本”。

```
Sun Crypto Accelerator Sun ONE Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

Your selection (0 to quit): 2
```

3. **键入二进制文件和域的位置，以及域和服务器的名称。**

```
You will now be prompted for four pieces of information:
 1. The location of the Sun ONE Application Server binaries
 2. The location where Sun ONE Server domains are stored
 3. The Application Server domain (e.g. domain1)
 4. The Application Server server name (e.g. server1)

Full path to Application Server binaries: [/opt/SUNWappserver7]:
/opt/SUNWappserver7
Full path to Application Server domains:
[/var/opt/SUNWappserver7]: /var/opt/SUNWappserver7
Application Server domain: domain1
Application Server server name: server1
This script will update your Sun ONE Application Server
installation in /opt/SUNWappserver7 to use the Sun Crypto
Accelerator.
You will need to restart your admin server after this has
completed.
Ok to proceed? [Y/N]: y
Using database directory
/var/opt/SUNWappserver7/domains/domain1/server1/config...
Module "Sun Crypto Accelerator 4000" added to database.
/opt/SUNWappserver7 has been configured to use
the Sun Crypto Accelerator.

<Press ENTER to continue>
```

注 – 默认的安装目录可能会有所不同，具体取决于您的 Sun ONE Application Server 7 版本。

4. **键入** `0` **退出。**

▼ 生成服务器证书

1. **浏览至 “管理 GUI” 的 “Certificate Management” 部分。**

   选择左窗格中的 “Security” 链接，并选择右窗格中的 “Certificate Management” 选项卡。您现在位于 “管理 GUI” 的 “Certificate Management” 部分的 “Request” 子菜单窗口中。

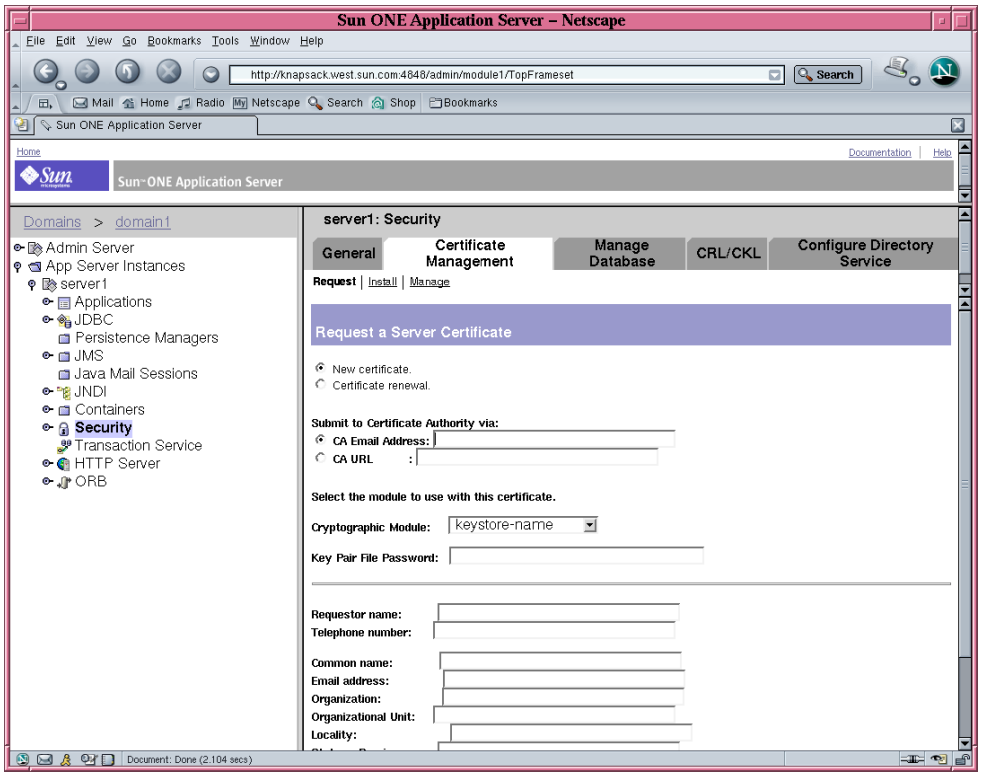

图 5-6 Sun ONE Application Server 管理服务器的申请服务器证书对话框

2. **使用以下信息填写表单以生成证书申请：**

   a. **选择一个新证书。**

      如果您可以直接将证书申请发送到可通过 Web 访问的认证机构或注册机构，请选择 “CA URL” 链接。否则，请选择 “CA Email Address”，然后输入您要将证书申请发送至的电子邮件地址。

   b. **选择您要使用的 “Cryptographic Module”。**

      此下拉菜单中包含每一个密钥库的条目。务必选择正确的密钥库。不要选择 “SUNW acceleration only”。

c. 在 “Key Pair File Password” 对话框中，为将要拥有密钥的用户输入密码。

此密码为 *username:password* （参见表 5-1）。

d. 在表 5-6 列出的申请人信息字段中输入正确的信息。

表 5-6 申请人信息字段

字段	说明
Requestor Name	申请人的联系信息
Telephone Number	申请人的联系信息
Common Name	在来访者的浏览器中键入的 Web 站点域
Email Address	申请人的联系信息
Organization	公司名称
Organizational Unit	（可选）公司部门
Locality	（可选）城市、郡县、公国或国家/地区
State	（可选）省/州的全称
Country	由两个字母组成的国家/地区 ISO 代码 （例如，中国为 CN）

e. 单击 “OK” 提交信息。

3. 利用认证机构生成证书。

- 如果已选择将证书申请发送给 CA URL，则证书申请会自动发送到该处。
- 如果已选择 “CA Email Address”，请复制通过电子邮件发送给您的证书申请及标题，然后将其交给证书机构。

4. 一旦生成证书，请将证书及标题一起复制到剪贴板上。

注 – 证书通常以文本格式向您提供，这与证书申请不同。请将此数据保留在剪贴板上，以便在第 130 页 “安装服务器证书” 的步骤 4 中使用。

▼ 安装服务器证书

1. **在管理 GUI 右窗格中的 “Certificate Management” 部分，选择 “Install” 链接。**
   您现在位于 “管理 GUI” 的 “Certificate Management” 部分的 “Request” 子菜单窗口中。

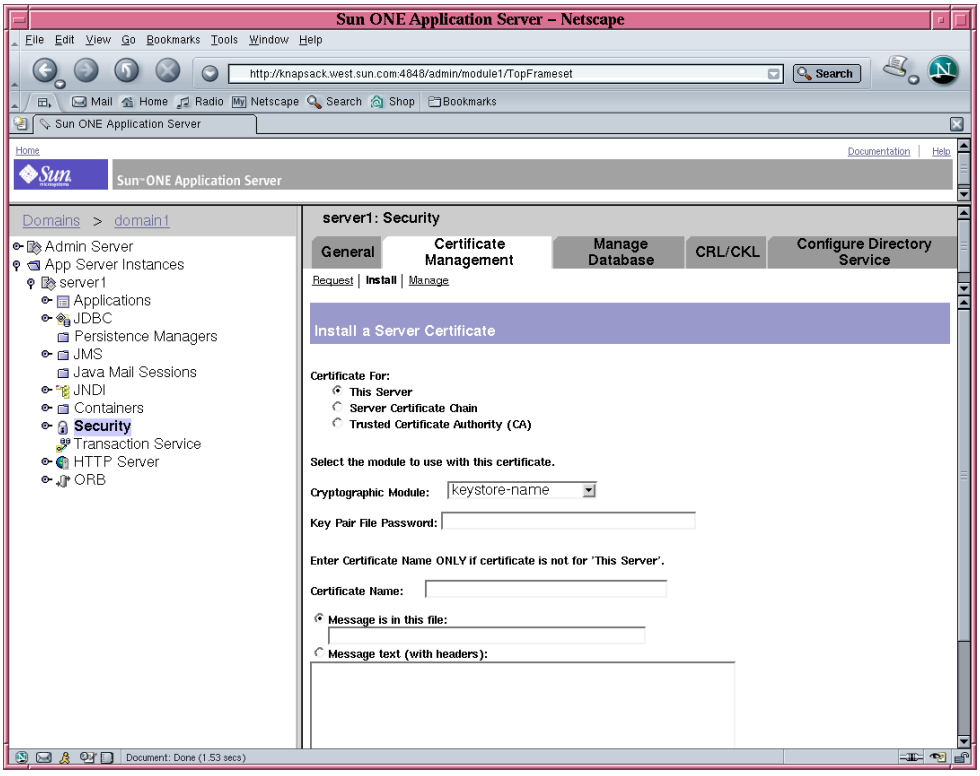

图 5-7 Sun ONE Application Server 管理服务器的安装服务器证书对话框

2. **填写表单，安装证书：**

表 5-7 要安装证书的字段

字段	说明
Certificate For	本服务器。
Cryptographic Module	此下拉菜单中包含每一个密钥库的条目。务必选择正确的密钥库名称。要使用 Sun Crypto Accelerator 4000 板，所选择模块的名称必须与您在申请证书时选择的名称相同。
Key Pair File Password	此密码为 *username:password*。
Certificate Name	多数情况下，您可以将此字段留空。如果提供一个名称，该名称将会改变应用程序服务器在运行 SSL 支持时用来访问证书和密钥的名称。此字段的默认值为 `Server-Cert`。

3. **选择 “Message text (with headers)”单选按钮。**

4. **单击 “Message text (with headers)”单选按钮，并将从认证机构复制的证书 （第 128 页 “生成服务器证书”的步骤 4）复制到单选按钮下方的文本框内。**

5. **单击 “OK”。**

   屏幕上会显示证书的一些基本信息。

6. **如果输入的内容正确无误，请单击 “Add Server Certificate”。**

   系统会提示您重新启动应用程序服务器。此时，请不要重新启动应用程序服务器，因为它将在 SSL 配置完毕后重新启动。另外，系统还会提示您，为使应用程序服务器使用 SSL，必须对应用程序服务器进行适当的配置。

▼ 启用应用程序服务器以使用 SSL

1. **在终端窗口中键入以下命令。**

   此外，还必须在执行此命令之后键入 Sun ONE Application Server 管理服务器的密码。

注 – 如果您在本地主机上运行此命令，并且 Sun ONE Application Server 管理服务器已配置为使用默认端口 4848，则可以忽略 `--host` *hostname* `--port` *administration-server-port* 参数。

```
# installation-directory/bin/asadmin create-ssl --user app-admin --host
hostname --port administration-server-port --type http-listener --certname
keystore-name:server-certificate-name --instance server-name http-listener
password>
```

2. **在 “管理 GUI” 的左窗格中，选择 “HTTP Server” 链接左侧的扩展图标。**
   屏幕上会显示 “HTTP Server” 子菜单项。

3. **选择 “HTTP Server” 链接下方的 “HTTP Listeners” 子菜单项。**

4. **在右窗格中，选择您希望为 SSL/TLS 配置的 HTTP 监听程序，并选择该 HTTP 监听程序的相关链接。**
   屏幕上会显示一个窗口，从中您可以编辑 HTTP 监听程序的属性。

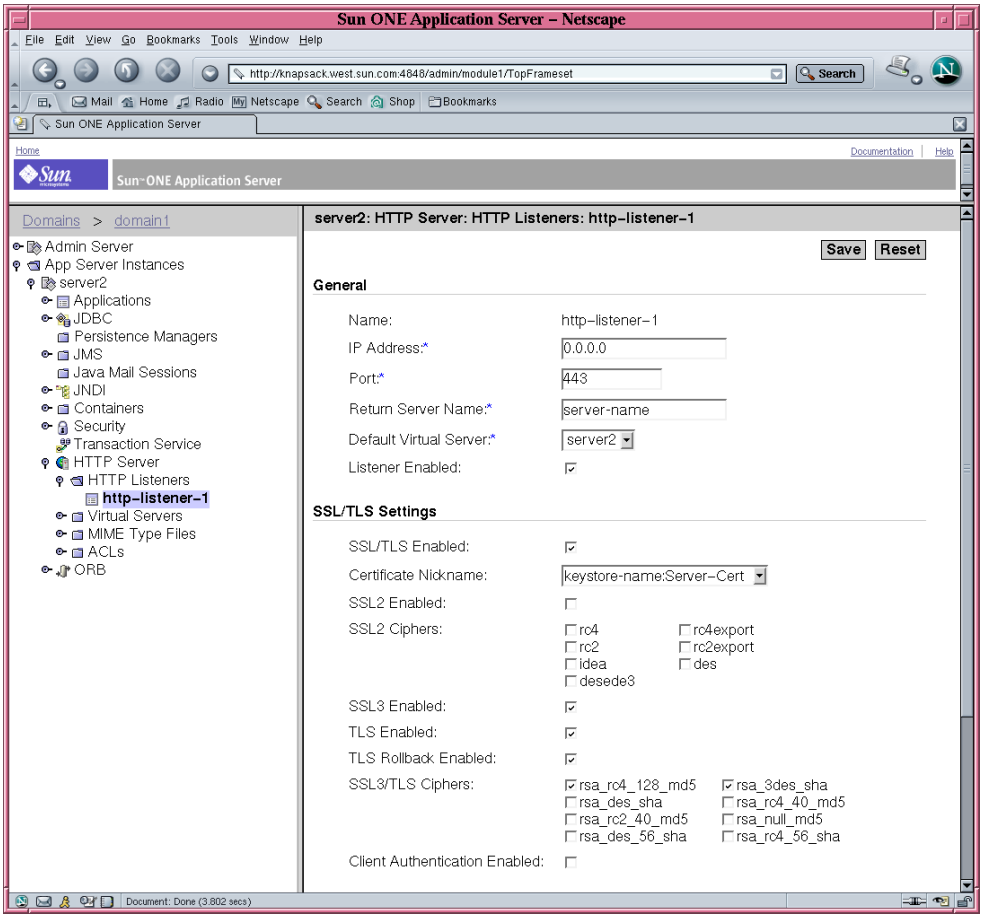

图 5-8 Sun ONE Application Server 管理服务器的 HTTP 监听程序属性对话框

5. **对于 “SSL/TLS Settings”，验证 “Certificate Nickname” 是否与您在步骤 1 的第 131 页 “启用应用程序服务器以使用 SSL” 中，通过命令的 `--certname` 选项所选的证书别名一致。**

6. **至少选中以下复选框：**
   - SSL/TLS Enabled
   - SSL3 Enabled
   - TLS Enabled
   - TLS Rollback Enabled
   - SSL3/TLS Ciphers：`rsa_rc4_128_md5` 和 `rsa_3des_sha`
7. **设置端口 — 通常为 443。**
8. **要使用回滚，还必须在访问您的服务器的浏览器中启用 TLS。**
   - 对于 Netscape Navigator 6.0，应选中 “TLS”和 “SSL3”。
   - 对于 Microsoft Internet Explorer 5.0 和 5.5，使用 “TLS Rollback”选项。
   - 对于 “TLS Rollback”，应选中 “TLS”并确保禁用 “SSL3”和 “SSL2”。
9. **单击 “Save”。**
10. **选择 “App Server Instances”并在左窗格中选择服务器例程，然后在右窗格中选择 “Apply Changes”。**
11. **停止并启动服务器以使更改生效。**

    `init.conf` 文件会自动进行修改以使 “Security”显示为 “On”，并且所有虚拟服务器会自动指定默认的安全参数。

    在服务器上启用 SSL 后， URL 将使用 `https` 而不使用 `http`。指向已启用 SSL 的服务器上的文档的 URL 具有如下格式：

```
https://server-name.domain.dom:port-number
```

    例如：

```
https://admin.sun.com:443
```

注 – 如果使用默认的安全 HTTP 端口号 (443)，则无需在 URL 中输入此端口号。

有关说明，请参阅以下网站提供的《*Sun ONE Application Server 7 Administrator's Guide to Security*》中的 “启用 SSL/TLS”章节：
`http://docs.sun.com/source/816-7158-10/sgencryp.html#14403`

安装和配置 Sun ONE Directory Server 5.2

本部分介绍如何安装和配置 Sun ONE Directory Server 5.2 以使用板。您必须按顺序执行这些步骤。有关使用 Sun ONE Directory Server 的详细信息，请参阅 Sun ONE Directory Server 文档。本部分包括以下过程：

安装 Sun ONE Directory Server 5.2

此过程将从命令行中安装目录服务器软件。

▼ 安装 Sun ONE Directory Server 5.2

1. **下载 Sun ONE Directory Server 5.2 软件。**
   以下 URL 提供了该目录服务器软件：`http://www.sun.com/`
2. **切换至安装目录。**
3. **执行 `./idsktune` 命令，确保已安装了推荐的修补程序。**
4. **解压目录服务器软件。**
5. **执行 `setup` 脚本以安装软件。**

注 – 无需分别安装各个软件包，因为 `setup` 脚本会安装所有软件包。

安装之后， Sun ONE Directory Server 和管理服务器会自动启动。

手动启动 Directory Server

1. **切换至启动目录。**

```
# cd /var/Sun/mps
```

2. **执行** `start-admin` **命令。**

```
# ./start-admin
```

3. **切换至** `slapd-`*servername* **目录。**

```
# cd slapd-servername
```

其中 *servername* 是例程名。

4. **键入** `start-slapd` **命令。**

```
# ./start-slapd
```

配置 Sun ONE Directory Server 5.2

本节包括以下过程：为目录服务器例程创建信任数据库；向目录服务器注册板；生成并安装服务器证书；查看和安装主要 CA 证书；以及启用目录服务器以使用 SSL。

在配置过程中，配置目录和 Sun ONE Directory Server 管理服务器必须开启并运行。

▼ 创建信任数据库

此过程用于添加 Sun Crypto Accelerator 4000 模块，同时适用于 32 位安装和 64 位安装。

1. **启动目录服务器控制台。**
2. **在控制台主窗口中选择要配置的目录服务器例程，并选择 “Open”。**
3. **在出现的新窗口中，选择 “Console” → “Security” → “Manage Certificates”。**
此步骤将为目录服务器例程创建信任数据库。

a. **选择密码并输入到两个框中，然后单击 “OK”（参见**图 5-9**）。**

b. **关闭随后出现的 “Manage Certificates”对话框。**

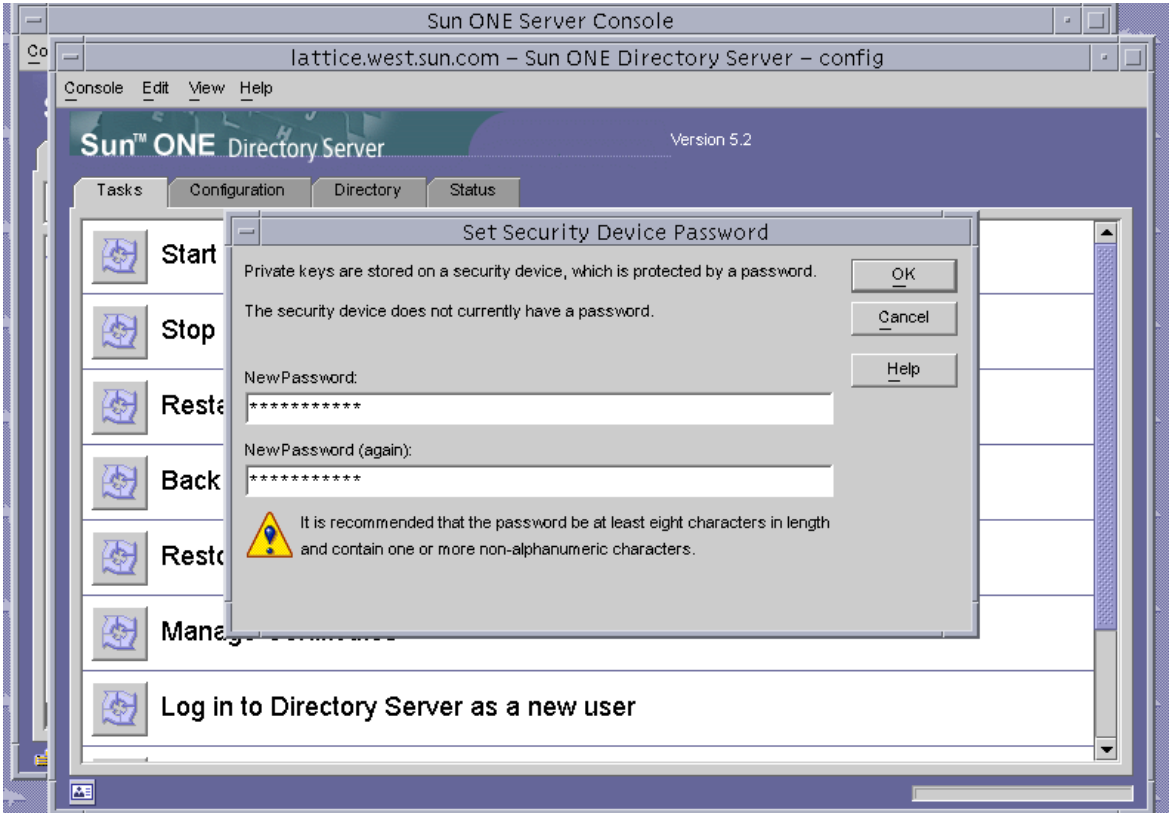

图 5-9 Sun ONE Directory Server 的设置安全设备密码对话框

4. **在弹出的新窗口中，选择 “Console” → “Security” → “Configure Security Modules”。**

a. **单击 “Install”。**

b. **在 “*Enter the PKCS#11 module driver filename*”条目中，键入以下路径：**

```
/opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

5. 在 “*Enter an identifying name for this module* 条目中，输入名称，例如：

```
Sun Crypto Accelerator 4000
```

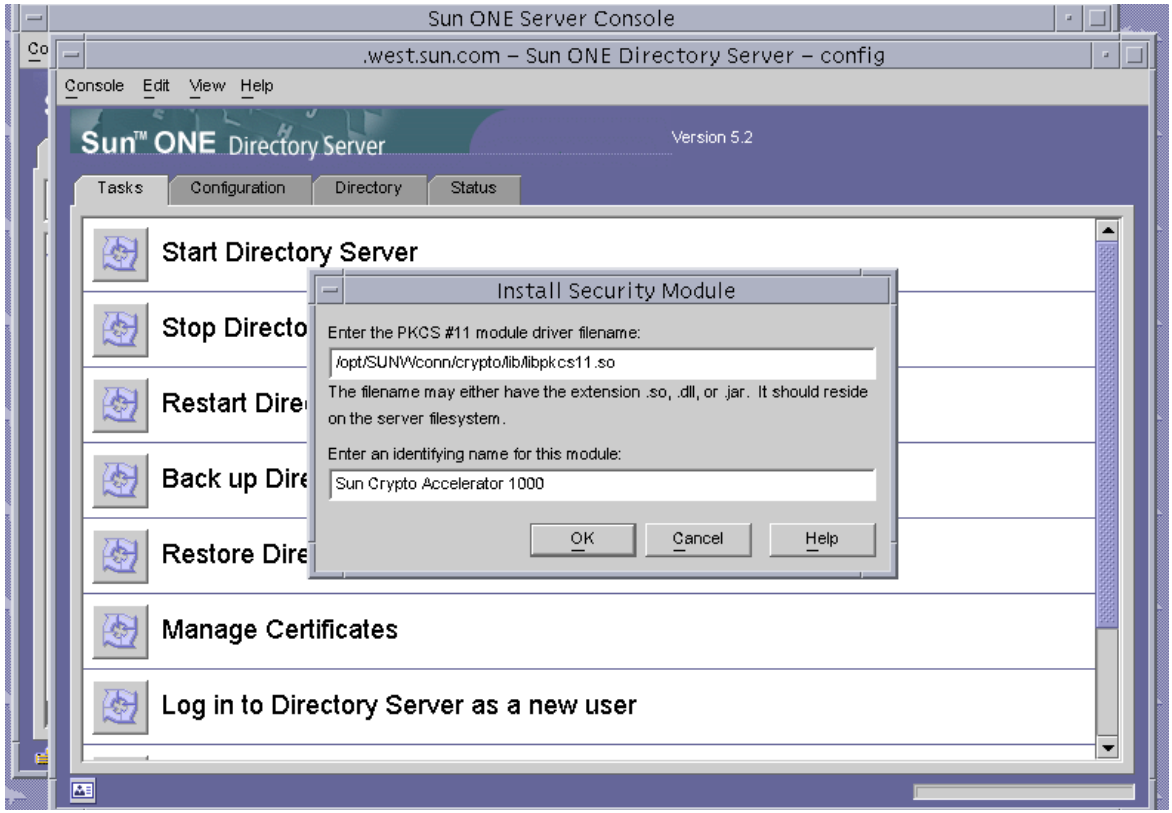

图 5-10 Sun ONE Directory Server 的安装安全模块对话框

6. **单击 “OK”。**

▼ 向目录服务器注册板 （32 位）

此过程将通过命令行添加 32 位板模块。

1. **键入以下命令，设置适当的路径。**

```
# setenv LD_LIBRARY_PATH server-inst/lib:${LD_LIBRARY_PATH}
```

2. **将板添加到** secmod.db **数据库中。**

   a. **切换至以下目录：**

```
# cd server-inst/alias
```

   b. **使用** modutil **实用程序添加程序库。**

```
# server-inst/shared/bin/modutil -dbdir . -nocertdb -add "Sun Crypto Acclerator
4000" -libfile /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

▼ 向目录服务器注册板 （64 位）

此过程将通过命令行添加 64 位板模块。

1. **从** http://www.mozilla.org **网站上获取 64 位版本的 Netscape Security Services (NSS) 实用程序。**

```
ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_3_2_RTM/SunO
S5.8_64_OPT.OBJ/
```

保存 nss-3.3.2.tar.gz tar 文件。

2. **键入以下命令，设置适当的路径。**

注 – 本节中，*server-inst* 是指产品的根安装目录，*nss64-inst* 指您安装 64 位版本的 NSS 工具的位置。

```
# setenv LD_LIBRARY_PATH server-inst/lib/64:${LD_LIBRARY_PATH}
```

3. **将板添加到** secmod.db **数据库中。**

   a. **切换至** alias **目录：**

```
# cd server-inst/alias
```

   b. **添加程序库。**

```
# nss64-inst/bin/modutil -dbdir . -nocertdb -add "Sun Crypto Acclerator 4000"
-libfile /opt/SUNWconn/cryptov2/lib/64/libvpkcs11.so
```

生成并安装服务器证书

除表 5-8 中介绍的不同路径变量之外，此过程对于所安装的 32 位和 64 位版本的 PKCS#11 程序库是相同的。

表 5-8 32 位和 64 位路径变量区别

变量定义	32 位	64 位
LD_LIBRARY_PATH	*server-inst*/lib	*server-inst*/lib/64
NSS 工具的位置	*server-inst*/shared/bin	*nss64-inst*（无论将 NSS 工具安装在何处）

表 5-9 介绍了本节中的 certutil 命令所用的变量。

表 5-9 certutil 变量说明

变量	说明
token-name	PKCS#11 令牌的名称；即您在初始化板时选择的密钥库名称。
subject-name	数字证书上声明的名称，通常格式如下： CN=*Fully-Qualified-Domain-Name*, OU=*Organization-Unit*, O=*Organization.* 名称会因组织而异。
output-file	证书申请的位置。
certfile	ASCII 编码证书的位置。
instname	目录服务器例程名称。
nickname	用户选择的容易记忆的服务器证书名称。

▼ 生成服务器证书

1. **切换至以下目录。**

```
# cd server-inst/alias
```

2. **申请证书。**

```
# certutil -R -d . -h token-name -s "subject-name" -a -o output-file [-g key-size] -P
slapd-instname-
```

3. **将 *output-file* 中的证书申请提交给您选择的认证机构。**

   将 base64 编码的证书放入名为 *certfile* 的文本文件中。

▼ 安装服务器证书

1. **安装服务器证书。**

```
# certutil -A -d . -h token-name -t "Pu,Pu,Pu" -P slapd-instname- -a -i certfile -n
nickname
```

查看和安装主要 CA 证书

Sun ONE Directory Server 包含了一些广为人知且倍受信任的 Root Certificate Authority（主要认证机构）证书。如果您的服务器证书由这些著名的主要认证机构签发，请跳过此过程。

▼ 查看目录服务器已识别的主要认证机构 CA 证书

1. **从目录服务器控制台窗口中，打开板的目录服务器例程。**
2. **从控制台窗口顶部的菜单中，选择 “Console” → “Security” → “Manage Certificates”。**
3. **选择 “Manage Certificates”窗口顶部的 “CA Certs”选项卡。**

   此时会显示 Sun ONE Directory Server 例程已识别的 CA 证书列表。您可以突出显示某个条目，然后单击 “Detail”按钮来查看特定 CA 证书的详细信息。

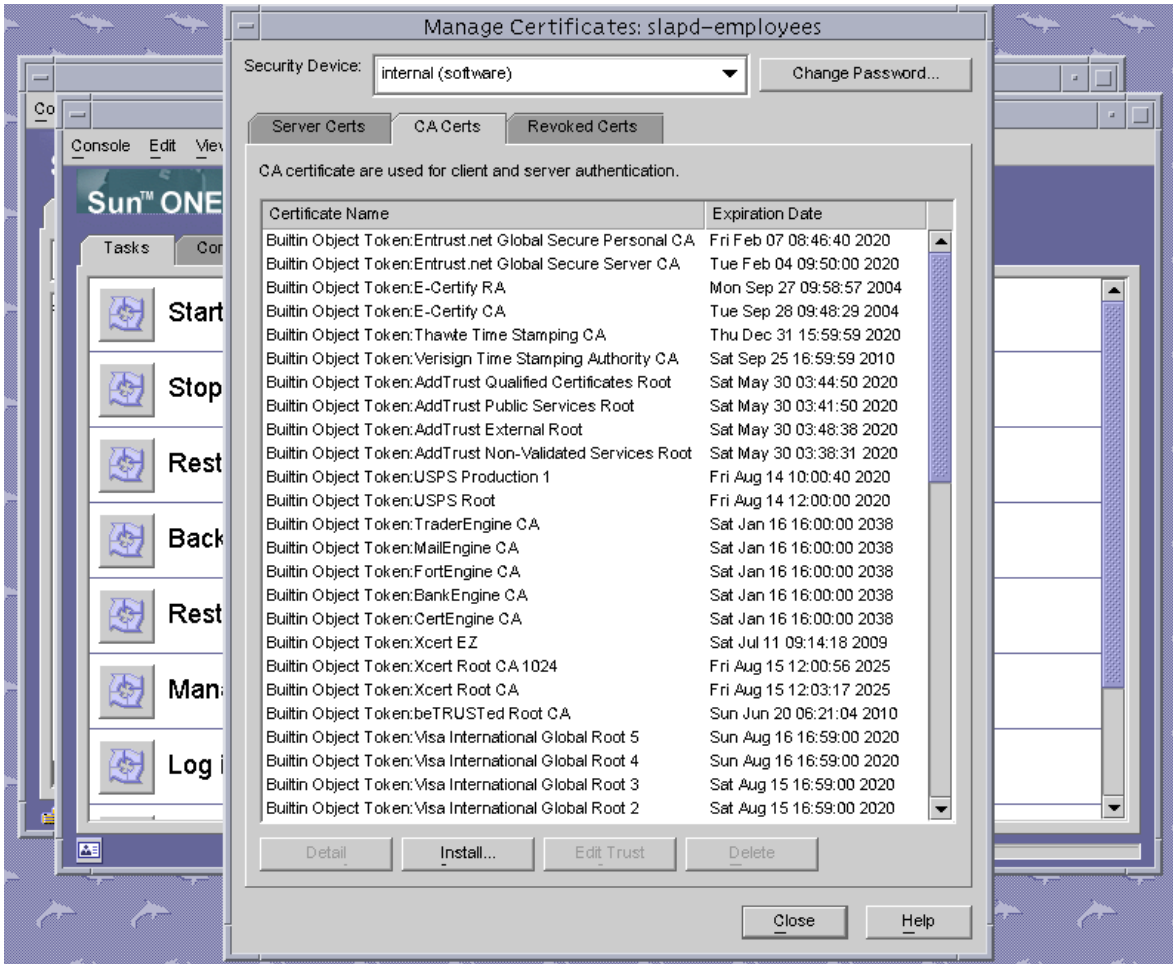

图 5-11 Sun ONE Directory Server 的管理证书对话框

▼ 安装主要 CA 证书

仅当您从专属 PKI（proprietary PKI）获取证书时才可执行以下过程。也就是说，如果您使用 VeriSign、 Thawte 或 GTE，则不要执行此过程。如果证书由主要供应商签发，并且它们的间接 CA 未列在 Sun ONE 默认的信任 CA 列表中，则使用此过程。

1. **切换至 `alias` 目录。**

```
# cd server-inst/alias
```

2. **安装主要 CA 证书。**

注 – 如果安装多个 CA 证书，请使用不同的 `-n` 值。如果使用相同的 `-n` 值，则证书会相互覆盖。使用 CA 证书主题名的 CommonName 组件替换 `CA-Cert`（在 SubjectName 中查找 CN=）。

```
# certutil -A -d . -P slapd-instname- -n "CA-Cert" -t "CT,CT,CT" -a -i path-to-ca-cert
```

▼ 启用目录服务器以使用 SSL

1. **启动目录服务器控制台（如果尚未启动）。**

```
# ./cd server-root
# ./startconsole
```

2. **在控制台主窗口的左窗格中，双击板的目录服务器例程，以打开目录服务器例程。**
3. **在控制台主窗口中单击 “Directory” 选项卡。**
4. **在 “Directory” 选项卡的左窗格中打开 `cn=config` 条目，并修改以下参数（参见** 图 5-12**）：**

   a. **将 `nsslapd-security` 设为 “On”。**

   b. **将 `nsslapd-secureport` 设为所需的端口（默认端口为 636）。**

c. 单击 “OK”。

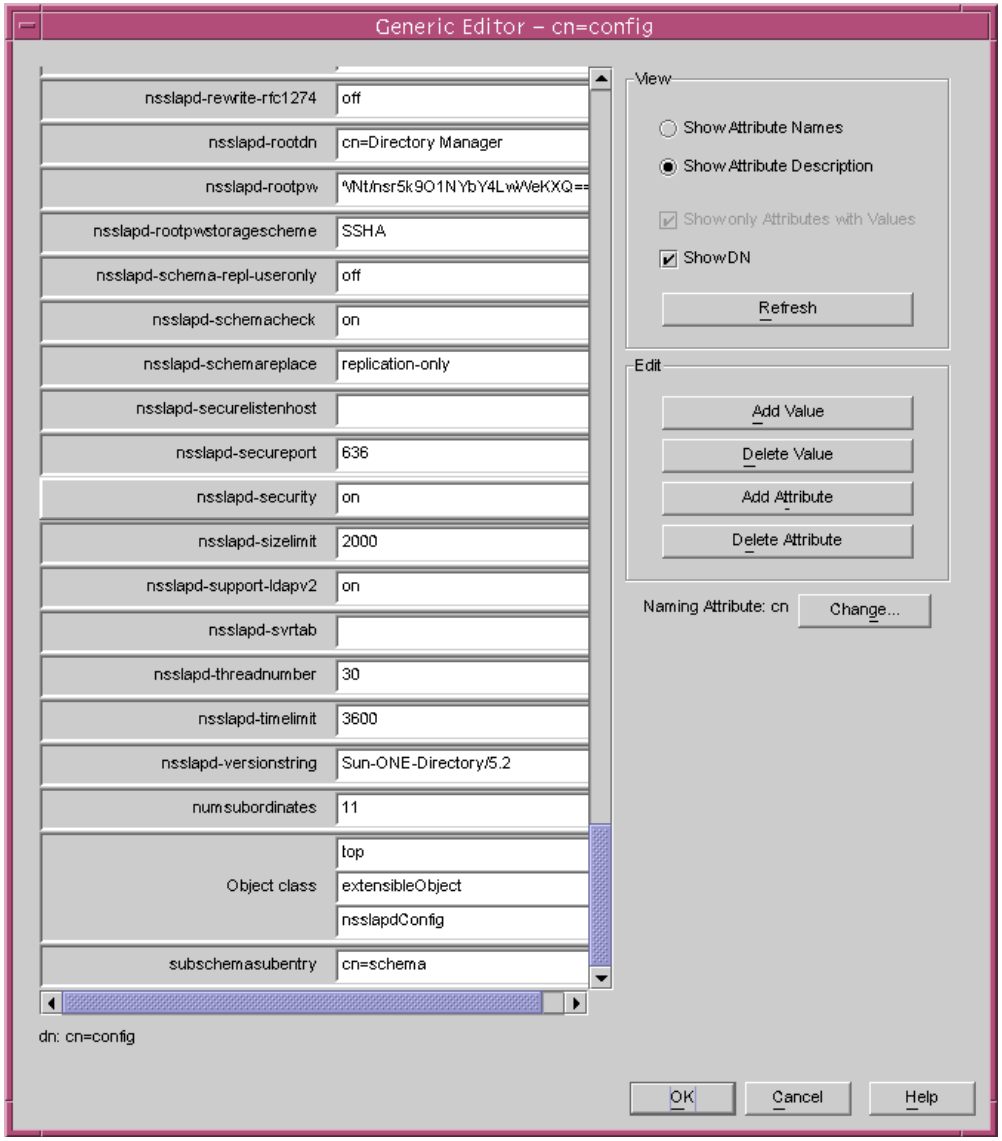

图 5-12 Sun ONE Directory Server 的 `cn=config` 编辑器对话框

5. **在控制台主窗口的左窗格中打开** `cn=encryption,cn=config` **条目，并修改以下参数（参见**图 5-13**）：**

   a. **将** `nssslЗ` **设为 “On”**。

   b. **使用 “Add Attribute” 按钮添加值为** `alias/slapd-`*instname*`-cert8.db` **的** `nsCertFile`。

   c. **使用 “Add Attribute” 按钮添加值为** `alias/slapd-`*instname*`-key3.db` **的** `nsKeyFile`。

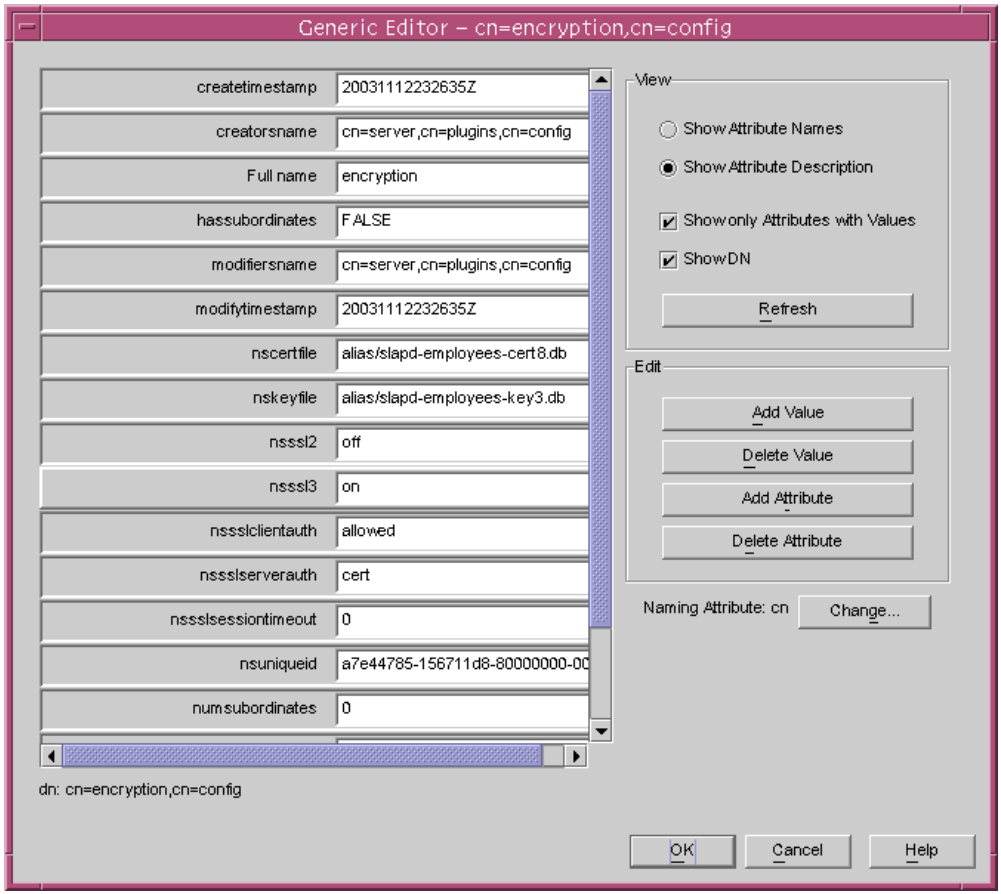

图 5-13 Sun ONE Directory Server 的 `cn=encryption,cn=config` 对话框

   d. **单击 “OK”**。

6. **在 `cn=encryption,cn=config` 下方的数据库中创建新条目。**

   a. **在主窗口中，右键单击加密图标，然后从菜单中选择 “New” → “Other”。**

   b. **选择 `nsEncryptionModule`。**

   c. **将 “Full Name” 属性的值从 “New” 更改为 “RSA”（远程安全访问）（参见** 图 5-14）。

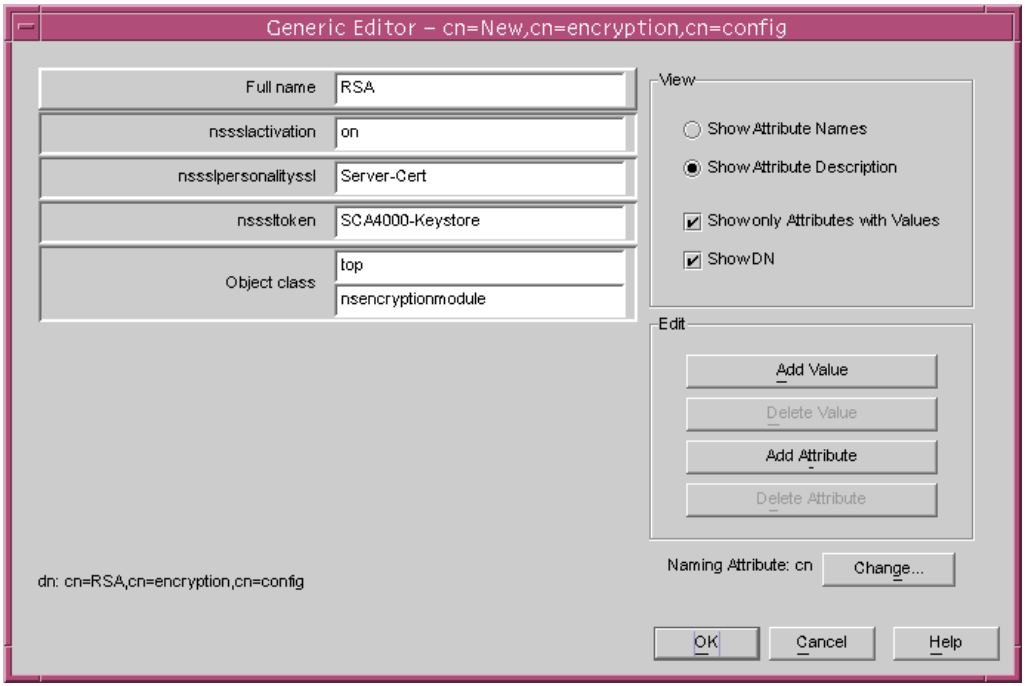

图 5-14 Sun ONE Directory Server 的 `nsEncryption` 模块对话框

   d. **使用 “Add Attribute” 按钮添加以下属性和值：**

`nsssltoken`	*token-name*
`nsslpersonalityssl`	*nickname*
`nssslactivation`	`on`

   e. **单击 “OK”。**

安装和配置 Sun ONE Messaging Server 5.2

本部分介绍如何安装和配置 Sun ONE Messaging Server 5.2 以使用板。您必须按顺序执行这些步骤。有关安装和使用 Sun ONE Messaging Server 的详细信息，请参阅 Sun ONE Messaging Server 文档。本部分介绍以下主题：

安装 Sun ONE Messaging Server 5.2

此过程将从命令行中安装 Sun ONE Messaging Server 5.2。

▼ 安装 Sun ONE Messaging Server 5.2

1. **下载 Sun ONE Messaging Server 5.2 软件。**
   以下 URL 提供了该消息服务器软件：`http://www.sun.com/`
2. **切换至安装目录并解压消息服务器软件。**
3. **使用 `setup` 脚本安装消息服务器软件。**
   a. **提示时键入安装路径。**
   b. **提示时键入希望安装的组件。**
   c. **执行 `./setup` 命令以安装组件。**

配置 Sun ONE Messaging Server 5.2

本节介绍以下过程：为消息服务器例程创建信任数据库；向消息服务器注册板；生成并安装服务器证书；以及启用消息服务器以使用 SSL。

在配置过程中，配置目录和 Sun ONE Messaging Server 管理服务器必须开启并运行。

▼ 创建信任数据库

1. **启动消息服务器控制台。**
2. **打开 Sun ONE Messaging Server 例程。**
   此时会出现图 5-15 所示的菜单：

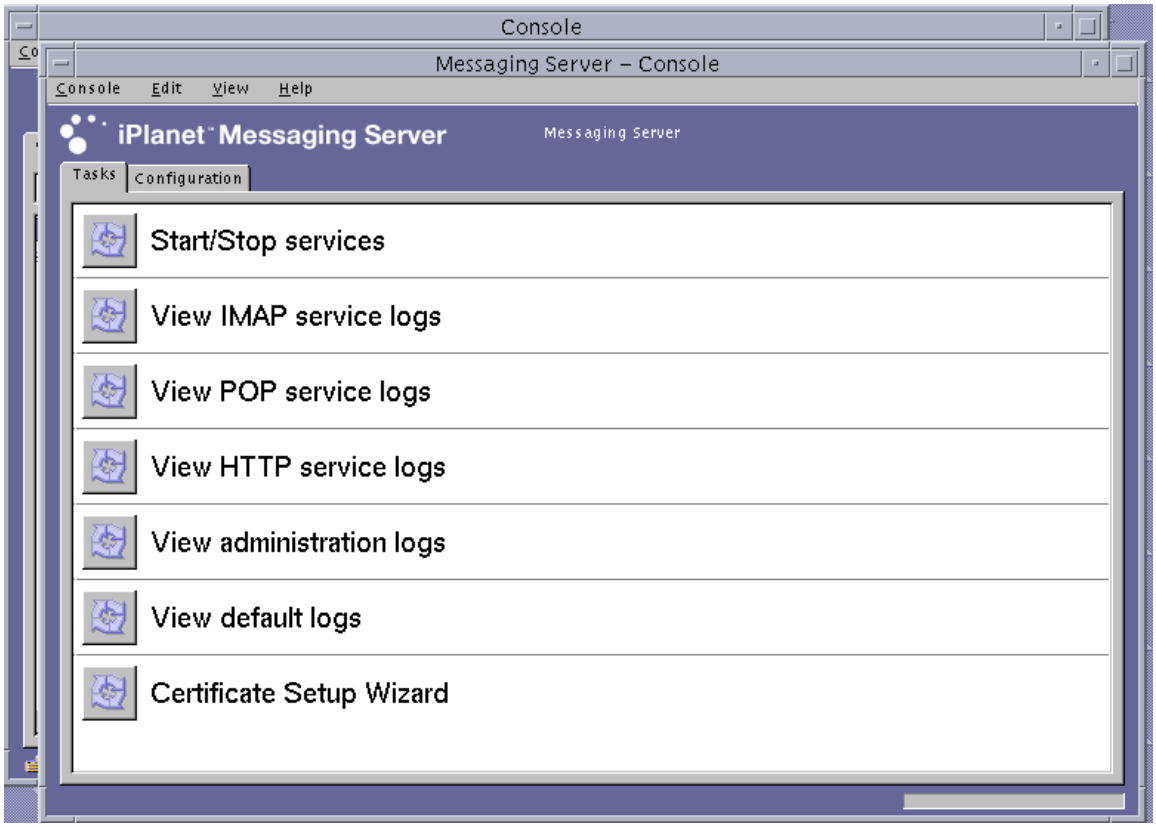

图 5-15 Sun ONE Messaging Server 控制台主窗口

3. **选择 “Console” → “Certificate Setup Wizard”。**
   屏幕上会显示 “Certificate Setup Wizard” 窗口。
   a. **单击 “Next”。**
   b. **选择 “internal (software)” 令牌。**
   c. **选择 “Do not install a certificate”，然后单击 “Next”。**
   d. **单击 “Next”。**

e. 为内部数据库设置密码，然后单击 “Next”。

f. 单击 “Done”。

▼ 向消息服务器注册板

1. 切换至以下目录。

```
# cd server-root/shared/bin
```

2. 确保 LD_LIBRARY_PATH **变量设置正确。**

```
# setenv LD_LIBRARY_PATH server-root/lib:${LD_LIBRARY_PATH}
```

3. 将板模块添加到 secmod.db **数据库中。**

```
# ./modutil -dbdir ../../admin-serv/config \
-nocertdb \
-add "Sun Crypto Accelerator 4000" \
-libfile "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
```

▼ 生成服务器证书

1. 选择 “Console” -> “Certificate Setup Wizard”，打开证书安装向导，以让消息服务器控制台来申请证书。

a. 单击 “Next”。

b. 选择与您要在其中存储密钥的 Sun Crypto Accelerator 4000 令牌相匹配的令牌，如 图 5-16 **中所示。**

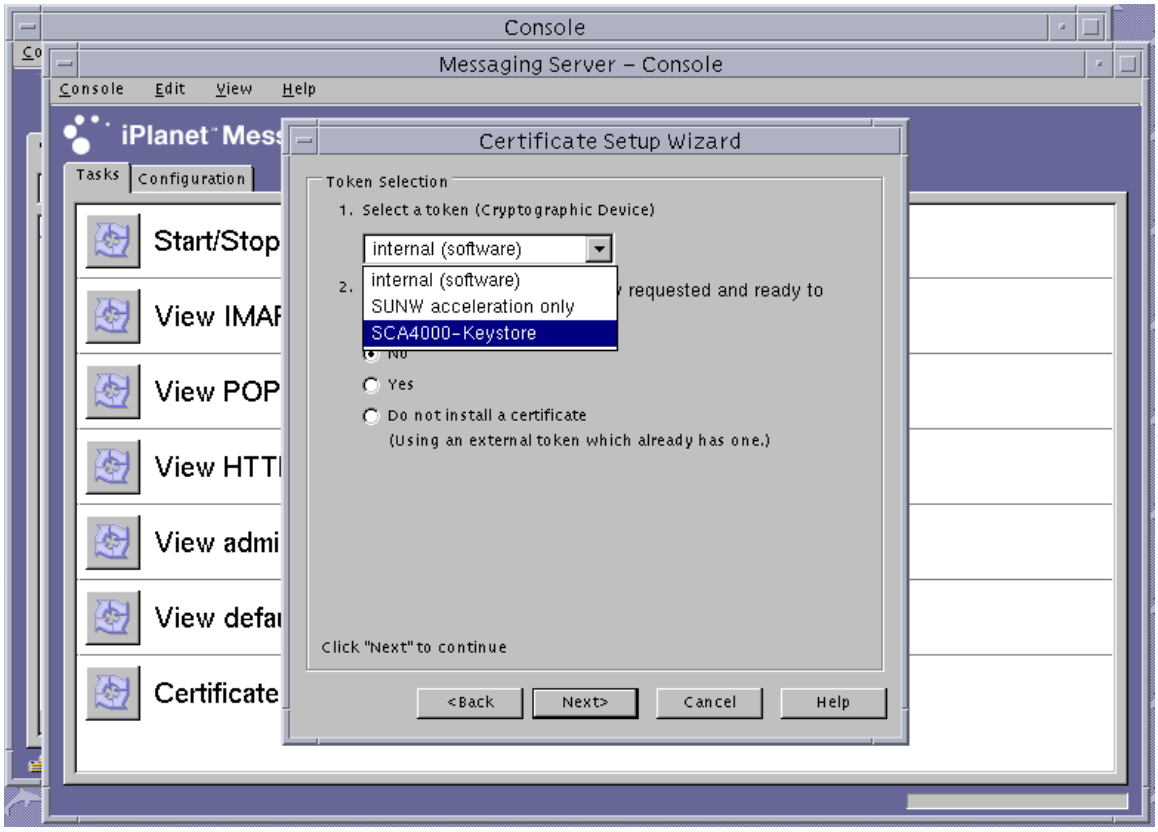

图 5-16 Sun ONE Messaging Server 的证书安装向导令牌选择对话框

c. 对 “Is the certificate already requested and ready to install?” 回答 “No”，然后单击 “Next”。

d. 单击 “Next”。

e. **选择 “New Certificate”，然后选择将证书申请提交给认证机构的方法 （电子邮件或 HTTPS）（**图 5-17**），然后单击 “Next”。**

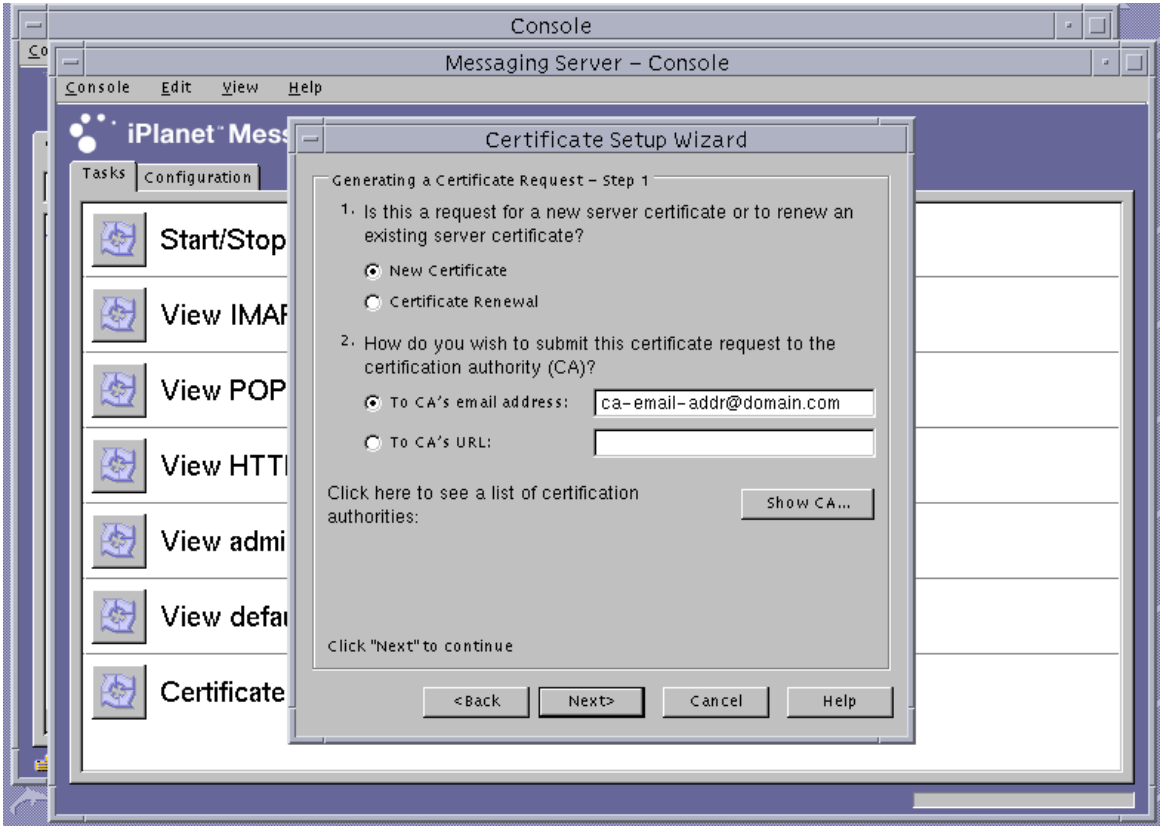

图 5-17 Sun ONE Messaging Server 的证书安装向导证书申请对话框

f. 在表 5-10 **列出的申请人信息字段中输入正确的信息，然后单击 “Next”。**

表 5-10 申请人信息字段

字段	说明
Requestor Name	申请人的联系信息
Telephone Number	申请人的联系信息
Common Name	在来访者的浏览器中键入的 Web 站点域
Email Address	申请人的联系信息
Organization	公司名称

表 5-10 申请人信息字段 *（续）*

字段	说明
Organizational Unit	（可选）公司部门
Locality	（可选）城市、郡县、公国或国家/地区
State	（可选）省/州的全称
Country	由两个字母组成的国家/地区 ISO 代码 （例如，中国为 CN）

g. 此时，系统会要求您输入在创建信任数据库时使用的密码。改为输入密钥库用户的密码 (*username:password*)，然后单击 “Next”。

有关 *username:password* 的详细信息，请参见表 5-1。

h. 如果在步骤 e 中选择了 HTTPS 方法，则申请已发送到认证机构。如果在步骤 e 中选择了电子邮件方法，请单击 “Copy to Clipboard”，然后单击 “Next”（图 5-18）。

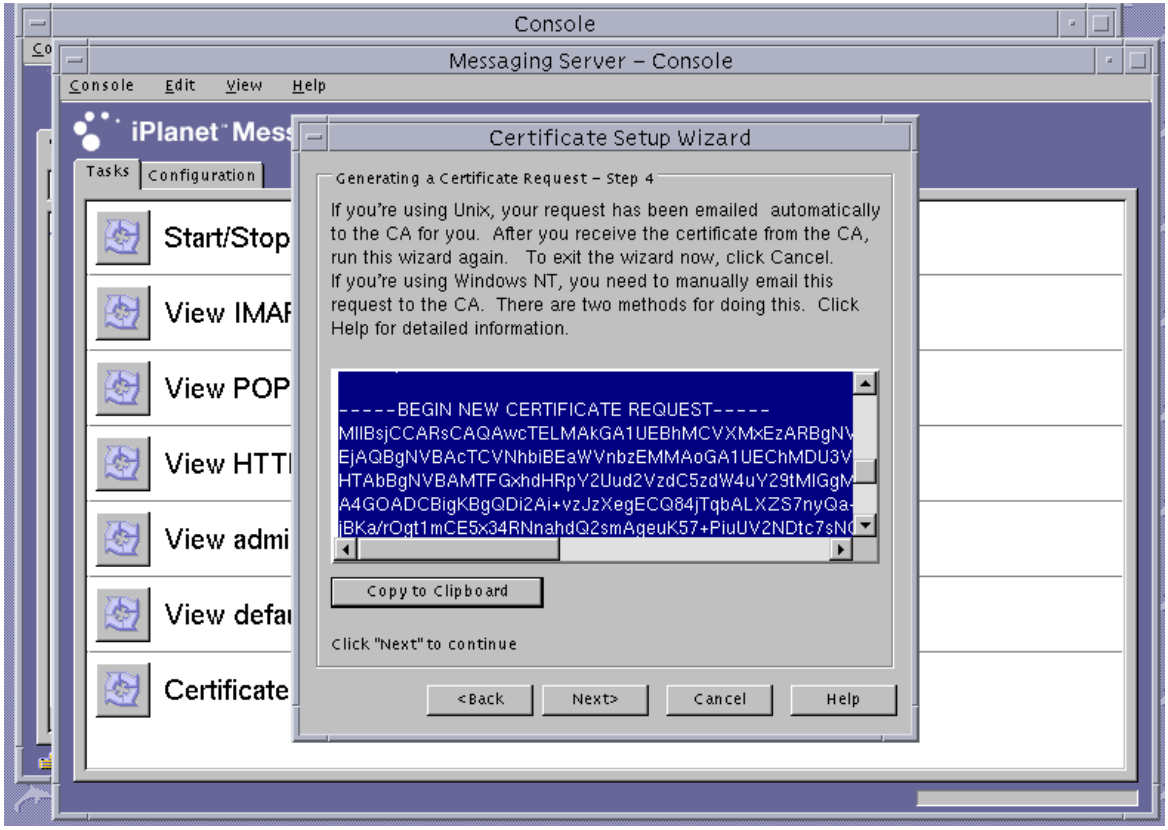

图 5-18 Sun ONE Messaging Server 的证书安装向导证书发送对话框

i. 单击 “Next”。

注 – 申请证书之后，证书安装向导会继续运行，以便您将已签发的证书安装到 Sun Crypto Accelerator 4000 密钥库中。如果您在生成证书之后 （且在安装证书之前）退出了证书安装向导，则可以重新启动证书安装向导，并从退出的位置继续安装证书。

▼ 安装服务器证书

1. **如果您在生成服务器证书过程中退出了证书安装向导，请选择 “Console” -> “Certificate Setup Wizard”，然后在第一个屏幕上单击 “Next”，以重新启动该向导。**
2. **选择与您要在其中安装证书的 Sun Crypto Accelerator 4000 令牌相匹配的令牌。**
   此令牌必须与您在其中生成申请的令牌相同。
3. **当询问是否准备安装服务器证书时，回答 “Yes”，然后单击 “Next”。**
4. **单击 “Next”。**

5. **选择 “This Server”，然后输入密钥库密码 (*username:password*)（如果 “向导”未提供），然后单击 “Next”（参见**图 5-19）。

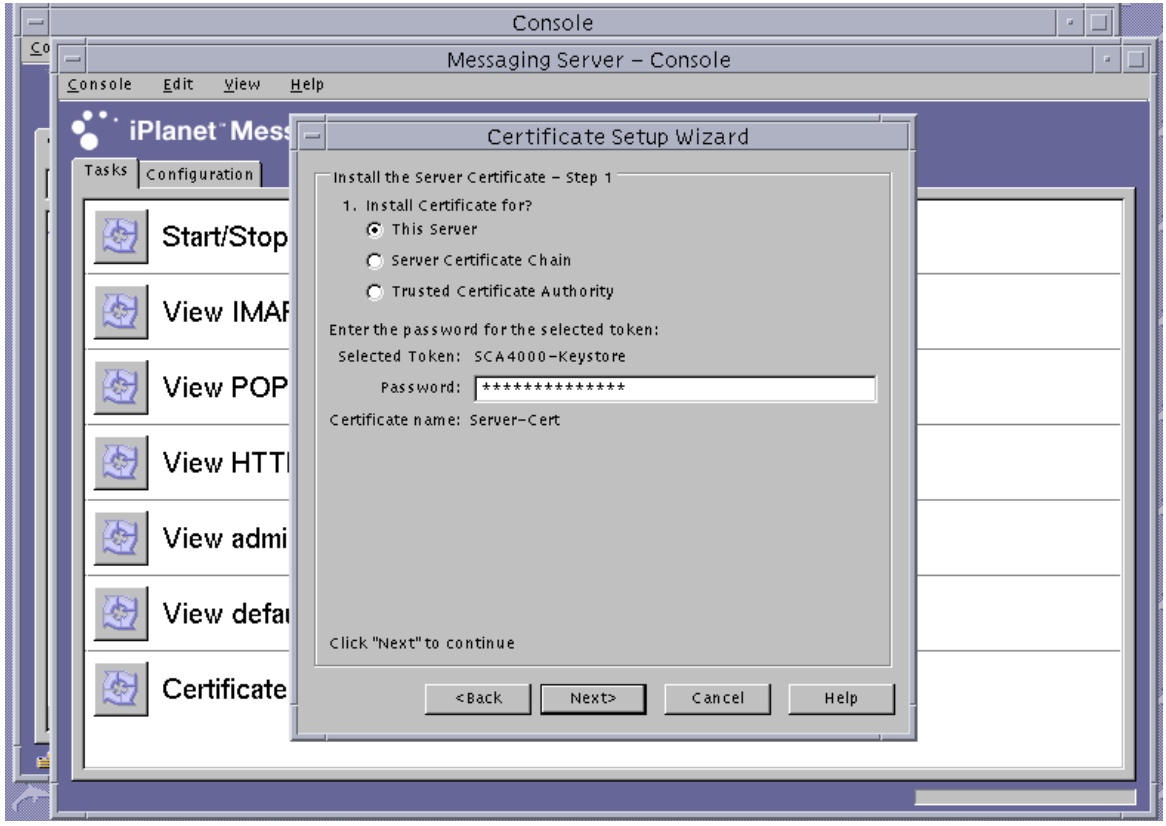

图 5-19 Sun ONE Messaging Server 的证书安装向导密码对话框

注 – 默认的证书名称为 `Server-Cert`。

---

6. **将 base 64 编码的证书复制到剪贴板上，并粘贴到题为 “The certificate is located in the following text field” 的文本框中，然后单击 “Next”（参见**图 5-20）。

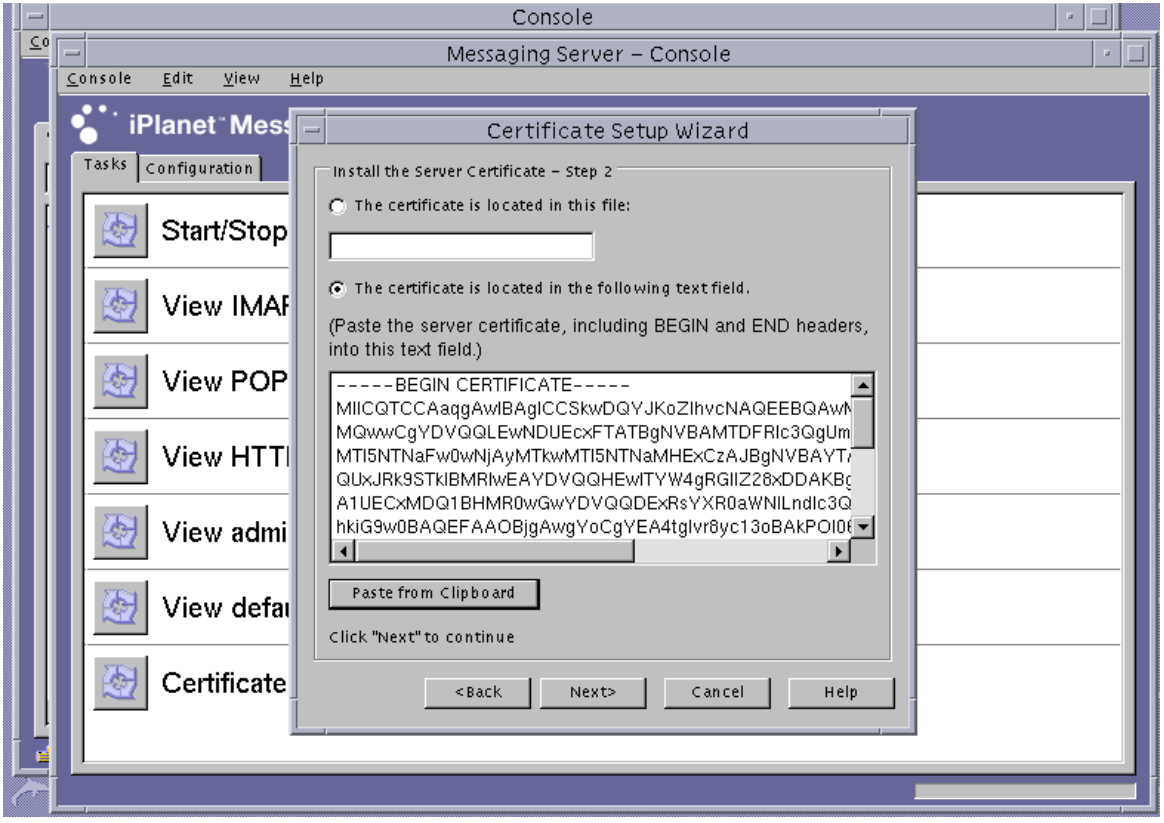

图 5-20 Sun ONE Messaging Server 的证书安装向导证书输入对话框

a. **单击 “Add”，添加证书。**

b. **单击 “Done”。**

7. **添加主要 CA 证书（仅当证书不是来自消息服务器所信任的主要认证机构时才有必要执行此步骤）。**

   此步骤需用证书安装向导。

   a. **在消息服务器控制台中，选择 “Console” → “Certificate Setup Wizard”。**

   b. **单击 “Next”。**

   c. **选择 “internal (software)” 作为令牌，对 “Is the certificate already requested and ready to install?” 回答 “Yes”，然后单击 “Next”。**

   d. **单击 “Next”。**

e. 选择 “Trusted Certificate Authority”，然后单击 “Next”。

f. 将 base 64 编码的 CA 证书复制到剪贴板上，并粘贴到题为 “The certificate is located in the following text field” 的文本框中，然后单击 “Next”。

g. 单击 “Add”，添加证书 （图 5-21）。

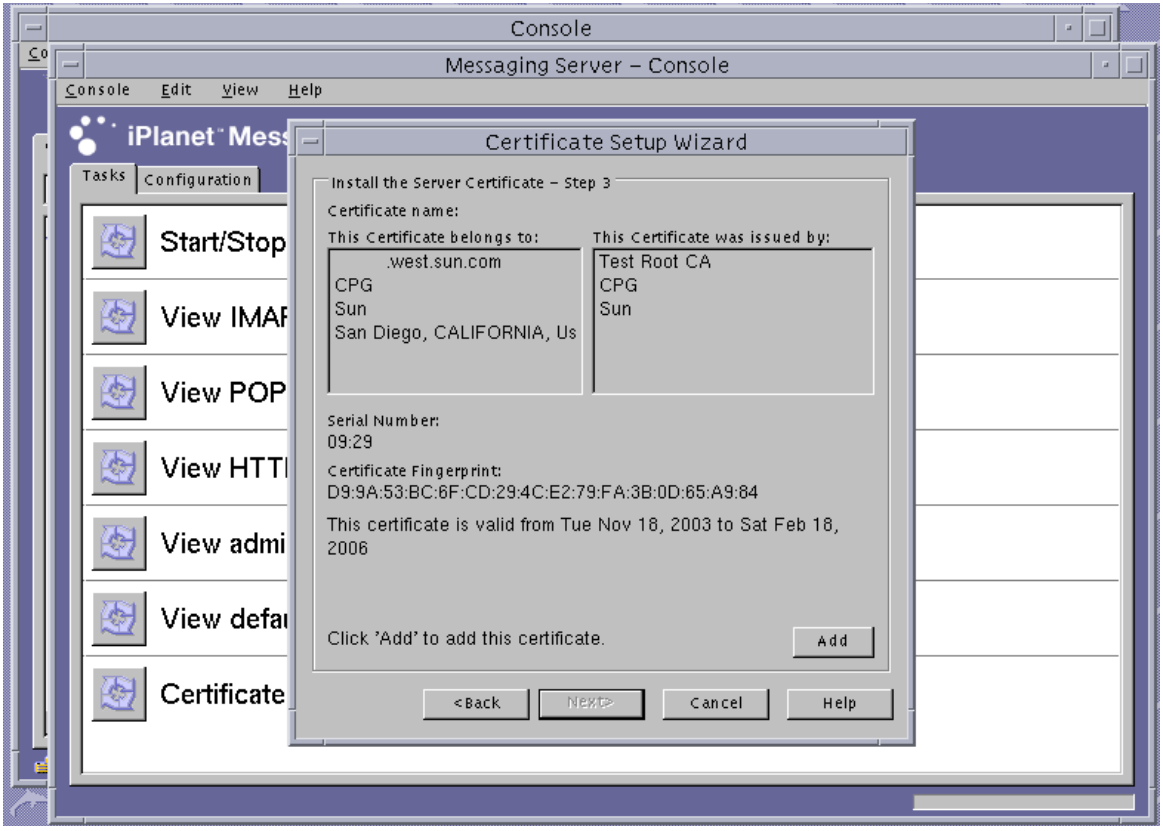

图 5-21 Sun ONE Messaging Server 的证书安装向导密码对话框

h. 单击 “Done”。

▼ 启用消息服务器以使用 SSL

1. 使用 `su` 命令，成为您要为其运行消息服务器的用户。

如果您忘记此用户名，可以在 *server-root*`/msg-`*instname*`/config/msg.conf` 文件中搜索 `local.serveruid` 属性，以找到此用户名。

```
# cd server-root/msg-instname
# su username
```

2. 使用 `configutil` 工具设置消息服务器的 SSL 参数。

表 5-11 介绍了用于 `configutil` 工具的变量定义。

表 5-11 `configutil` 变量说明

变量	定义
keystorename	在步骤 1 中使用的密钥库的名称。
certname	所用证书的容易记忆的名称。默认名称为 `Server-Cert`。
portnumber	在 SSL 上运行 POP3 的端口号；通常为 995。

```
# ./configutil -o nsserversecurity -v on
# ./configutil -o encryption.rsa.nssslactivation -v on
# ./configutil -o encryption.rsa.nsssltoken -v keystorename
# ./configutil -o encryption.rsa.nssslpersonalityssl -v certname
# ./configutil -l -o service.pop.enablesslport -v yes
# ./configutil -l -o service.pop.sslport -v portnumber
```

3. 在消息服务器控制台中，单击用于管理 Sun ONE Messaging Server 例程的控制台窗口中的 “Configuration” 选项卡。在 “Messaging Server” -> “Services” -> “IMAP” 下面，单击 “System” 选项卡。

4. 在上一个窗口中，为 “Use separate port for IMAP over SSL” 设置端口号。默认端口为 993。

5. **为消息服务器例程配置** `sslpassword.conf` **文件。**

```
# cd server-root/msg-instname/config
# vi sslpassword.conf
```

使用 *tokenname:username:password* 替换 `Internal (Software) token:netscape!` 行。其中 *tokenname* 是密钥库名称。此令牌名是您在步骤 1 中选择的、用于在其中生成密钥的令牌名称。 *username:password* 用于验证该令牌。有关 *username:password* 的详细信息，请参见表 5-1。

6. **更改** `sslpassword.conf` **文件的所有权和访问权限。**

由于 `sslpassword.conf` 文件包含用于验证密钥资料的密码信息，因此，该文件必须由运行守护程序的用户拥有，且仅允许此类用户读取。

```
# cd server-root/msg-instname/config
# chown msg-user sslpassword.conf
# chmod 0400 sslpassword.conf
```

7. **从命令行重新启动服务器。**

```
# cd server-root
# msg-instname/start-msg
```

安装和配置 Sun ONE Portal Server 6.2

本部分介绍如何安装和配置 Sun ONE Portal Server 6.2 以使用板。您必须按顺序执行这些步骤。有关使用 Sun ONE Portal Server 的详细信息，请参阅 Sun ONE Portal Server 文档。本部分包括以下过程：

本部分介绍如何安装和配置 Sun ONE Portal Server 6.2 以使用板。您必须按顺序执行这些步骤。有关使用 Sun ONE Portal Server 的详细信息，请参阅 Sun ONE Portal Server 文档。

Sun ONE Portal Server 6.2 包含 Sun ONE Web Server 6.0。在安装和配置门户服务器之前，必须安装和配置 Sun ONE Web Server 软件（参阅第 113 页“安装和配置 Sun ONE Web Server 6.0”）。

注 – 在安装并配置 Sun ONE Web Server 以用于门户服务器时，请使用以下安装路径：`/opt/SUNWam/servers`。

安装 Sun ONE Portal Server 6.2

本节介绍如何从命令行中安装 Sun ONE Portal Server 6.1。

▼ 安装 Sun ONE Portal Server 6.2

1. **下载 Sun ONE Portal Server 6.1 软件。**
   以下 URL 提供了该门户服务器软件：`http://www.sun.com/`
2. **切换至安装目录并解压门户服务器软件。**
3. **使用 `setup` 脚本安装门户服务器软件。**
   a. **提示时输入安装路径。**
   b. **提示时键入您希望安装的组件。**
   c. **执行 `./setup` 命令以安装组件。**

注 – 在安装过程中会自动创建信任数据库。

配置 Sun ONE Portal Server 6.2

本节介绍以下过程：配置门户服务器安全远程访问 (SRA) 网关；向门户服务器注册板；生成并安装服务器证书；以及启用门户服务器以使用 SSL。

开始之前，请确保已安装 SRA 和网关服务器证书（自签或由任何 CA 签发）。在配置过程中， Sun ONE Portal Server 管理服务器必须开启并运行。

▼ 向门户服务器注册板

1. **使用** vcaadm **实用程序为板创建新用户帐户（参阅第 53 页“使用 vcaadm 实用程序”）。**

```
vcaadm{vca0@localhost, sec-officer}> create user
New user name: username
Enter new user password:
Confirm password:
User crypta created successfully.
```

2. **加载 Sun Crypto Accelerator 4000 模块。**

LD_LIBRARY_PATH 变量必须指向以下位置：

```
/usr/lib/mps/secv2/
```

a. 加载模块。

```
# /usr/bin/mps/modutil -dbdir /etc/opt/SUNWps/cert/default -add "Sun Crypto
Accelerator 4000" -libfile /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

b. 验证是否已加载此模块。

```
# /usr/bin/mps/modutil -list -dbdir /etc/opt/SUNWps/cert/default -nocertdb
```

生成并安装服务器证书

在以下过程中， LD_LIBRARY_PATH 环境变量必须指向以下位置：

```
/usr/lib/mps/secv1/
```

表 5-12 介绍了本节中的 certutil 命令所用的变量。

表 5-12 certutil 变量说明

变量	说明
token-name	PKCS#11 令牌的名称；即您在初始化板时选择的密钥库名称。
subject-name	数字证书上声明的名称，通常格式如下： CN=*Fully-Qualified-Domain-Name*, OU=*Organization-Unit*, O=*Organization*. 名称会因组织而异。
output-file	证书申请的位置。
certfile	ASCII 编码证书的位置。
instname	门户服务器例程名称。
nickname	用户选择的容易记忆的服务器证书名称。

▼ 生成服务器证书

1. **切换至以下目录。**

```
# cd /etc/opt/SUNWps/cert/default
```

2. **申请证书。**

```
# /usr/bin/mps/bin/certutil -R -d . -h token-name -s "subject-name" -a -o output-file
[-g key-size]
```

3. **将 *output-file* 中的证书申请提交给您选择的认证机构。**

   将 base64 编码的证书放入名为 *certfile* 的文本文件中。

▼ 安装服务器证书

1. 安装服务器证书。

```
# /usr/bin/mps/certutil -A -d . -h token-name -t "Pu,Pu,Pu" -a -i certfile -n nickname
```

查看和安装主要 CA 证书

Sun ONE Portal Server 包含了一些广为人知且倍受信任的 Root Certificate Authority（主要认证机构）证书。如果您的服务器证书由这些著名的主要认证机构签发，请跳过此过程。

▼ 查看门户服务器已识别的主要 CA 证书

- **键入以下命令：**

```
# /usr/bin/mps/certutil -L -d /etc/opt/SUNWps/cert/default
```

▼ 安装主要 CA 证书

仅当您从专属 PKI（proprietary PKI）获取证书时才可执行以下过程。也就是说，如果您使用 VeriSign、 Thawte 或 GTE，则不要执行此过程。如果证书由主要供应商签发，并且它们的间接 CA 未列在 Sun ONE 默认的信任 CA 列表中，则使用此过程。

1. 切换至 certificate database 目录。

```
# cd /etc/opt/SUNWps/cert/default
```

2. 安装主要 CA 证书。

注 – 如果您安装多个 CA 证书，请使用不同的 `-n` 值。如果使用相同的 `-n` 值，则证书会相互覆盖。使用 CA 证书主题名的 CommonName 组件替换 `CA-Cert`（在 SubjectName 中查找 CN=）。

```
# /usr/bin/mps/certutil -A -d . -n "CA-Cert" -t "CT,CT,CT" -a -i path-to-ca-cert
```

▼ 启用门户服务器以使用 SSL

1. **创建** `/etc/opt/SUNWps/cert/default/.nickname` **文件**。

```
# vi /etc/opt/SUNWps/cert/default/.nickname
```

此文件必须仅包含以下行 （无空格）：

```
keystore-name:server-cert
```

2. **选择加速密码**。

注 – 要在 Sun Crypto Accelerator 4000 硬件中加速 DES 和 3DES 算法，则 `/etc/opt/SUNWconn/cryptov2/sslreg` 文件必须存在。有关说明，请参阅 第 99 页 “启用和禁用批量加密”。

板会加速 RSA 功能，但仅支持对 DES 和 3DES 密码的加速。要启用其中一种密码，请执行以下操作：

```
Gateway >> Security >> Enable SSL Cipher Selection: >> SSL3
Ciphers: >>
SSL3_RSA_WITH_3DES_EDE_CBC_SHA or
SSL3_RSA_WITH_DES_CBC_SHA
```

3. **修改** `/etc/opt/SUNWps/platform.conf.`*gateway-profile-name* **以启用板**。

```
gateway.enable.accelerator=true
```

4. **从终端窗口中重新启动网关**。

```
# InstallDir/SUNWps/bin/gateway -n gateway-profile-name start
```

网关会提示您输入密钥库密码。输入 *sra-keystore*:*username*:*password* 的密码或 pin。

第 6 章

安装和配置 Apache Web Server 软件

本章介绍如何安装和配置 Apache Web Server 软件以使用板，包括以下几节：

- 第 164 页 “配置 Apache Web Server 1.3x”
- 第 170 页 “构建和配置 Apache Web Server 2.x”
- 第 174 页 “配置 Apache Web Server，使其在重新引导期间启动但不进行用户交互操作”
- 第 175 页 “在安装 Sun Crypto Accelerator 4000 软件之后配置与 Apache 一起使用的 Sun Crypto Accelerator 1000”

当配置 Apache Web Server 以使用板，需要满足以下软件要求：

- Apache Web Server 1.3.26 或更高版本 — 1.3.26 版本随 Sun Crypto Accelerator 4000 软件提供
- 用于 Solaris 8 的修补程序 109234-09，可从 `http://sunsolve.sun.com` 获取
- 用于 Solaris 9 的修补程序 113146-02，可从 `http://sunsolve.sun.com` 获取
- Sun Crypto Accelerator 4000 软件附带的 `SUNWkcl2a` 软件包

添加 `SUNWkcl2a` 软件包后，系统会使用 Apache Web Server 和 mod_ssl 1.3.26 进行配置。

注 – Apache Web Server 不使用第 96 页 “概念和术语”（第 5 章）中介绍的密钥库和用户帐户功能。

注意 – 配置 Apache Web Server 时，不要让它同时与 Sun Crypto Accelerator 1000 板和 Sun Crypto Accelerator 4000 板配合使用。否则， Apache 将无法正常工作。

注 – 默认情况下，系统已为 Apache 软件启用了批量加密功能，且不能禁用。

配置 Apache Web Server 1.3x

本节介绍如何使用 apsslcfg 脚本配置 Web 服务器以使用板。此外，本节还介绍了如何创建和安装服务器证书。

▼ 配置 Apache Web Server

1. **创建** httpd **配置文件 （如果尚未创建）**。

   对于 Solaris 系统， httpd.conf-example 文件通常位于 /etc/apache 目录下。您可以将此文件用作模板并进行如下复制：

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

2. **用您的服务器名替换** httpd.conf **文件中的** ServerName。

3. **启动** apsslcfg。

```
# /opt/SUNWconn/cryptov2/bin/apsslcfg
```

4. **选择** 1，**配置 Apache Web Server 以使用 SSL**。

注 – 本过程假定您在提示时选择选项 1。如要选择选项 2，请参阅第 89 页 “使用 apsslcfg 脚本”。

```
Sun Crypto Accelerator Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Apache.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Apache for SSL
2. Work with Apache keys

Your selection (0 to quit): 1
```

5. **键入 Apache 二进制文件的路径。**

   在 Solaris 系统上，此路径通常为 `/usr/apache`。

```
Please enter the directory where the Apache
binaries and libraries exist [/usr/apache]: /usr/apache
```

6. **键入 Apache 配置文件的路径。**

   在 Solaris 系统上，此路径通常为 `/etc/apache`。

```
Please enter the directory where the Apache configuration files exist
[/etc/apache]: /etc/apache
```

7. **为系统创建远程安全访问 (RSA) 密钥对。**

   如果现在不创建密钥对，则以后必须使用 `apsslcfg` 生成密钥对。

```
Do you wish to create a new RSA keypair and certificate request? [Y/N]: Y
```

   如果您对此问题回答 “否”，则跳至第 167 页 “生成服务器证书”。

8. **提供用于存储密钥的目录。**

   如果提供的目录不存在，则系统会创建该目录。

```
Where would you like the keys stored? [/etc/apache/keys]: /etc/apache/keys
```

9. **为密码资料选择一个基本名称。**

   此名称附带不同的后缀以区别密钥文件、证书申请文件和证书文件。

```
Please choose a base name for the key and request file: base-name
```

10. 提供长度介于 512 和 2048 位之间的密钥。

对于大多数 Web 服务器应用程序而言， 1024 位已经足够安全。不过，如果您愿意，也可选择更安全的密钥。

```
What size would you like the RSA key to be [1024]? 1024
Using configuration from /opt/SUNWconn/cryptov2/ssl/openssl.cnf
Generating a 1024 bit RSA private key
........++++++
.....................................................++++++
writing new private key to /etc/apache/keys/base-name
```

11. 创建您的 PEM 密码。

此密码用以保护密钥资料。务必选择安全且易记的密码。如果忘记密码，将无法访问您的密钥。

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

注意 – 必须记住输入的密码。没有密码，就无法访问您的密钥。丢失的密码无法找回。

▼ 生成服务器证书

1. **使用您在第 164 页 “配置 Apache Web Server” 步骤 7 中创建的密钥来创建证书申请。**

   a. **键入密码以访问密钥。然后在以下申请人信息字段中键入正确的信息。**

   表 6-1 对申请人信息字段进行了说明。

```
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) []: Company
Organizational Unit Name (eg, section) []: Department
SSL Server Name (eg, www.company.com) []:www.company.com
Email Address []:admin@company.com
```

表 6-1 申请人信息字段

字段	说明
Country Name	由两个字母组成的国家/地区 ISO 代码 （例如，中国为 CN）
State or Province Name	（可选）州/省的全名，或输入圆点 (.)
Locality	城市、郡县、公国或国家/地区
Organization Name	公司名称
Organizational Unit Name	公司部门
SSL Server Name	在来访者的浏览器中键入的 Web 站点域
Email Address	申请人的联系信息

2. **按照说明修改** `/etc/apache/httpd.conf` **文件**。

   此时，会出现关于密钥和证书文件的信息以及如何修改 `/etc/apache/httpd.conf` 文件的说明。

```
The keyfile is stored in /etc/apache/keys/base-name-key.pem.
The certificate request is in /etc/apache/keys/base-name-certreq.pem.

You will need to edit /etc/apache/httpd.conf for the following items:

You must specify the ports that Apache will listen to for
SSL connections, as well as for non-SSL connections.  One
way to accomplish this is to add the following lines in
the Listen section:

Listen 80
Listen 443

In the LoadModule section, add the following:

LoadModule ssl_module /usr/apache/libexec/mod_ssl.so.version-number

In the AddModule section, add the following:

AddModule mod_ssl.c
```

注 – 屏幕上将显示您的配置对应的 *version-number*。

3. **如果选择不设置** VirtualHost**，则必须在** httpd.conf **文件中将** SSLEngine、SSLCertificateFile **和** SSLCertificateKeyFile **指令刚好置于** SSLPassPhraseDialog **指令前面**。

```
You may need a virtual host directive similar to
what is shown below:

<VirtualHost _default_:443>
        SSLEngine on
        SSLCertificateFile /etc/apache/keys/base-name-cert.pem
        SSLCertificateKeyFile /etc/apache/keys/base-name-key.pem
</VirtualHost>

You must add the following line after all of your VirtualHost
definitions:

SSLPassPhraseDialog exec:/opt/SUNWconn/cryptov2/bin/apgetpass

Other SSL-related directives and their explanations
can be found in the Sun Crypto Accelerator documentation.

Other Apache-related directives may need to be configured
in order to start your Apache Web Server. Please refer
to your Apache documentation.

<Press ENTER to continue>
```

如果对第 171 页 “配置 Apache Web Server 2.x” 步骤 7 中的问题回答 “否”，则系统还会向您提供如何生成密码资料的其它信息。

```
Since you did not create keys, you will need to
make sure that you have a key file and a certificate
file in place before enabling SSL for Apache.

You can create a new key file and certificate request
by selecting the "Generate a keypair and request a
certificate for Apache" option after choosing
"Work with Sun ONE and Apache keys" from the
apsslcfg main menu.
```

4. **在结束** apsslcfg **时键入** 0 **退出**。

▼ 安装服务器证书

1. **从** `/etc/apache/keys/`*base-name*`-certreq.pem` **文件（其中** *base-name* **已在第 164 页“配置 Apache Web Server”步骤 9 中设置）中复制带标题的证书请求并将其发送给认证机构。**

2. **生成证书后，请创建证书文件** `/etc/apache/keys/`*base_name*`-cert.pem` **并将您的证书粘贴到该文件中。**

3. **启动 Apache Web Server。**

   以下路径假定您的 Apache 二进制文件目录为 `/usr/apache/bin`。如果它不是您的二进制文件目录，请键入正确的路径。

   ```
   # /usr/apache/bin/apachectl sslstart
   ```

4. **提示时，请输入您的 PEM 密码。**

5. **在浏览器中输入以下 URL，检查已启用 SSL 的新 Web 服务器：**
   `https://`*server-name*`:`*server-port*`/`

   注意：默认的 *server_port* 为 443。

注 – 有关如何自签用于测试的证书，请参阅 mod_SSL 和 OpenSSL 文档。

构建和配置 Apache Web Server 2.x

Sun Crypto Accelerator 4000 软件不包含 Apache Web Server 2.x 的 mod_ssl 程序库。本节介绍您在构建 Web 服务器时所需的选项，并介绍如何配置 Apache Web Server 2.x 以使用板。

构建 Apache Web Server 2.x

要开始此过程，您的 OpenSSL 工具必须已安装所有必要的修补程序。本节仅介绍板的特定选项，并不包含构建完整的 Apache 2.x 套件所需的所有说明。有关完整说明，请访问 `http://www.apache.org` 网站上的文档。

▼ 构建 Apache 2.x

1. **预设** `SH_LIBS` **环境变量以符合** `configure` **脚本。**

```
sh:
# SH_LIBS="-lssl -lcrypto"
# export SH_LIBS
csh/tcsh:
# setenv SH_LIBS "-lssl -lcrypto"
```

2. **切换至安装目录并执行** `configure` **脚本。**

   此脚本有许多命令行选项。下面是在配置 Web 服务器以使用板时所需的选项：

```
# ./configure --enable-ssl --enable-mods-shared=ssl
--with-ssl=/opt/SUNWconn/cryptov2
```

3. **脚本运行完毕后，请执行以下操作之一：**

   a. **如果是首次构建并安装 Apache 2.x，请键入以下命令。**

```
# make
# make install
```

   b. **如果希望为现有的 Apache Web Server 2.x 构建 mod_ssl 共享程序库，请键入以下命令：**

```
# make shared-build
# cp modules/ssl/.libs/mod_ssl.so Apache-directory/modules
```

配置 Apache Web Server 2.x

本部分介绍如何配置 Web 服务器以使用板，过程包括生成并安装服务器证书以及启用 Web 服务器以使用 SSL。

▼ 生成服务器证书

1. 生成密钥和证书申请。

```
# /opt/SUNWconn/cryptov2/bin/openssl req \
-new -newkey rsa:keysize -keyout key-output-file \
-out cert-request-output-file \
-config /opt/SUNWconn/cryptov2/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....................................................................
..........++++++
.......++++++
writing new private key to '/tmp/key1.pem'
```

2. 键入密码以保护密钥文件。

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

3. 键入 “Distinguished Name”（识别名）的值 （参见表 6-2）。

```
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]:California
Locality Name (eg, city) []:San Diego
Organization Name (eg, company) []: Company
Organizational Unit Name (eg, section) []: Company Division
SSL Server Name (eg, www.company.com) []:www.company.com
Email Address []: admin@domain.com
```

表 6-2 识别名字段

字段	说明
Country Name	由两个字母组成的国家/地区 ISO 代码 （例如，中国为 CN）
State or Province Name	（可选）州/省的全名，或输入圆点 (.)
Locality Name	（可选）城市、郡县、公国或国家/地区
Organization Name	公司名称
Organizational Unit Name	（可选）公司部门
SSL Server Name	在来访者的浏览器中键入的 Web 站点域
Email Address	申请人的联系信息

▼ 安装服务器证书

- **将带标题的证书请求复制到您在第 172 页 “生成服务器证书”步骤 1 中创建密钥文件的目录。**

▼ 启用 SSL

1. **在 Apache Web Server 2.x 安装目录的 `conf` 子目录下编辑 `ssl.conf` 文件。**
   `ssl.conf` 文件中有数个指令；必须配置下列指令才能使 Web 服务器使用板。

```
Listen port-number
ServerName fully-qualified-domain-name
SSLEngine on
SSLCertificateFile path-to-certificate-file
SSLCertificateKeyFile path-to-key-file
```

2. **启动 Apache Web Server。**
   这里假定您的 Apache 二进制文件目录为 `/usr/apache/bin`。如果它不是您的二进制文件目录，请键入正确的目录。

```
# /usr/apache/bin/apachectl sslstart
```

3. **提示时，请输入您的 PEM 密码。**

4. **在浏览器中输入下面的 URL，检查已启用 SSL 的新 Web 服务器：**

   `https://`*server-name*`:`*server-port*`/`

   默认的 *server_port* 为 443。

注 – 有关如何自签用于测试的证书，请参阅 mod_SSL 和 OpenSSL 文档。

配置 Apache Web Server，使其在重新引导期间启动但不进行用户交互操作

使用加密密钥，您可以使 Apache Web Server 在重新引导期间自动启动。

▼ 创建加密密钥以使 Apache Web Server 在重新引导期间自动启动

1. **验证 `httpd.conf` 文件中是否存在以下条目：**

```
SSLPassPhraseDialog exec:/opt/SUNWconn/cryptov2/bin/apgetpass
```

   此指令将从 `/etc/apache` 目录下受保护的密码文件中检索密码。

2. **使用以下文件命名规则，在 `/etc/apache` 目录下创建仅包含密码的密码文件：**

```
server-name:port.KEYTYPE.pass
```

   - *server-name* – 您在 `httpd.conf` 文件的 ServerName 指令中指定的值
   - *port* – SSL 服务器所运行的端口 （例如， 443）
   - *KEYTYPE* – `RSA` 或 `DSA`

   示例：对于使用 `RSA` 密钥在端口 443 上运行 SSL 的服务器 （名为 `webserv101`），可以在 `/etc/apache` 目录下创建以下文件：

```
webserv101:443.RSA.pass
```

更改密码文件的访问权限和所有权，如下所示：

```
# chmod 400 server-name:port.KEYTYPE.pass
# chown root server-name:port.KEYTYPE.pass
```

有关详细说明，请参阅 mod_SSL 和 OpenSSL 文档。

在安装 Sun Crypto Accelerator 4000 软件之后配置与 Apache 一起使用的 Sun Crypto Accelerator 1000

安装 SUNWkcl2a 软件包之后，系统会使用 Apache Web Server mod_ssl 1.3.26 进行配置。

如果希望配置 Sun Crypto Accelerator 1000 板以便与 Apache 配合使用，必须安装以下修补程序。

在装有 SUNWkcl2a 软件包的 Solaris 8 系统上，要配置 Sun Crypto Accelerator 1000 以便与 Apache 1.3.26 配合使用，必须安装以下修补程序：

- 对于 Apache 1.3.26 – 修补程序 ID 109234-09 或更高版本
- 对于 Sun Crypto Accelerator 1000 1.0 版软件 – 修补程序 ID 112869-02
- 对于 Sun Crypto Accelerator 1000 1.1 版软件 – 修补程序 ID 113355-01

在装有 SUNWkcl2a 软件包的 Solaris 9 系统上，要配置 Sun Crypto Accelerator 1000 以便与 Apache 1.3.26 配合使用，必须安装以下修补程序：

- 对于 Apache 1.3.26 – 修补程序 ID 113146-01 或更高版本
- 对于 Sun Crypto Accelerator 1000 1.1 版软件 – 修补程序 ID 113355-01

第 7 章

故障诊断和排除

本章介绍 Sun Crypto Accelerator 4000 软件的诊断测试程序和故障排除过程，包括以下几节：

SunVTS 诊断软件

核心 SunVTS 程序包提供了用于执行一系列测试的测试控件和用户界面。其中一些测试程序随 SUNWvts 和 SUNWvtsx 软件包一起提供，组成 Solaris 8/9 Software Supplement CD 上的工具套件。其它使用核心 SunVTS 程序包的零散测试程序则随所测试设备的驱动程序软件一起提供。

Sun Crypto Accelerator 4000 板可通过三个 SunVTS 测试程序进行测试。其中两个测试程序， nettest 和 netlbtest，与 SunVTS 5.1 Patch Set (PS) 2 版本以后的核心 SunVTS 软件捆绑在一起。这些测试程序用于对板的以太网电路进行测试。

第三个 SunVTS 测试程序 vcatest 位于 Sun Crypto Accelerator 4000 CD 上的 SUNWvcav 软件包中，它与核心 SunVTS 程序包一起用于诊断板的加密电路。

为 vca 驱动程序安装 SunVTS netlbtest 和 nettest 支持

表 7-1 说明了如何更新已安装的 SunVTS 软件以便为 vca 驱动程序提供 SunVTS netlbtest 和 nettest 支持。

表 7-1 vca 驱动程序必需的 SunVTS netlbtest 和 nettest 软件

基本 Solaris 软件	基本 SunVTS 软件	必需的替换软件包	必需的更新修补程序
Solaris 8 7/01	SunVTS4.4		111854-04
Solaris 8 10/01	SunVTS4.5		112250-04
Solaris 8 2/02	SunVTS4.6	SunVTS5.1ps2	
Solaris 9 5/02	SunVTS5.0	SunVTS5.1ps2	
Solaris 9 9/02	SunVTS5.1		113614-11
Solaris 8 HW 12/02	SunVTS5.1ps1		113614-11
Solaris 9 12/02	SunVTS5.1ps1		113614-11
Solaris 8 HW 5/03	SunVTS5.1ps2		
Solaris 9 4/03	SunVTS5.1ps2		

SunVTS 软件位于每个 Solaris 版本附带的 Solaris Software Supplement CD 上。表 7-1 “基本 SunVTS 软件”栏中列出的 SunVTS 软件版本位于同一行内 Solaris 版本附带的 Solaris Software Supplement CD 上。

表 7-1 中以 “SunVTS”开头的条目表示一套 SunVTS 软件包的版本。每套 SunVTS 软件包中必须安装 SUNWvts 和 SUNWvtsx 软件包。

表 7-1 “必需的替换软件包”栏中列出的 SunVTS 软件包必须替换以前安装的 SunVTS 软件包。添加 SunVTS 替换软件包之前，应删除以前安装的 SunVTS 软件包。删除以前安装的 SunVTS 软件包时，所用的方法必须与以前安装它们时所用的方法相同。例如，如果以前安装软件包时所用的命令是 pkgadd，则应使用 pkgrm 命令删除软件包。

如果表 7-1 “必需的更新修补程序”栏中列有条目，则使用 patchadd 命令安装该修补程序以更新 “基本 SunVTS 软件”栏中列出的 SunVTS 软件包。添加必需的修补程序之前，不要删除以前安装的 SunVTS 软件包。

使用 patchadd 命令安装修补程序 113614-11 相当于用 SunVTS5.1ps2 软件包替换以前安装的 SunVTS 软件包。

以下网址提供了替换软件包：http://www.sun.com/oem/products/vts/

以下网址提供了更新修补程序：http://sunsolve.sun.com/

注 – 安装 SUNWvcav 软件包之前，必须先安装必需的 SunVTS 软件包和修补程序。SUNWvcav 软件包中包括 SunVTS 测试程序 vcatest。

使用 SunVTS 软件执行 vcatest、nettest 和 netlbtest

有关如何执行和监控这些诊断测试程序的说明，请参阅 SunVTS 测试程序参考手册、用户指南和快速参考卡。这些文档位于 http://docs.sun.com 网站上的 “Solaris on Sun Hardware Documentation Set”中。此外，您的系统 Solaris 版本附带的 Solaris Software Supplement CD 中也提供了这些文档。

注 – 只有在安装了必需的 SunVTS 软件包和 SunVTS 修补程序之后才能使用 SunVTS。

▼ 执行 vcatest

1. **以超级用户身份启动 SunVTS。**

```
# /opt/SUNWvts/bin/sunvts
```

有关启动 SunVTS 的详细说明，请参阅 SunVTS 用户指南。

以下说明假定您已使用 CDE 用户界面启动了 SunVTS。

2. **在 “SunVTS Diagnostic”主窗口中，将 “System Map”设为 “Logical”模式。**

注 – 系统也支持 “Physical”模式；不过，本过程假定使用 “Logical”模式。

---

3. **清除所有测试程序的复选框，将它们禁用。**
4. **选择 “Cryptography”的复选框，然后再选择 “Cryptography”的加号框，显示 Cryptography 组中的所有测试程序。**

5. **清除 Cryptography 组中除 `vcatest` 以外的复选框。**
   - 如果显示了 `vcatest`，则转至步骤 6。
   - 如果未显示 `vcatest`，则可以通过检测系统以找到它，方法是：选择“Commands”下拉菜单中的“Reprobe System”。

   有关确切步骤，请参阅 SunVTS 用户指南。检测过程完成并显示 `vcatest` 后，继续执行步骤 6。

6. **选择其中一个 `vcatest` 例程，然后单击右键并拖动鼠标以显示“Test Parameter Options”对话框。**

   第 180 页“`vcatest` 的测试参数选项”介绍了这些只属于 `vcatest` 的选项。

7. **选择所有必要的选项后，从“Within Instance”下拉菜单中单击“Apply”以更改所选的 `vcatest` 例程；或者从“Across All Instances”下拉菜单中选择“Apply”以更改选定的所有 `vcatest` 例程。**

   进行该操作后，对话框消失，并且返回“SunVTS Diagnostic”主窗口。

8. **选择其中一个 `vcatest` 例程，然后单击右键并拖动鼠标以显示“Test Execution Options”对话框。**

   显示“Test Execution Options”对话框的另一种方法是选择“Options”下拉主菜单，然后再选择“Test Executions”。这些选项是通用 SunVTS 控件，将会影响所有测试程序。有关详细信息，请参阅 SunVTS 用户指南。

9. **选择所有必要的选项后，单击“Apply”以清除对话框并返回“SunVTS Diagnostic”主窗口。**

10. **单击“Start”执行所选的测试程序。**

11. **单击 Stop 停止所有测试程序。**

`vcatest` 的测试参数选项

表 7-2 说明了 `vcatest` 子测试程序。

表 7-2 `vcatest` 子测试程序

测试程序名称	说明
`CDMF`	测试 CDMF 批量加密
`DES`	测试 DES 批量加密
`3DES`	测试 3DES 批量加密
`RSA`	测试 RSA 公钥和私钥
`DSA`	测试 DSA 签名验证

表 7-2 vcatest 子测试程序 *（续）*

测试程序名称	说明
MD5	测试 MD5 消息摘要/数字签名
SHA1	测试 SHA1 摘要密钥创建
RNG	测试随机号码生成

vcatest 命令行语法

要从命令行 （而非 CDE 界面）执行 vcatest，请在命令行字符串中指定所有参数。

在 32 位模式下，vcatest 的路径是 /opt/SUNWvts/bin/。在 64 位模式下，路径是 /opt/SUNWvts/bin/sparcv9/。

vcatest 的命令行界面能够支持所有 SunVTS 标准选项。测试程序专用的选项通过 -o 参数指定。

有关标准命令行参数的定义，请参阅 《SunVTS 测试程序参考手册》。vcatest 是一个功能模式的测试程序，因此必须包括 -f 参数。使用 -u 参数可以显示用法消息，或者使用 -v 参数显示 VERBOSE （详细）消息。方括号中包含的项目表示可选条目。

下面是一个在 32 位模式下将 vcatest 作为独立程序调用的示例。以下命令用于在 vca0 上执行所有子测试程序：

```
# /opt/SUNWvts/bin/vcatest -f -o dev=vca0,tl=all
```

下面是一个在 64 位模式下从 SunVTS 体系中调用 vcatest 的示例。以下命令用于在 vca2 上执行 RSA、 DSA 和 MD5 测试程序：

```
# /opt/SUNWvts/bin/sparcv9/vcatest -f -o dev=vca2,tl=RSA+DSA+MD5
```

从命令行中运行 vcatest 时，如果忽略某个选项，则会使用该选项的默认操作，如表 7-3 中所示。

表 7-3 vcatest 命令行语法

选项	说明
dev=vca*N*	指定要测试的设备的例程，如 vca0 或 vca2。如果不指定，则默认为 vca0。请注意 *N* 表示要测试的设备的例程号。
tl=*testlist*	指定要执行的子测试程序的列表。 tl 的子测试程序由 + （加号）隔开。支持的子测试程序为 CDMF、 DES、 3DES、 DSA、 RSA、 MD5、 SHA1 和 RNG，因此 tl=CDMF+DES+3DES+DSA+RSA+MD5+SHA1+RNG 将启用所有子测试。您也可以插入 tl=all，以便执行所有测试程序。如果未指定任何子测试程序，则默认为 all。

▼ 执行 netlbtest

1. **以超级用户身份启动 SunVTS。**

```
# /opt/SUNWvts/bin/sunvts
```

有关启动的详细说明，请参阅 SunVTS 用户指南。

以下说明假定您已使用 CDE 用户界面启动了 SunVTS。

2. **在 “SunVTS Diagnostic” 主窗口中，将 “System Map” 设为 “Logical” 模式。**

注 – 系统也支持 “Physical” 模式；不过，本过程假定使用 “Logical” 模式。

3. **清除所有测试程序的复选框，将它们禁用。**

4. **选择 “Network” 的复选框，然后再选择 “Network” 的加号框，显示 Network 组中的所有测试程序。**

5. **清除 Network 组中除 vca*N*(netlbtest) 以外的复选框。**

请注意 *N* 表示要测试的设备的例程号。

- 如果显示了 vca*N*(netlbtest)，则转至步骤 6。
- 如果未显示 vca*N*(netlbtest)，则可以通过检测系统以找到它，方法是：选择 “Commands” 下拉菜单中的 “Reprobe System”。

有关确切步骤，请参阅 SunVTS 用户指南。检测过程完成并显示 vca*N*(netlbtest) 后，继续执行步骤 6。

6. **选择 “Intervention Mode”按钮。选择其中一个** vca*N*(netlbtest) **例程，然后单击右键并拖动鼠标以显示 “Test Parameter Options”对话框。**

   SunVTS 测试程序参考手册中介绍了只属于 netlbtest 的选项。

7. **选择所有必要的选项后，从 “Within Instance”下拉菜单中选择 “Apply”以更改所选的** vca*N*(netlbtest) **例程；或者从 “Across All Instances”下拉菜单中选择 “Apply”以更改所有选定的** vca*N*(netlbtest) **例程。**

   进行该操作后，对话框消失，并且返回 “SunVTS Diagnostic”主窗口。

8. **选择其中一个** vca*N*(netlbtest) **例程，然后单击右键并拖动鼠标以显示 “Test Execution Options”对话框。**

   显示 “Test Execution Options”对话框的另一种方法是选择 “Options”下拉主菜单，然后再选择 “Test Executions”。这些选项是通用 SunVTS 控件，将会影响所有测试程序。有关详细信息，请参阅 SunVTS 用户指南。

9. **选择所有必要的选项后，选择 “Apply”以清除对话框并返回 “SunVTS Diagnostic”主窗口。**

10. **单击 “Start”执行所选的测试程序。**

11. **单击 Stop 停止所有测试程序。**

▼ 执行 nettest

1. **以超级用户身份启动 SunVTS。**

```
# /opt/SUNWvts/bin/sunvts
```

   有关启动的详细说明，请参阅 SunVTS 用户指南。

注 – 以下说明假定您已使用 CDE 用户界面启动了 SunVTS。

---

2. **在 “SunVTS Diagnostic”主窗口中，将 “System Map”设为 “Logical”模式。**

注 – 系统也支持 “Physical”模式；不过，本过程假定使用 “Logical”模式。

---

3. **清除所有测试程序的复选框，将它们禁用。**

4. **选择 “Network”的复选框，然后再选择 “Network”的加号框，显示 Network 组中的所有测试程序。**

5. **清除 Network 组中除 vca*N*(nettest) 以外的复选框。**

   请注意 *N* 表示要测试的设备的例程号。

   - 如果显示了 vca*N*(nettest)，则转至步骤 6。
   - 如果未显示 vca*N*(nettest)，则在安装 vca*N* 板的服务器上的另一个窗口中输入 ifconfig -a。此时会列出以下条目：

   ```
   vcaN up inet ip-address plumb
   ```

   如果未列出上述 ifconfig 条目，则 nettest 探测程序认为此设备不可测试。按照 ifconfig online 手册页说明，使界面联机。

   如果 ifconfig -a 列出了前面的条目，请返回 “SunVTS Diagnostic”主窗口，然后通过在 “Commands”下拉菜单中选择 “Reprobe System”来检测系统以查找 vca。

   有关确切步骤，请参阅 SunVTS 用户指南。检测过程完成并显示 vca0(nettest) 后，继续执行步骤 6。

6. **选择其中一个 vca*N*(nettest) 例程，然后单击右键并拖动鼠标以显示 “Test Parameter Options”对话框。**

   SunVTS 测试程序参考手册中介绍了只属于 nettest 的选项。

7. **选择所有必要的选项后，从 “Within Instance”下拉菜单中选择 “Apply”以更改所选的 vca*N*(nettest) 例程；或者从 “Across All Instances”下拉菜单中选择 “Apply”以更改所有选定的 vca*N*(nettest) 例程。**

   进行该操作后，对话框消失，并且返回 “SunVTS Diagnostic”主窗口。

8. **选择其中一个 vca*N*(nettest) 例程，然后单击右键并拖动鼠标以显示 “Test Execution Options”对话框。**

   显示 “Test Execution Options”对话框的另一种方法是选择 “Options”下拉主菜单，然后再选择 “Test Executions”。这些选项是通用 SunVTS 控件，将会影响所有测试程序。有关详细信息，请参阅 SunVTS 用户指南。

9. **选择所有必要的选项后，选择 “Apply”以清除对话框并返回 “SunVTS Diagnostic”主窗口。**

10. **单击 “Start”执行所选的测试程序。**

11. **单击 Stop 停止所有测试程序。**

注 – 不要同时执行 nettest 和 netlbtest。

使用 kstat 确定加密活动

Sun Crypto Accelerator 4000 板没有配备用于反映板上加密活动的指示灯或其它指示器。要确定加密作业请求是否已真正在板上执行，请使用 kstat(1M) 命令显示设备的用法：

```
# kstat vca:0
module: vca                     instance: 0
name:   vca0                    class:    misc
        3desbytes               3040
        3desjobs                5
        crtime                  65.342725895
        dsasign                 0
        dsaverify               0
        rngbytes                10592
        rngjobs                 187
        rngsha1bytes            16328
        rngsha1jobs             327
        rsaprivate              9
        rsapublic               0
        snaptime                106956.467004482
```

注 – 在上面的示例中， 0 是 vca 设备的例程号。此号码应反映您正在为其执行 kstat 命令的板的例程号。

显示的 kstat 信息指明了加密请求或 “作业”是否正发送给 Sun Crypto Accelerator 4000 板。*作业*值随时间变化，表明板正在加速那些发送给 Sun Crypto Accelerator 4000 板的加密作业请求。如果无加密作业请求发送给板，请根据 Web 服务器的特定配置来验证您的 Web 服务器配置。

不要试图解释 kstat(1M) 返回的内核/驱动程序统计值。这些值保存在驱动程序内，以便于进行现场支持服务。含义和实际名称可能会随时间而变化。

注 – 如果 nostats 属性已在 /kernel/drv/vca.conf 文件中定义，则不会捕获和显示统计数据。此属性可以用来防止进行通信量分析。

使用 OpenBoot PROM FCode 自测程序

以下测试程序有助于在系统无法引导时识别适配器的故障。

通过在 OpenBoot PROM `ok` 提示符下运行 `test` 或 `test-all` 命令，可以调用 FCode 自测诊断程序。如果在执行诊断程序时发生故障，则会显示相应的消息。有关 `test` 和 `test-all` 命令的详细信息，请参阅 《*OpenBoot Command Reference Manual*》。

FCode 自测程序按子组件运行大多数功能子组件，并确保：

- 在适配器板安装期间的连通性
- 验证系统引导过程所需的所有组件是否正常

▼ 执行以太网 FCode 自测诊断程序

要执行以太网诊断程序，您必须先在 OpenBoot PROM `ok` 提示符下输入重置命令，以使系统停止。如果不重置系统，诊断测试程序可能会导致系统挂起。

有关本节中 OpenBoot 命令的详细信息，请参阅 《*OpenBoot Command Reference Manual*》。

1. **关闭系统。**

   使用 《*Solaris Handbook for Sun Peripherals*》中所述的标准关机过程。

2. **在 OpenBoot PROM `ok` 提示符下，将 `auto-boot?` 配置变量设为 `false`。**

```
ok setenv auto-boot? false
```

3. **重置系统。**

```
ok reset-all
```

4. **键入** `show-nets` **以显示设备列表，并选择所需的选项：**

   您会看到类似于下面示例的设备列表，这些设备因适配器而异。

```
ok show-nets
a) /pci@8,600000/network@1
b) /pci@8,700000/network@5,1
q) NO SELECTION
Enter Selection, q to quit: a
/pci@8,600000/network@1 has been selected.
Type ^Y ( Control-Y ) to insert it in the command line.
e.g. ok nvalias mydev ^Y for creating devalias mydev for
/pci@8,600000/network@1
```

注 – 要使用 `test` 命令执行以下自测程序，必须将以太网端口连接至网络。

---

5. **使用** `test` **命令执行自测程序：**

   运行 `test` 命令时，将会执行以下测试程序：

   - `vca` 寄存器测试程序 （仅在 `diag-switch?` 设为 true 时发生）
   - 内部回送测试程序
   - 链路连接/断开测试程序

注 – 对于使用外部回送缆线的 1000 Mbps 连接，由于链路时钟无法调整，因此无法执行 Sun Crypto Accelerator 4000 UTP 适配器自测程序。对于此类测试，本地端口和远程端口必须调整为主控时钟与从属时钟。使用外部回送缆线时，本地端口和远程端口相同。因此，单个端口不能既是主控时钟又是从属时钟，因为这样会始终导致 PHY 链路连接失败。要使 Sun Crypto Accelerator 4000 UTP 适配器自测程序可以正确测试 1000 Mbps 连接，必须连接远程 1000BASE-T 端口。

键入以下命令：

```
ok test device-path
```

如果通过 `test` 测试，则会看到以下消息：

```
ok test /pci@8,600000/network@1
Testing /pci@8,600000/network@1
Register tests: passed
Internal loopback test: passed
/pci@8,600000/network@1: 100 Mbps half duplex link up
```

如果板未连接至网络，则会看到以下消息：

```
ok test /pci@8,600000/network@1
Testing /pci@8,600000/network@1
Register tests: passed
Internal loopback test: passed
/pci@8,600000/network@1: link down
```

6. **测试适配器之后，请键入以下命令，以将 OpenBoot PROM** `ok` **提示符界面恢复至标准操作模式：**

```
ok setenv diag-switch? false
```

7. **将** `auto-boot?` **配置参数设为** `true`。

```
ok setenv auto-boot? true
```

8. **重置并重新引导系统。**

排除 Sun Crypto Accelerator 4000 板的故障

本节介绍用于排除板故障的 OpenBoot PROM 级命令。有关以下小节所述命令的详细说明，请参阅 《*OpenBoot Command Reference Manual*》。

show-devs 命令

要确定 Sun Crypto Accelerator 4000 设备是否在系统中列出，请在 OpenBoot PROM ok 提示符下键入 show-devs 命令以显示设备列表。设备列表中的行将类似于下面的示例。这些行的内容可能会有所不同，具体取决于板：

```
ok show-devs
.
.
/chosen
/packages
/upa@8,480000/SUNW,ffb@0,0
/pci@8,600000/network@1
/pci@8,600000/SUNW,qlc@4
/pci@8,600000/SUNW,qlc@4/fp@0,0
.
.
```

在上面的示例中， /pci@8,600000/network@1 条目表示板的设备路径。系统中的每块板均应有各自的设备路径行。

.properties 命令

要确定是否正确列出了 Sun Crypto Accelerator 4000 的设备属性，请在 ok 提示符下，键入 .properties 命令以显示属性列表。

```
ok .properties
assigned-addresses        82000810 00000000 00102000 00000000 00002000
                           81000814 00000000 00000400 00000000 00000100
                           82000818 00000000 00200000 00000000 00200000
                           82000830 00000000 00400000 00000000 00100000
d-fru-len                 00 00 00 00
d-fru-off                 00 00 e8 00
d-fru-dev                 eeprom
s-fru-len                 00 00 08 00
s-fru-off                 00 00 e0 00
s-fru-dev                 eeprom
compatible                70 63 69 38 30 38 36 2c 62 35 35 35 2e 31 30 38
reg                       00000800 00000000 00000000 00000000 00000000
                           02000810 00000000 00000000 00000000 00002000
                           02000814 00000000 00000000 00000000 00000100
                           02000818 00000000 00000000 00000000 00200000
                           02000830 00000000 00000000 00000000 00100000
address-bits              00 00 00 30
max-frame-size            00 00 40 00
network-interface-type    ethernet
device-type               network
name                      network
local-mac-address         00 03 ba 0e 99 ca
version                   Sun PCI Crypto Accelerator 4000 1000Base-T
FCode 2.11.13 03/03/04
phy-type                  mif
board-model               501-6039
model                     SUNW,pci-vca
fcode-rom-offset          00000000
66mhz-capable
fast-back-to-back
devsel-speed              00000001
class-code                00100000
interrupts                00000001
max-latency               00000040
min-grant                 00000040
subsystem-vendor-id       0000108e
subsystem-id              00003de8
revision-id               00000002
device-id                 0000b555
vendor-id                 00008086
```

watch-net 命令

要监控网络连接情况，请在 ok 提示符下，键入 apply watch-net 命令和设备路径：

```
ok apply watch-net /pci@8,600000/network@1
/pci@8,600000/network@1: 1000 Mbps full duplex link up
Watch ethernet packets
'.' is a good packet and 'X' is a bad packet
Press any key to stop
.....X...X......X.....
```

系统将会监控网络通信状态。每次收到无错误的数据包时，便会显示一个 “.” 符号；每次收到可由网络硬件接口检测到的出错数据包时，便会显示一个 “X” 符号。

第 8 章

PKCS#11 界面

本章介绍板在 PKCS#11 界面中的执行信息，并假定 Sun Crypto Accelerator 4000 软件安装在默认位置。此外，本章还假定您熟悉 PKCS#11 界面。有关 PKCS#11 标准以及头文件 `pkcs11.h`、`pkcs11f.h` 和 `pkcs11t.h` 的原始副本信息，请访问以下网址：`http://www.rsasecurity.com/rsalabs/PKCS`。

本章包括以下几节：

常规问题

Sun Crypto Accelerator 4000 板和相关的软件提供 PKCS#11 界面。Sun Crypto Accelerator 4000 软件中提供了大多数应用程序所需的 PKCS#11 功能。

PKCS#11 设计用于单用户系统。Solaris 操作系统必须处理多个互不信任的并发用户，因此是多用户系统。为了适应这一情况，板添加了可识别和验证多个用户的功能，而无须扩展 PKCS#11。对于每个接受加密 PIN 的 PKCS#11 函数，必须为其指定以下格式的字符串：*username:password*（参见表 5-1）。通常，此 PIN 结构通过应用程序向上传播，尽管少数专为此板编写的应用程序可能会要求分别提供用户名和密钥。

PKCS#11 提供有限的管理工具，只有两个函数：`C_InitToken`（用于初始化令牌）和 `C_InitPin`（用于设置用户 PIN）。板不使用此工具，而使用 `vcaadm` 实用程序。

`vcaadm` 安全主管 (SO) 与 UNIX 超级用户并无关系。另外，板用户的 `userid`（由安全主管使用 `vcaadm` 创建）也与 UNIX 用户名或 ID 无关。

PKCS#11 使用独特的插槽和令牌概念。令牌类似于智能卡，插入*插槽*中。在 Sun Crypto Accelerator 4000 系统中，插槽和令牌没有区别。本指南通常使用术语“*令牌*”；但应用程序和其它文档可能使用术语“*插槽*”。

每块板最多支持一个*密钥库*。安全主管使用 `vcaadm` 指定每个密钥库的名称。每个密钥库由板表示为 PKCS#11 令牌，令牌标签是相关密钥库的名称，并用空格填充至 32 个字符。多块板可以支持单个密钥库，以便获得高可用性。

另外，有一个特殊的令牌，其标签为 `SUNW acceleration only`（仅限 SUNW 加速）。此令牌不能存储任何永久密钥，且应用程序不能登录到此令牌。提交到此令牌的请求在所有可用的板之间进行分配。

许多应用程序显示令牌列表 — 令牌通常由 PKCS#11 令牌标签标识。（令牌标签是由安全主管指定的相关密钥库的名称，以空格填充。）

管理板以使用 PKCS#11

Sun Crypto Accelerator 4000 系统通过 `vcaadm` 实用程序进行管理 （参阅第 4 章）。安全主管可以命名密钥库并创建用户帐户，为每个帐户指定一个初始密码。安全主管还可控制板是否在 FIPS 模式下操作 （参阅第 195 页 “PKCS#11 和 FIPS 模式”）。

板支持许多 PKCS#11 机制。它可以无条件地使用大多数机制。不过，管理员可对以下机制的提供方式进行一定的控制：

- `CKM_SSL3_SHA1_MAC`
- `CKM_SSL3_MD5_MAC`
- `CKM_SSL3_PRE_MASTER_KEY_GEN`
- `CKM_SSL3_MASTER_KEY_DERIVE`
- `CKM_SSL3_KEY_AND_MAC_DERIVE`
- `CKM_TLS_PRE_MASTER_KEY_GEN`
- `CKM_TLS_MASTER_KEY_DERIVE`
- `CKM_TLS_KEY_AND_MAC_DERIVE`

这些机制始终由 acceleration-only 令牌提供。仅当存在 `/etc/opt/SUNWconn/cryptov2/sslreg` 时，这些机制才由带有密钥库的令牌提供。要创建此文件，请作为超级用户键入以下命令：

```
# touch /etc/opt/SUNWconn/cryptov2/sslreg
```

重新启动应用程序以使此更改生效。

当这些机制可用时，网络安全服务 (NSS) 可以识别它们。当提供这些机制时， NSS 将通过较小的缓冲器对 `C_DigestUpdate` 进行多次调用，致使性能降低。因此，默认情况下不提供这些机制。

安装和管理使用加密服务的应用程序

PKCS#11 程序库的默认位置是：`/opt/SUNWconn/cryptov2/lib/libvpkcs11.so`

大多数应用程序的配置文件或数据库都包含 PKCS#11 程序库的位置。（这些配置文件或数据库有时可通过图形用户界面 (GUI) 进行访问）。使用编辑器或 GUI，输入上面的值作为默认位置。

当某个密钥具有 `CKA_SENSITIVE` 属性时，则涉及该密钥的操作会仅限于硬件。然而，硬件并非支持密钥的所有操作和所有类型。如果应用程序请求的操作无法在硬件中执行，而且密钥的 `CKA_SENSITIVE` 属性为 “True”，则该操作会失败。第 196 页 “硬件加速和敏感密钥”中详细介绍了哪些密钥、操作和机制组合可用的具体规则。如果您的应用程序因这些规则的限制而无法操作，则可对其进行配置，使其密钥标记为 “非敏感”。

是否提供 `SSL...` 和 `TLS...` 机制由管理员控制。如果应用程序需要这些机制，或者您想体验启用这些机制之后的性能效果，请参阅第 194 页 “管理板以使用 PKCS#11”。

如果板处于 FIPS 模式，则它仅提供 FIPS 认可的机制 （参阅第 195 页 “PKCS#11 和 FIPS 模式”）。

PKCS#11 和 FIPS 模式

当安全主管使用 `vcaadm` 将 Sun Crypto Accelerator 4000 板置入 FIPS 模式时，该板符合联邦信息处理标准 FIPS 140-2 级别 3。有关 FIPS 140-2 的详情，请访问以下网址：`http://www.nist.gov`。

在 FIPS 模式下操作板会导致板操作出现以下变化：

- 板本身仅提供 FIPS 认可的机制。
- 所有密钥和关键安全参数以加密形式通过 PCI 总线。
- 在启动时以及生成密钥和随机数时会进行特定的附加完整性检查。
- 随机数由 FIPS 认可的算法生成，该算法结合了保存的状态以及由基于热信噪的发生器 （使用散列法和算术）所生成的真正随机数据 （熵）。基于热信噪的发生器所生成的 512 位用于输出数据的每个 160 位。（在非 FIPS 模式中，基于热信噪的发生器所生成的 512 位经过 SHA-1 算法散列至 160 位。）

FIPS 模式仅可应用于 Sun Crypto Accelerator 4000 板本身。如上所述，当板置于 FIPS 模式时，板仅提供 FIPS 认可的机制。要注意的是， MD5、 RC2 和 RC4 均未得到 FIPS 认可。但是，由于 FIPS 规则仅适用于硬件，因此软件仍将继续提供其通常所提供的所有机制。

在 FIPS 模式下进行操作时，主要的不同之处是非 FIPS 认可的操作只能在软件中进行，有以下两种结果：

- 使用非 FIPS 认可的机制进行的加密操作将不会被加速。
- 如果使用非 FIPS 认可的机制进行的加密操作涉及 CKA_SENSITIVE 属性设为“True”的密钥，则操作会失败，因为 CKA_SENSITIVE 属性设为“True”的密钥只能用于硬件。

硬件加速和敏感密钥

板根据硬件的功能、安全要求和性能选择操作的执行位置。

PKCS#11 可以指定多种密钥类型和机制，但它们并非全部可用于硬件。当应用程序请求的操作、密钥和机制组合并非全部可用于硬件时，可以部分在软件中执行，部分在硬件中执行，或者完全在软件中执行。

当密钥的 CKA_SENSITIVE 属性为“True”时，则使用该密钥的任何操作必须安全地执行，也就是说，密钥资料不能离开硬件。如果硬件无法安全地执行操作，则会失败。另一方面，当密钥的 CKA_SENSITIVE 属性为“False”时，板将根据性能高低在硬件与软件之间作出选择。本节介绍的规则用于确定是选择硬件、软件还是选择停止操作。

为方便起见，定义了以下几组密钥和机制：

- hardware_key_set =
  - RSA，密钥大小不超过 2048 位
  - DSA，密钥大小不超过 1024 位
  - DES
  - 3DES
  - CDMF
- hardware_mechanism_set =
  - CKM_CDMF_...，不包括 CKM_CDMF_ECB
  - CKM_DES_...，不包括 CKM_DES_ECB
  - CKM_DES3_...，不包括 CKM_DES3_ECB
  - CKM_DSA
  - CKM_MD5，不适用于 FIPS 模式
  - CKM_RSA_...
  - CKM_SHA_1
- hardware_wrap_mechanism_set =
  - CKM_AES_CBC_PAD
  - CKM_CDMF_CBC_PAD
  - CKM_DES_CBC_PAD
  - CKM_DES3_CBC_PAD
  - CKM_RC2_CBC_PAD，不适用于 FIPS 模式

为了使任何操作均可在硬件中安全地执行，密钥必须在 hardware_key_set 中，并且机制必须在 hardware_mechanism_set 中。如果密钥在 hardware_key_set 中但机制未在 hardware_mechanism_set 中，则操作可能由硬件加速，但需要软件的协助。

C_DeriveKey 可在硬件中加速，但需要软件协助，因此它并不是硬件级安全。

下表介绍操作是否涉及密钥和操作位置：

表 8-1 处理大多数涉及密钥的加密操作

情况	CKA_SENSITIVE**=False**	CKA_SENSITIVE**=True**
硬件级安全	对于 RSA、DSA 和大容量缓冲器为硬件； 否则为软件	硬件
硬件加速，但可能需要软件协助	对于 RSA、DSA 和大容量缓冲器为硬件和软件；否则为软件	失败
仅限于软件	软件	失败

C_WrapKey 和 C_UnwrapKey 涉及对两个密钥的两种操作。对于 C_Wrap 密钥，将会执行编码操作，以对已打包密钥 (wrapped key) 进行编码，然后是加密操作，该操作使用打包密钥 (wrapping key) 对编码值进行加密。 C_UnwrapKey 与此相反，进行解密和解码。

如果已打包密钥为 RSA 或 DSA 密钥，且打包机制为 hardware_wrap_mechanism_set，则编码和加密步骤都在硬件中进行。此操作对两种密钥都是硬件级安全。

如果未能满足上述任何条件，则在软件中执行编码步骤。此操作对于已打包密钥不是硬件级安全。加密步骤将与使用打包密钥和机制的 C_Encrypt 操作同样对待。参见表 8-1。

下表汇总了各种情况：

表 8-2 C_WrapKey 和 C_UnwrapKey 的失败条件

条件	**已打包密钥为敏感密钥时失败**	**打包密钥为敏感密钥时失败**
已打包密钥为 RSA 或 DSA 且机制在 hardware_wrap_mechanism_set 中	–	–
打包密钥在 hardware_key_set 中且机制在 hardware_mechanism_set 中	失败	–
其它所有情况	失败	失败

C_Digest 在主机内存中组合整个缓冲器。如果缓冲器空间较大，但不超过 65532 字节，则 C_DigestFinal 会将整个缓冲器发送至硬件。否则，将在软件中处理整个缓冲器。

C_DigestKey 将密钥资料记入主机内存，随后通过 C_DigestUpdate 将其作为普通数据进行处理。如果密钥的 CKA_SENSITIVE 属性为 “True”，则会失败。

开发应用程序以使用 PKCS#11

必要的头文件位于 /opt/SUNWconn/cryptov2/include 中；将此目录添加至包含路径，并包含 cryptoki.h。 Sun Crypto Accelerator 4000 软件中提供了低级别的包含文件 pkcs11.h、 pkcs11f.h 和 pkcs11t.h。这些文件与 PKCS#11 web 站点 (http://www.rsasecurity.com/rsalabs/PKCS) 上提供的文件相同。 pkcs11_preamble.h 文件存在于包含目录中，必须置于低级别文件之前。

pkcs11 程序库的路径为：/opt/SUNWconn/cryptov2/lib/libvpkcs11.so。

Sun Crypto Accelerator 4000 程序库可以作为普通程序库进行链接，也可以通过 dlopen (3DL) 动态地将其打开。

当作为普通程序库进行链接时，使用以下命令：

```
cc [flags] files... -L /opt/SUNWconn/cryptov2/lib \
-R /opt/SUNWconn/cryptov2/lib -l vpkcs11 [other libraries...]
```

代码应直接调用函数，如下面的示例所示：

```
rv = C_Initialize(NULL);
```

动态链接时，使用以下命令 （已删节了错误处理）：

```
cc [flags] files... -ldl [ other libraries ... ]

#include "cryptoki.h"
#include <dlfcn.h>
#include <link.h>

void *cryptdlhandle;
CK_RV (*getfunctionlistp) (CK_FUNCTION_LIST_PTR *);
CK_FUNCTION_LIST *pk11funclist; /* may need to be globally
accessible */
CK_RV rv;
/* dlopen Sun Cryptoaccelerator 4000 library */
cryptodlhandle =
    dlopen("/opt/SUNWconn/cryptov2/lib/libvpkcs11.so",
    RTLD_NOW | RTLD_LOCAL | RTLD_GROUP);
if (cryptodlhandle == NULL) ...
/* Get pointer to C_GetFunctionList function */
getfunctionlistp = dlsym(cryptodlhandle, "C_getFunctionList");
if (getfunctionlistp == NULL) ...
/* Get libvpksc11's cryptki function list */
rv = (*getfunctionlistp) (&pk11funclist);
if (rv != CKR_OK) ...
```

代码应间接调用函数，如下所示：

```
rv = pk11funclist -> C_Initialize(NULL);
```

Sun Crypto Accelerator 4000 软件的任意限制非常少。大部分资源仅受主机内存的限制。令牌 （包括 acceleration-only 令牌）的最大数目为 1024。

为了防止故障或恶意程序产生的阻断服务攻击消耗过多核心内存，软件将任何 Solaris 用户 （非进程）能够耗用的核心内存数量限制为不超过 16 MB。此限制不可配置。

以下建议可以防止核心内存耗尽的问题：

- 不要丢弃多步骤操作。调用适当的终止函数 （例如， `C_EncryptFinal`）或在完成时关闭会话。
- 不要丢弃不需要的对象。关闭正在创建的会话（仅对易失对象有效）或在完成时调用 `C_DestroyObject`。
- 切勿一次提交超大型 （数兆字节）数据区块。（此操作不适用于摘要操作，因为较大的摘要操作始终在软件中进行。）

不执行 PKCS#11 管理函数 `C_InitToken` 和 `C_InitPin`。拒绝执行带 `CKU_SO`（安全主管）标记的 `C_Login` 函数。

在 PKCS#11 中， *public token （公共令牌）*对象为可见的永久对象，无须验证即可删除。由于 Sun Crypto Accelerator 4000 软件已知的用户与 Solaris 用户无关，加之软件需在 C_Login 完成后才能确定用户身份，这些对象需要在全局范围内显示给所有用户，因而可由任何用户删除。由于此行为不可接受，因此不允许存在公共令牌对象。创建公共令牌对象的任何尝试都将失败。

易失 （会话）对象的数目仅受虚拟内存的限制。永久对象必须全部装入板上的 RAM，但实际应用并不受此限制。为与此概念保持一致，指示内存最大值的 CK_TOKEN_INFO 结构字段 （由 C_GetTokenInfo 函数返回）都设置为 CK_EFFECTIVELY_INFINITE。不执行 C_GetObjectSize 函数。

不执行可选 *dual operation* 函数 （C_DigestEncryptUpdate、C_DecryptDigestUpdate、 C_SignEncryptUpdate 和 C_DecryptVerifyUpdate），且由 C_GetTokenInfo 返回的标记字段中的 CKF_DUAL_OPERATIONS_FLAG 为 “False”。

仅对 C_GetOperationState 与其伴随函数 C_SetOperationState 进行有限的执行。仅在操作为 C_Digest 且累积输入数据大小不超过 65532 字节时，C_GetOperationState 才能完成。

Sun Crypto Accelerator 4000 系统所提供的令牌被视为不可删除。因此，CK_GetSlotInfo 返回的 CKF_REMOVABLE_DEVICE 标记为 “False”。

不执行 C_WaitForSlotEvent 函数，且 Sun Crypto Accelerator 4000 系统永不调用作为 Notify 参数传送至 C_OpenSession 的回调函数。软件永远不会通过 C_OpenSession 的 pApplication 参数将控制交回给调用应用程序。

Sun Crypto Accelerator 4000 板包含高质量的真正随机数发生器。因此，它不需要输入源数字，实际上 C_SeedRandom 将会因为 CKR_RANDOM_SEED_NOT_SUPPORTED 而被拒绝。

如果函数的执行取决于不受限制的主机内存中的关键字段，则当它们涉及在 CKA_SENSITIVE 属性设为 “True”时创建的密钥时，这些函数将会失败。具体规则如下：

- 如果密钥将 CKA_SENSITIVE 设为 “True”，则 C_DigestKey 会失败。
- 如果基本密钥或要衍生的密钥将 CKA_SENSITIVE 设为 “True”，则对于所有机制，C_DeriveKey 均会失败。
- 如果已打包或已解包的密钥将 CKA_SENSITIVE 设为 “True”，且以下任何条件为 “True”，则 C_WrapKey 和 C_UnwrapKey 会失败。
  - 密钥为除 RSA 或 DSA 密钥之外的其它密钥。
  - 机制为除 CKM_DES_CBC_PAD、 CKM_DES3_CBC_PAD、 CKM_RC2_CBC_PAD 或 CKM_AES_CBC_PAD 之外的其它机制。

- 如果密钥将 CKA_SENSITIVE 设为 “True”，则涉及以下机制的任何操作均将失败：
  - CKM_AES...
  - CKM_CDMF_ECB
  - CKM_DES_ECB
  - CKM_DES3_ECB
  - CKM_DH...
  - CKM_MD5_HMAC...
  - CKM_RC2...
  - CKM_RC4...
  - CKM_SHA_1_HMAC...
  - CKM_SSL3...
  - CKM_TLS...
- 如果 CKA_SENSITIVE 设为 “True”，则涉及大于 2048 位的 RSA 密钥或大于 1024 位的 DSA 密钥的任何操作均会失败。

CKA_EXTRACTABLE 属性默认值为 “True”。 CKA_SENSITIVE 属性的默认值与 CKA_EXTRACTABLE 相反。尝试将 CKA_SENSITIVE 和 CKA_EXTRACTABLE 均设为 “False”时，会导致 CKR_TEMPLATE_INCONSISTENT 失败。

通常检测不到属性不一致情况。例如，当某个模板多次包含相同的属性时，执行仅使用最后一个值。对于与密钥类型不相关的属性，只是简单地将其忽略。不能检测到所有无效的属性。

不执行 CKA_LOCAL、CKA_ALWAYS_SENSITIVE 和 CKA_NEVER_EXTRACTABLE 属性。

软件返回的错误代码并非总是期望的代码。特别是对于许多错误可能返回 CKR_MECHANISM_INVALID，而其它值可能更合适。返回代码 CKR_HOST_MEMORY 通常意味着内部调用 malloc(3c) 命令失败。返回此错误后，可能未正确保存重要状态，因此尝试继续时可能失败 （除非通过调用 C_Finalize）。

为减少开销，软件在执行 C_EncryptInit 和类似函数时，有时会延迟将密钥发送至板，直至出现需要加密的实际数据。延迟的结果是：某些 PKCS#11 声明的错误，本应由 C_EncryptInit （和类似函数）报告，实际上却在以后首次调用 C_EncryptUpdate （和类似函数）时报告。

Sun Crypto Accelerator 4000 软件中提供了下列可由 PKCS#11 指示符识别的机制。尽管 CKM_SSL3... 和 CKM_TLS... 机制也显示在列表中，但是，只有在 /etc/opt/SUNWconn/cryptov2/sslreg 文件存在时，它们才可用于带密钥库的令牌 （参阅第 194 页 “管理板以使用 PKCS#11”）。

- CKM_AES_CBC
- CKM_AES_CBC_PAD
- CKM_AES_ECB
- CKM_AES_KEY_GEN
- CKM_CDMF_CBC
- CKM_CDMF_CBC_PAD
- CKM_CDMF_ECB
- CKM_CDMF_KEY_GEN
- CKM_DES2_KEY_GEN

- CKM_DES3_CBC
- CKM_DES3_CBC_PAD
- CKM_DES3_ECB
- CKM_DES3_KEY_GEN
- CKM_DES_CBC
- CKM_DES_CBC_PAD
- CKM_DES_ECB
- CKM_DES_KEY_GEN
- CKM_DH_PKCS_DERIVE
- CKM_DH_PKCS_KEY_PAIR_GEN
- CKM_DSA
- CKM_DSA_KEY_PAIR_GEN
- CKM_MD5
- CKM_MD5_HMAC
- CKM_MD5_HMAC_GENERAL
- CKM_RC2_CBC
- CKM_RC2_CBC_PAD
- CKM_RC2_ECB
- CKM_RC2_KEY_GEN
- CKM_RC4
- CKM_RC4_KEY_GEN
- CKM_RSA_PKCS
- CKM_RSA_PKCS_KEY_PAIR_GEN
- CKM_RSA_X_509
- CKM_SHA_1
- CKM_SHA_1_HMAC
- CKM_SHA_1_HMAC_GENERAL
- CKM_SSL3_KEY_AND_MAC_DERIVE
- CKM_SSL3_MASTER_KEY_DERIVE
- CKM_SSL3_MD5_MAC
- CKM_SSL3_PRE_MASTER_KEY_GEN
- CKM_SSL3_SHA1_MAC
- CKM_TLS_KEY_AND_MAC_DERIVE
- CKM_TLS_MASTER_KEY_DERIVE
- CKM_TLS_PRE_MASTER_KEY_GEN

RSA、 DSA 和 Diffie-Hellman 密钥的最大大小如下：

表 8-3 最大密钥大小

密钥	非敏感密钥大小最大值	敏感密钥大小最大值
RSA	4096	2048
DSA	4096	1024
DH	2048	不可用

不要假设对象句柄或会话句柄为较小的整数或按顺序分配。这些句柄可能为任何无符号长整型。

可传送至 C_Initialize 的互斥回调函数指示符会被忽略。

在许多情况下，对小数量数据的操作由主机处理器 （而不是由板）进行处理，因为将操作发送至板的成本超出在主机上执行操作的成本。但是，当操作涉及 CKA_SENSITIVE 属性设为 “True”的对象时，将会在板中进行。

如果所有 C_DigestUpdate 缓冲器的累积大小超出 65532 字节，则由主机中的软件处理摘要操作。这同样适用于 C_Digest。因此，较小的和极大量的数据将由软件进行处理。

当用户成功执行 C_Login 函数并保留在高速缓存中时，有关永久对象的信息会引入进程中。以后，另一进程创建、删除或修改永久对象时，可能不会加以观注。发生在板上的操作将使用最新状态的密钥。（操作在板上执行的条件是：板能执行操作且密钥敏感；或者板能执行操作且缓冲器足够大，能对其进行调整）。对于其它所有情况 （包括 C_FindObjects 函数），操作将使用高速缓存状态的密钥在软件中执行。

注意 – 不要以为上述高速缓存密钥行为在将来的版本中保持不变。

正如 PKCS#11 标准所要求，当用户调用 C_Logout 函数或关闭最后的 PKCS#11 会话时，所有永久对象句柄均将失效。软件将从软件高速缓存器中清除令牌对象。后续成功的 C_Login 函数会引入所有当时最新的令牌对象。请注意，此登录可用于不同用户，因此会引入不同的令牌对象组。但是，即使此登录用于相同用户，令牌对象可能也不会获得与以前相同的句柄。

附录 **A**

规格

本附录介绍 Sun Crypto Accelerator 4000 MMF 和 UTP 适配器的规格，包括以下几节：

Sun Crypto Accelerator 4000 MMF 适配器

本节介绍 Sun Crypto Accelerator 4000 MMF 适配器的规格。

连接器

图 A-1 显示了 Sun Crypto Accelerator 4000 MMF 适配器的连接器。

图 A-1 Sun Crypto Accelerator 4000 MMF 适配器连接器

表 A-1 列出了 SC 连接器 (850 nm) 的特性。

表 A-1 SC 连接器链接特性 (IEEE P802.3z)

特性	62.5 微米 MMF	50 微米 MMF
操作范围	最长 260 米	最长 550 米

物理尺寸

表 A-2 物理尺寸

尺寸	测量	测量 （公制）
长度	12.283 英寸	312.00 毫米
宽度	4.200 英寸	106.68 毫米

性能规格

表 A-3 性能规格

功能	规格
PCI 时钟	最大 33/66 MHz
PCI 数据瞬间传输速率	最大 64 字节 （瞬间）
PCI 数据/地址宽度	32/64 位
PCI 模式	主控/从属
1 Gbps, 850 nm	1000 Mbps （全双工）

电源要求

表 A-4 电源要求

规格	测量
最大功耗	6.25 W @ 5V 12.75 W @ 3.3V
电压容差	5V +/- 5% 3.3V +/- 5%

接口规格

表 A-5 接口规格

功能	规格
PCI 时钟	33 MHz 或 66 MHz
主机接口	PCI 2.1，支持 33 MHz 或 66 MHz 时钟速率以及 3.3V 或 5V 电源
PCI 总线宽度	32 位或 64 位

环境规格

表 A-6 环境规格

条件	工作规格	存储规格
温度	0° 至 +55°C， +32° 至 +131°F	-40° 至 +75°C， -40° 至 +167°F
相对湿度	5 至 85%（无凝结）	0 至 95%（无凝结）

Sun Crypto Accelerator 4000 UTP 适配器

本节介绍 Sun Crypto Accelerator 4000 UTP 适配器的规格。

连接器

图 A-2 显示了 Sun Crypto Accelerator 4000 UTP 适配器的连接器。

图 A-2 Sun Crypto Accelerator 4000 UTP 适配器连接器

表 A-7 列出了 Sun Crypto Accelerator 4000 UTP 适配器所用的 5 类连接器的特性。

表 A-7 5 类连接器的链接特性

特性	说明
操作范围	最长 100 米

物理尺寸

表 A-8 物理尺寸

尺寸	测量	测量 （公制）
长度	12.283 英寸	312.00 毫米
宽度	4.200 英寸	106.68 毫米

性能规格

表 A-9 性能规格

功能	规格
PCI 时钟	最大 33/66 MHz
PCI 数据瞬间传输速率	最大 64 字节 （瞬间）
PCI 数据/地址宽度	32/64 位
PCI 模式	主控/从属
1 Gbps	1000 Mbps （全双工）
100 Mbps	100 Mbps （全双工和半双工）
10 Mbps	10 Mbps （全双工和半双工）

电源要求

表 A-10 电源要求

规格	测量
最大功耗	6.25 W @ 5V 12.75 W @ 3.3V
电压容差	5V +/- 5% 3.3V +/- 5%

接口规格

表 A-11 接口规格

功能	规格
PCI 时钟	33 MHz 或 66 MHz
主机接口	PCI 2.1，支持 33 MHz 或 66 MHz 时钟速率以及 3.3V 或 5V 电源
PCI 总线宽度	32 位或 64 位

环境规格

表 A-12 环境规格

条件	工作规格	存储规格
温度	0° 至 +55°C， +32° 至 +131°F	-40° 至 +75°C， -40° 至 +167°F
相对湿度	5 至 85%（无凝结）	0 至 95%（无凝结）

附录 **B**

在不使用安装脚本的情况下安装软件

本附录介绍如何在不使用产品 CD 所提供的安装脚本 (`/cdrom/cdrom0/install`) 的情况下手动安装 Sun Crypto Accelerator 4000 软件。其中包括以下几节：

手动安装软件

Sun Crypto Accelerator 4000 软件随产品 CD 提供。您可能需要从 SunSolve Web 站点 (`http://sunsolve.sun.com`) 下载修补程序。有关详细信息，请参阅第 10 页 “必需的修补程序”。

▼ 手动安装软件

1. **将 Sun Crypto Accelerator 4000 CD 放入与系统相连的 CD-ROM 驱动器。**
   - 如果系统正在运行 Sun Enterprise Volume Manager，则会自动将 CD-ROM 挂装到 `/cdrom/cdrom0` 目录。
   - 如果系统未运行 Sun Enterprise Volume Manager，请按以下方法挂装 CD-ROM：

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

您可在 /cdrom/cdrom0 目录中找到以下文件和目录。

表 B-1 /cdrom/cdrom0 目录中的文件

文件或目录	内容	
Copyright	美国版权文件	
FR_Copyright	法国版权文件	
install	用于安装 Sun Crypto Accelerator 4000 软件的安装脚本	
remove	用于删除 Sun Crypto Accelerator 4000 软件的删除脚本	
Docs	*Sun Crypto Accelerator 4000 板 1.1 版安装和用户指南* *Sun Crypto Accelerator 4000 板发布说明*	
Packages	Sun Crypto Accelerator 4000 软件包：	
	SUNWkcl2r	加密核心组件
	SUNWkcl2u	加密管理实用程序和程序库
	SUNWkcl2a	Apache 的 SSL 支持 *（可选）*
	SUNWkcl2m	加密管理手册页 *（可选）*
	SUNWvcar	VCA Crypto Accelerator (root)
	SUNWvcau	VCA Crypto Accelerator (usr)
	SUNWvcaa	VCA 管理
	SUNWvcafw	VCA 固件
	SUNWvcamn	VCA Crypto Accelerator 手册页 *（可选）*
	SUNWvcav	VCA Crypto Accelerator 的 SunVTS 测试程序 *（可选）*
	SUNWkcl2o	SSL 开发工具和程序库 *（可选）*
	SUNWkcl2i.u	采用 KCLv2 Crypto 的 IPsec 加速 *（可选）*

必需的软件包必须按特定的顺序安装，并且必须在安装任何可选软件包之前安装。安装必需的软件包之后，您可以按任意顺序安装和删除可选软件包。

仅在计划将 Apache 用作 Web 服务器时，才有必要安装可选的 SUNWkcl2a 软件包。

仅在计划重新链接到另一（不支持）版本的 Apache Web Server 时，才有必要安装可选的 SUNWkcl2o 软件包。

仅在计划执行 SunVTS 测试时，才有必要安装可选的 SUNWvcav 软件包。您必须在安装 SunVTS 4.4 或最新 5.x 版本之后才能安装 SUNWvcav 软件包。

注 – Sun Crypto Accelerator 4000 CD 中的可选 SUNWkcl2i.u 软件包只有 .u 扩展名。安装该软件包之后，其名称会更改为 SUNWkcl2i。该软件包在 CD 上的 .u 扩展名表示此软件包专用于 sun4u 体系结构。

1. **通过输入以下命令安装必需的软件包：**

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2r SUNWkcl2u SUNWkcl2m SUNWvcar SUNWvcau SUNWvcaa SUNWvcamn
SUNWvcafw
```

2. **（可选）要检查是否正确安装了软件，请运行** pkginfo **命令。**

```
# pkginfo SUNWkcl2r SUNWkcl2u SUNWvcar SUNWvcau SUNWvcaa SUNWvcafw
system      SUNWkcl2r      KCLv2 Crypto (Root)
system      SUNWkcl2u      KCLv2 Crypto Support Software
system      SUNWvcaa       VCA Crypto Accelerator/Gigabit Ethernet Admin
system      SUNWvcafw      VCA Crypto Accelerator/Gigabit Ethernet firmware
system      SUNWvcar       VCA Crypto Accelerator/Gigabit Ethernet Drivers
system      SUNWvcau       VCA Crypto Accelerator/Gigabit Ethernet Daemon
```

3. **（可选）要检查是否已附带了驱动程序，请运行** prtdiag **命令。**

   参阅 prtdiag(1m) 联机手册页。

```
# prtdiag -v
```

4. **（可选）运行** modinfo **命令，查看是否已加载模块。**

```
# modinfo | grep Crypto
62   1317f62  20b1f 198   1  vca (VCA Crypto/Ethernet v1.102)
63   13360e9  12510 200   1  kcl2 (Kernel Crypto Library v1.148)
197  136d5d6   19b0 199   1  vcactl (VCA Crypto Control v1.19)
```

安装可选软件包

如果只想安装为 Apache Web Server 和 Sun Crypto Accelerator 4000 联机手册页提供 SSL 支持的可选软件包，请输入以下命令：

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2a SUNWkcl2m
```

若要安装所有的可选软件包，请输入以下命令：

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2a SUNWkcl2m SUNWvcamn SUNWvcav SUNWkcl2o SUNWkcl2i.u
```

有关上述示例中可选软件包的内容说明，请参阅表 B-1。

目录和文件

表 B-2 列出了 Sun Crypto Accelerator 4000 软件在采用默认方式安装时所创建的目录。

表 B-2 Sun Crypto Accelerator 4000 目录

目录	内容
/etc/opt/SUNWconn/vca/keydata	密钥库数据 （已加密）
/opt/SUNWconn/cryptov2/bin	实用程序
/opt/SUNWconn/cryptov2/lib	支持程序库
/opt/SUNWconn/cryptov2/sbin	管理命令

图 B-1 显示了这些目录和文件的层次结构。

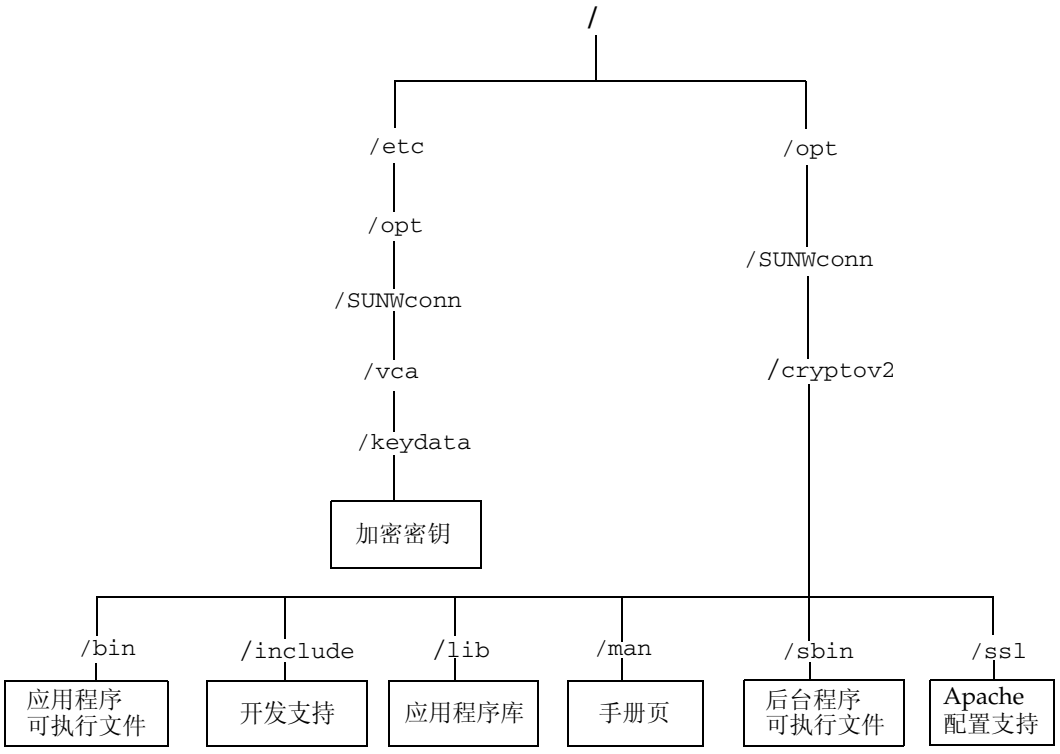

图 B-1 Sun Crypto Accelerator 4000 目录和文件

注 – 安装板的硬件和软件之后，您需使用配置和密钥库信息来初始化板。有关如何初始化板的信息，请参阅第 62 页 “通过 vcaadm 初始化板”。

手动删除软件

如果您已创建了密钥库 （参阅第 65 页 “通过 vcaadm 管理密钥库”），则在删除软件之前必须删除 Sun Crypto Accelerator 4000 板配置的密钥库信息。 zeroize 命令可删除所有密钥资料，但不能删除密钥库文件 （存储于安装板的物理主机的文件系统中）。有关 zeroize 命令的详细说明，请参阅第 74 页 “在板上执行软件零置”。要删除保存在系统中的密钥库文件，请先成为超级用户，然后删除密钥库文件。如果尚未创建任何密钥库文件，则可以跳过该步骤。

注意 – 如果某个密钥库正在使用中，或者由其他用户和密钥库共用，切勿删除该密钥库。要释放对密钥库的引用，必须关闭 Web 服务器和/或管理服务器。

注意 – 删除 Sun Crypto Accelerator 4000 软件之前，请禁用任何与 Sun Crypto Accelerator 4000 板配合使用的 Web 服务器。否则，这些 Web 服务器将无法工作。

▼ 手动删除软件

- **成为超级用户，使用 pkgrm 命令只删除您所安装的软件包。**

注意 – 安装的软件包必须按所示顺序删除。不按此顺序删除软件包时会显示相关性警告，并且会使核心模块仍处于加载状态。

如果您安装了所有软件包，则应按如下所示顺序进行删除：

```
# pkgrm SUNWkcl2o SUNWvcav SUNWvcar SUNWkcl2a SUNWkcl2u SUNWkcl2r
SUNWvcamn SUNWkcl2m SUNWkcl2i SUNWvcaa SUNWvcafw SUNWvcau
```

注 – 安装或删除 Sun Crypto Accelerator 4000 板的 SunVTS 测试程序 (SUNWvcav) 时，如果 SunVTS 正在运行，则在安装或删除之后必须重新检测系统，以更新可用的测试程序。有关详细信息，请参见您的 SunVTS 文档。

附录 C

Apache Web Server 的 SSL 配置指令

本附录介绍通过 Sun Crypto Accelerator 4000 软件为 Apache Web Server 配置 SSL 支持时所用的指令。您应在 `http.conf` 文件中配置指令。有关详细信息，请参阅 Apache Web Server 文档。

1. `SSLPassPhraseDialog exec:`*program*

   环境：全局

   该指令用于通知 Apache Web Server 应执行指定的 *program*，以收集密钥文件的密码。 *program* 会将收集到的密码输出到标准输出设备上。

   如果存在多个密钥文件，并且它们使用共同的密码，则 *program* 只执行一次 （再次运行 *program* 之前，将会尝试每个收集到的密码。）

   program 执行时使用两个参数：第一个参数是服务器名称，采用 *servername*:*port* 格式，如 `www.fictional-company.com:443`。端口 443 是基于 SSL 的 Web 服务器的典型端口。第二个参数是密钥文件中的密钥类型 (*keytype*)。 *keytype* 可以是 RSA 或 DSA。

注 – 由于该程序可以在系统启动期间运行，因此应对其进行设计，以应付控制台不是 `tty` 设备的情况 （即 `tty`(3c) 返回 false 值）。

   随附的程序 `/opt/SUNWconn/cryptov2/bin/apgetpass` 可供 *program* 执行文件使用。该程序会自动提示您输入密码，而且在输入密码时不显示密码。

   另外，随附的 `sslpassword` 程序还可以自动搜索文件中的密码，从而避免在 Web 服务器启动期间进行用户交互操作。它将在名为 `/etc/apache/`*servername*:*port*.*keytype*`.pass` 的文件中搜索密钥文件的密码。如果该文件不存在，则使用 `/etc/apache/default.pass` 文件。这些密码文件仅包含未加密的密码，密码自成一行。

注 – 密码文件应通过权限加以保护，从而只允许 Web 服务器以其身份运行的 UNIX 用户读取文件。该用户应该是使用标准 Apache `User` 指令配置的同一用户。

   如果未指定，则默认操作会使用内部提示机制。请勿使用默认操作，而使用随附的 `sslpassword` 程序，以避免系统启动时的交互问题。

2. `SSLEngine (on|off)`

   环境：全局，虚拟主机

   该指令用于启用 SSL 协议。它通常在虚拟主机中使用，以便对一小部分服务器启用 SSL。常用的一种格式是：

```
<VirtualHost _default_:443>
SSLEngine on
</VirtualHost>
```

   此语句为监听端口 443 （标准 HTTPS 端口）的任何服务器配置 SSL。如果不存在，将禁用此协议 （默认设置）。

3. `SSLProtocol [+-]`*protocol*

   环境：全局，虚拟主机

   该指令用于配置服务器在进行 SSL 事务处理时应使用的协议。表 C-1 列出并说明了可用的协议：

表 C-1 SSL 协议

协议	说明
`SSLv2`	Netscape 提出的最初标准 SSL 协议
`SSLv3`	SSL 协议的更新版本，是大多数流行的 Web 浏览器支持的协议
`TLSv1`	`SSLv3` 的更新版本，当前正由 IETF 进行规范，支持它的浏览器很少
`all`	启用所有协议

   可用加号 (+) 或减号 (-) 来添加或删除协议。例如，要禁用对 SSLv2 的支持，可以使用以下指令：

```
SSLProtocol all -SSLv2
```

   上一语句与下一语句等效：

```
SSLProtocol +SSLv3 +TLSv1
```

4. `SSLCipherSuite` *cipher-spec*

   环境：全局，虚拟主机，目录， `.htaccess`

   SSLCipherSuite 指令用于配置可用的 SSL 密码及其首选项。在全局环境或虚拟主机环境中，该指令在初次 SSL 握手时使用。在目录环境中，它强制执行 SSL 重新协商以使用指定的密码。重新协商在读取请求之后且在发送响应之前发生。

   cipher-spec 可以是一个由冒号分隔的密码列表，表 C-2 列出了这些密码。在表 C-2 中，DH 指 Diffie-Hellman， DSS 指数字签名标准。

表 C-2 可用的 SSL 密码

密码标记	协议	密钥交换	验证	加密	MAC	类型
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES （168 位）	SHA1	
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES （168 位）	MD5	
RC4-SHA	SSLv3	RSA	RSA	ARCFOUR （128 位）	SHA1	
RC4-MD5	SSLv3	RSA	RSA	ARCFOUR （128 位）	MD5	
RC4-MD5	SSLv2	RSA	RSA	ARCFOUR （128 位）	MD5	
RC2-CBC-MD5	SSLv2	RSA	RSA	ARCTWO （128 位）		
DES-CBC-SHA	SSLv3	RSA	RSA	DES （56 位）	SHA1	
RC4-64-MD5	SSLv2	RSA	RSA	ARCFOUR （64 位）	MD5	
DES-CBC-MD5	SSLv2	RSA	RSA	DES （56 位）	MD5	
EXP-DES-CBC-SHA	SSLv3	RSA （512 位）	RSA	DES （40 位）	SHA1	导出
EXP-RC2-CBC-MD5	SSLv2	RSA （512 位）	RSA	ARCTWO （40 位）	SHA1	导出
EXP-RC2-CBC-MD5	SSLv3	RSA （512 位）	RSA	ARCTWO （40 位）	SHA1	导出
EXP-RC4-MD5	SSLv3	RSA （512 位）	RSA	ARCFOUR （40 位）	MD5	导出
EXP-RC4-MD5	SSLv2	RSA （512 位）	RSA	ARCFOUR （40 位）	MD5	导出
NULL-SHA	SSLv3	RSA	RSA	无	SHA1	
NULL-MD5	SSLv3	RSA	RSA	无	MD5	
ADH-DES-CBC3-SHA	SSLv3	DH	无	3DES （168 位）	SHA1	
ADH-DES-CBC-SHA	SSLv3	DH	无	DES （56 位）	SHA1	
ADH-RC4-MD5	SSLv3	DH	无	ARCFOUR （128 位）	MD5	
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES （168 位）	SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES （168 位）	SHA1	
EDH-RSA-DES-CBC-SHA	SSLv3	DH	RSA	DES （56 位）	SHA1	

表 C-2 可用的 SSL 密码 *（续）*

密码标记	协议	密钥交换	验证	加密	MAC	类型
EDH-DSS-DES-CBC-SHA	SSLv3	DH	DSS	DES （56 位）	SHA1	
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH （512 位）	RSA	DES （40 位）	SHA1	导出
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	DH （512 位）	DSS	DES （40 位）	SHA1	导出
EXP-ADH-DES-CBC-SHA	SSLv3	DH （512 位）	无	DES （40 位）	SHA1	导出
EXP-ADH-RC4-MD5	SSLv3	DH （512 位）	无	ARCFOUR （40 位）	MD5	导出

表 C-3 列出并说明了可以提供类似宏分组的别名。

表 C-3 SSL 别名

别名	说明
SSLv2	所有 SSL 版本 2.0 密码
SSLv3	所有 SSL 版本 3.0 密码
EXP	所有导出级别密码
EXPORT40	所有 40 位导出密码
EXPORT56	所有 56 位导出密码
LOW	长度较短的密码 （DES， 40 位 RC4）
MEDIUM	所有 128 位密码
HIGH	所有使用 Triple DES 的密码
RSA	所有使用 RSA 密钥交换的密码
DH	所有使用 Diffie-Hellman 密钥交换的密码
EDH	所有使用 Ephemeral Diffie-Hellman 密钥交换的密码
ADH	所有使用匿名 Diffie-Hellman 密钥交换的密码
DSS	所有使用 DSS 鉴定的密码
NULL	所有不使用加密功能的密码

您可使用表 C-4 中列出并说明的特殊字符来配置密码的首选项。

表 C-4 配置密码首选项的特殊字符

字符	说明
<none>	将密码添加到列表中
!	从列表中完全删除密码 — 无法再次添加密码
+	将密码添加到列表，并拖至当前位置 （可能要将其降级）
-	从列表中删除密码 （以后可在列表中添加）

cipher-spec 的默认值是

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
```

此默认值将配置除匿名 （未验证）的 Diffie-Hellman 之外的所有密码，将 ARCFOUR 和 RSA 置为首选项，然后是由高至低的加密级别。

5. `SSLCertificateFile` *file*

   环境：全局，虚拟主机

   该指令用于指定此服务器的 PEM 编码 X.509 证书文件的位置。

6. `SSLCertificateKeyFile` *file*

   环境：全局，虚拟主机

   该指令用于指定此服务器的 PEM 编码私钥文件的位置，它与使用 `SSLCertificateFile` 指令配置的证书对应。

7. `SSLCertificateChainFile` *file*

   环境：全局，虚拟主机

   该指令用于指定包含 PEM 编码证书 （用于构成服务器鉴定路径）的文件的位置。当服务器证书不是由客户机认可的认证机构直接签名时，您可使用该指令来协助客户机验证服务器证书。

   使用客户机验证 (`SSLVerifyClient`) 时，同时假定此链中的证书对于客户机验证有效。

8. `SSLCACertificateFile` *file*

   环境：全局，虚拟主机

   该指令用于指定包含认证机构 (CA) 证书级联 （用于客户机验证）的文件的位置。

9. `SSLCARevocationFile` *file*

   环境：全局，虚拟主机

   该指令用于指定包含 CA 证书调用列表级联 （用于客户机验证）的文件的位置。

10. SSLVerifyClient *level*

环境：全局，虚拟主机，目录， .htaccess

该指令用于配置服务器对客户机的验证。注意：正常情况下，该指令不需要用于电子商务应用程序，而用于其它应用程序。

表 C-5 列出并说明了 *level* 的值。

表 C-5 SSL 验证客户机级别

级别	说明
none	不要求客户机提供证书
optional	客户机可能需要提供有效证书
require	客户机*必须*提供有效证书
optional_no_ca	客户机可能需要提供证书，但证书无需有效

通常情况下使用 none 或 require。默认值为 none。

11. SSLVerifyDepth *depth*

环境：全局，虚拟主机，目录， .htaccess

该指令指定服务器允许的客户机证书的最大证书链深度。如果值为 0，则表示仅自签名证书为合格证书；如果值为 1，则表示客户机证书必须由服务器直接识别的 CA 签名（通过 SSLCACertificateFile）。值较大时允许 CA 授权。

12. SSLLog *filename*

环境：全局，虚拟主机

该指令指定用于记录 SSL 特定信息的日志文件。如果不指定（默认值），则不会记录 SSL 特定信息。

13. SSLLogLevel *level*

环境：全局，虚拟主机

该指令指定 SSL 日志文件中所记录信息的详细程度。表 C-6 列出并说明了 *level* 的值。

表 C-6 SSL 日志级别值

值	说明
none	不进行日志记录，但仍将错误消息发送到标准的 Apache 错误日志中
warn	包括警告消息
info	包括信息消息
trace	包括跟踪消息
debug	包括调试消息

14. `SSLOptions [+-] option`

环境：全局，虚拟主机，目录， `.htaccess`

该指令按目录来配置 SSL 运行选项。在选项前面加上加号 (+) 前缀，可将选项添加到当前配置中；或者使用减号 (-) 删除当前配置中的选项。如果多个选项应用于一个目录，则使用限制性最强的选项；选项不能合并。

表 C-7 列出并说明了这些选项。

表 C-7 可用的 SSL 选项

选项	说明
`StdEnvVars`	创建一组标准的与 SSL 相关的 CGI/SSI 环境变量 — 它会在性能上有所下降。
`ExportCertData`	导出 `SSL_SERVER_CERT`、`SSL_CLIENT_CERT` 和 `SSL_CLIENT_CERT_CHAIN`*n* (*n* = 0, 1, ...) 环境变量。这些变量包含 PEM 编码的客户机和服务器证书。
`FakeBasicAuth`	客户机证书的识别名 (DN) 被转换成一个 HTTP 基本验证用户名，且 “被伪装” 以进行验证。它允许在 SSL 客户机验证时使用标准的 Apache 访问控制机制，即不提示用户提供密码。Apache 密码文件中的这些用户的条目必须使用加密密码 `xxj31ZMTZzkVA`。它只是 “密码” 一词的加密形式 (`crypt`(3c))。
`StrictRequire`	由于忽略 `SSLRequireSSL` 而强制进行非法访问，即使存在会覆盖本指令的其它指令，如 `Satisfy Any` 等，也会如此。

15. `SSLRequireSSL`

环境：目录， `.htaccess`

除非使用 HTTPS，否则该指令禁止对给定目录的访问。您可使用该指令来防止因错误配置而导致目录内容受到未验证和未加密的访问。

附录 D

配置自定义应用程序以使用板

本附录介绍随板一起提供的软件。此软件可用于构建与 OpenSSL 兼容的应用程序，从而充分利用板的加密加速功能。本附录所述的编译方式并非有益于所有 OpenSSL 应用程序。某些应用程序由于使用 OpenSSL 程序库 （可从 `http://www.openssl.org` 下载）进行构建而受益。

配置自定义应用程序以使用板

有关构建应用程序以使用 Sun Crypto Accelerator 4000 软硬件的信息严格 “按原样” 提供，不是本产品正式支持的部分。此类信息可能有用，但不提供任何担保。如果需要 Sun 支持的解决方案，请与 Sun Professional Services （专业服务）联系，了解适于您的方案选项。

▼ 配置自定义应用程序以使用板

1. **安装包含必需头文件和程序库的 `SUNWkcl2o` 软件包。**
2. **配置应用程序，以包含 `/opt/SUNWconn/cryptov2/include` 中的 OpenSSL 头文件，例如具有以下编译程序标记的头文件：**

```
-I/opt/SUNWconn/cryptov2/include
```

3. **修改链接器，以包含指向适当程序库的引用。**

   大多数与 OpenSSL 兼容的应用程序均引用 `libcrypto.a` 或 `libssl.a` 程序库，或者同时引用这两个程序库。包括 Sun 加密程序库。可用下面的链接器属性来完成此操作：

```
-L/opt/SUNWconn/cryptov2/lib -R/opt/SUNWconn/cryptov2/lib \
-lcrypto -lssl -lkcl
```

附录 **E**

软件许可

本附录介绍 Sun 二进制代码许可协议以及第三方软件的声明和许可。

注 – 本附录中的第三方许可和声明完全由软件许可和声明的所有方提供。

Sun Microsystems, Inc.

二进制代码许可协议

打开软件介质包装之前，请仔细阅读本协议的条款和任何提供的补充许可条款 （统称 “协议”）。如果打开软件介质包装，即表示您接受本 “协议” 的条款。当通过电子方式访问软件时，如果您在本 “协议” 的末尾选择 “接受” 按钮，即表示您接受这些条款。如果您不接受所有这些条款，请立即将尚未使用的软件退回，以获得退款；或者，如果您通过电子方式访问软件，请在本 “协议” 的末尾选择 “拒绝” 按钮。

1. 使用许可。根据与您所支付费用相对应的用户数目和计算机硬件类别， Sun 授予您非独占且不可转让的许可，允许您仅在内部使用随附的软件和文档以及 Sun 提供的任何错误更正 （统称 “软件”）。

2. 限制。“软件” 属于机密文件，且受版权法保护。“软件” 的产权和所有相关的知识产权为 Sun 及其许可发行者所有。您只能制作一份用于备份目的的 “软件” 副本；除此之外，不得制作任何 “软件” 副本 （除非补充许可条款中另有规定）。除非与相关适用法律相抵触，否则您不可以修改、反编译 “软件” ，也不可以对 “软件” 进行逆向工程。您承认 “软件” 的设计、许可或用途并非用于设计、构造、操作或维护任何核设施。Sun 否认任何对此类用途适用性的明示或暗示保证。与 Sun 或其许可发行者的任何商标、服务商标、徽标或产品名称有关的权利、产权或利益，不在本 “协议” 的许可范围之内。

3. 有限担保。 Sun 向您保证，自购买之日 （以收据复件上的日期为准）起 90 天内，承载 “软件” 的介质 （如果有）在正常使用的情况下不会出现材料和工艺方面的缺陷。除非这些 “软件” 由第三方提供。根据此有限担保，您的唯一补救以及 Sun 承担的全部责任是更换 “软件” 介质或退还您为 “软件” 支付的费用 （由 Sun 决定）。

4. 担保免责声明。除非本 “协议” 明文规定，否则 SUN 拒绝承担任何明示或暗示的条件、表示和担保，包括任何对适销性、特定用途的适用性或非侵犯性作出的暗示担保（除非这些免责声明在法律上无效）。

5. **责任限制。除非与法律相抵触，否则无论采用何种责任理论，SUN 或其许可发行者均不会对任何因使用 “软件”或因无法使用 “软件”而导致的收入减少、利润损失或数据丢失负责，也不会对特殊、间接、必然、偶然或惩罚性的损害负责，即使 SUN 已被告知可能出现此类损失。**根据本 “协议”，不论发生何种情况， Sun 对您的责任，无论是合同、侵权行为 （包括过失）还是其它方面的责任，均不会超过您购买 “软件”所支付的金额。即使在前面所述的担保丧失其基本意义的情况下，上述限制也同样适用。

6. 终止。本 “协议”始终有效，直到被终止。您随时可以通过销毁所有 “软件”副本来终止本 “协议”。如果您不遵守本 “协议”中的任何条款， Sun 将会立即终止本 “协议”而不会发送任何通知。一旦终止，您必须销毁所有 “软件”副本。

7. 出口法规。本 “协议”下的所有 “软件”和技术数据均遵守美国出口控制法律，并且还可能遵守其它国家/地区的出口或进口法规。您必须严格遵守所有此类法律和法规，并确认您有责任在 “软件”送达之后获得所有必要的出口、转口或进口许可。

8. 美国政府的限制权利。如果 “软件”由美国 政府或以美国政府的名义，或者由美国政府的总承包商或任何等级的分包商采购，则政府对 “软件”和随附文档的权利将仅限于本 “协议”中规定的权利；这符合 48 CFR 227.7201 至 227.7202-4 条款（适于国防部 (DOD) 采购）以及 48 CFR 2.101 和 12.212 条款 （适于非国防部门采购）。

9. 管辖法律。任何与本 “协议”有关的活动均必须遵守加利福尼亚州法律和美国联邦法，而不遵守任何地方管辖区的法律条例。

10. 可分割性。如果本 “协议”的任何条款无法实施，则可以忽略该条款，本 “协议”的其余部分仍然有效，除非忽略该条款会损坏当事双方的意向，在这种情况下，应立即终止本 “协议”。

11. 完整性。本 “协议”是您与 Sun 就相关事项签订的完整协议。它将取代所有以前或同期的口头或书面通信、建议、声明和担保文件；且对于当事双方在本 “协议”有效期内就相关事项签订的报价、订购、承诺或其它通信文件，它将取代这些文件之间相冲突的条款或附加条款。除非当事双方的法人代表书面签署，否则不能变更本 “协议”。

如有疑问，请联系 : Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054

(Form ID#011801)

Sun Microsystems, Inc.

Sun Crypto Accelerator 4000 的补充条款

这些 Sun Crypto Accelerator 4000 补充条款是对二进制代码许可协议 （“BCL”）的补充。此处未定义的术语 （带双引号）与 BCL 中的含义一致。这些补充条款将取代 BCL 中任何不一致或相冲突的条款。使用 “软件”意味着接受此处补充的 BCL。

1. 第三方许可条款。“软件”的某些部分附带了第三方的声明和/或许可，用于限制对这些部分的使用。

第三方许可条款

OPENSSL 许可问题

OpenSSL Toolkit 采用双重许可，即 OpenSSL 许可和原始 SSLeay 许可规定的条件均适用于 OpenSSL Toolkit。下面是许可原文。实际上，这两个许可都是 BSD 式开放源代码许可。对于任何与 OpenSSL 有关的许可问题，请联系：
openssl-core@openssl.org。

OpenSSL 许可

如果满足以下条件，则允许以源代码和二进制形式进行再分发和使用（无论修改与否）：

1. 源代码的再分发必须保留以上版权声明、本文所列条件以及下述免责声明。
2. 以二进制形式进行的再分发必须复制以上版权声明、本文所列条件以及分发时随附的文档和/或其它材料中的下述免责声明。
3. 所有涉及本软件功能或使用的广告资料都必须包含以下声明：“本产品包括由 OpenSSL Project 开发的用于 OpenSSL Toolkit 的软件 (http://www.openssl.org/)。”
4. 事先未经书面许可，不得将 “OpenSSL Toolkit”和 “OpenSSL Project”字样用于本软件衍生产品的担保和促销。要获得书面许可，请联系以下电子邮件地址：openssl-core@openssl.org。
5. 事先未经 OpenSSL Project 书面许可，不得将本软件衍生产品命名为 “OpenSSL”，而且产品名称中不得出现 “OpenSSL”字样。
6. 以任何形式进行的再分发都必须保留以下声明：“本产品包括由 OpenSSL Project 开发的用于 OpenSSL Toolkit (http://www.openssl.org/) 的软件。”

本软件由 OpenSSL PROJECT “按原样”提供。对于任何明示或暗示的担保，包括但不限于对适销性和适用性的暗示担保，OpenSSL PROJECT 概不负责。无论因何种方式导致，无论采用何种有关责任的理论，无论合同、无过失责任或侵权行为 （包括过失或其他）， OpenSSL PROJECT 或其开发人员均不对任何由于使用本软件而导致的直接、间接、特殊、偶发、惩罚性或连带损失负责 （包括但不限于替代商品或服务的采购；无法使用软件、数据丢失或利润损失；或业务中断）。即使已被告知可能出现此类损失，也不负责。

本产品包括由 Eric Young (eay@cryptsoft.com) 编写的加密软件。本产品包括由 Tim Hudson (tjh@cryptsoft.com) 编写的软件。

原始 SSLeay 许可

版权所有 (C) 1995-1998 Eric Young (eay@cryptsoft.com) 保留所有权利。

本软件包是由 Eric Young (eay@cryptsoft.com) 编写的 SSL 工具。本工具的编写符合 Netscapes SSL。

只要符合以下条件，本程序库可以免费用于商业和非商业用途。以下条件适用于本次分发中的所有代码，可以是 RC4、 RSA、 lhash、 DES 等代码；而不仅仅指 SSL 代码。本次分发随附的 SSL 文档遵守相同的版权条款，但版权持有人为 Tim Hudson (tjh@cryptsoft.com) 。

版权仍属 Eric Young 所有，因此不得删除代码中的版权声明。

如果某产品中使用本软件包，则应说明 Eric Young 是所用程序库部分的编写者。说明可以采用程序启动时显示文本消息的形式，也可以包含在软件包随附的文档 （联机或文本）中。

如果满足以下条件，则允许以源代码和二进制形式进行再分发和使用 （无论修改与否）：

1. 源代码的再分发必须保留此版权声明、本文所列条件以及下述免责声明。
2. 以二进制形式进行的再分发必须复制以上版权声明、本文所列条件以及分发时随附的文档和/或其它材料中的下述免责声明。
3. 所有涉及本软件功能或使用的广告材料都必须包含以下声明：“本产品包括由 Eric Young (eay@cryptsoft.com) 编写的加密软件。”如果从所用程序库获得的程序与加密无关，可以删除 “加密”字样 :-)。
4. 如果包含 apps 目录 （应用程序代码）中的任何 Windows 特定代码 （或其衍生形式），则必须包含以下声明：“本产品包括由 Tim Hudson (tjh@cryptsoft.com) 编写的软件”。

本软件由 ERIC YOUNG “按原样”提供。对于任何明示或暗示的担保，包括但不限于对适销性和适用性的暗示担保， ERIC YOUNG 概不负责。无论因何种方式导致，无论采用何种有关责任的理论，无论合同、无过失责任或侵权行为 （包括过失或其他），编写者或开发人员均不对任何由于使用本软件而导致的直接、间接、特殊、偶发、惩罚性或连带损失负责 （包括但不限于替代商品或服务的采购；无法使用、数据或利润损失；或业务中断）。即使已被告知可能出现此类损失，也不负责。

不得更改此代码的任何公开版本或衍生产品的许可和分发条款。换句话说，此代码不得被复制以及受另一分发许可的约束 [包括 GNU 公共许可。]

``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 许可

mod_ssl 软件包依据 BSD 式许可进行分发，因此属于开放源代码软件。详细许可信息如下。

版权所有 (c) 1998-2000 Ralf S. Engelschall。保留所有权利。

如果满足以下条件，则允许以源代码和二进制形式进行再分发和使用（无论修改与否）：

1. 源代码的再分发必须保留以上版权声明、本文所列条件以及下述免责声明。
2. 以二进制形式进行的再分发必须复制以上版权声明、本文所列条件以及分发时随附的文档和/或其它材料中的下述免责声明。
3. 所有提及本软件功能或使用的广告资料都必须包含以下声明：“本产品包括由 Ralf S. Engelschall <rse@engelschall.com> 开发的用于 mod_ssl 项目 (http://www.modssl.org/) 的软件。”
4. 事先未经书面许可，不得将 “mod_ssl”名称用于本软件衍生产品的担保和促销。要获得书面许可，请联系以下电子邮件地址：rse@engelschall.com。
5. 未经 Ralf S. Engelschall 事先书面许可，不得将本软件的衍生产品命名为 “mod_ssl”，而且产品名称中也不得出现 “mod_ssl”字样。
6. 以任何形式进行的再分发都必须保留以下声明：“本产品包括由 Ralf S. Engelschall <rse@engelschall.com> 开发的用于 mod_ssl 项目 (http://www.modssl.org/) 的软件。”

本软件由 RALF S. ENGELSCHALL “按原样”提供。对于任何明示或暗示的担保，包括但不限于对适销性和适用性的暗示担保， RALF S. ENGELSCHALL 概不负责。无论因何种方式导致，无论采用何种有关责任的理论，无论合同、无过失责任或侵权行为（包括过失或其他）， RALF S. ENGELSCHALL 或其开发人员均不对任何由于使用本软件而导致的直接、间接、特殊、偶发、惩罚性或连带损失负责 （包括但不限于替代商品或服务的采购；无法使用、数据或利润损失；或业务中断）。即使已被告知可能出现此类损失，也不负责。

附录 **F**

手册页

本附录介绍板软件中提供的 Sun Crypto Accelerator 4000 命令和实用程序，并列出了每个命令和实用程序的联机手册页。

可用以下命令来查看联机手册页：

```
man -M /opt/SUNWconn/man pagename
```

表 F-1 列出并说明了可用的联机手册页。

表 F-1 Sun Crypto Accelerator 4000 联机手册页

手册页	说明
vca(7d)	用于控制对基本硬件加密加速器进行访问的叶节点驱动程序
vcad(1m)	提供密钥库服务的守护程序
vcaadm(1m)	用于处理与板相关的配置、帐户和密钥数据库的实用程序
vcadiag(1m)	允许超级用户重置板、零置密钥资料并执行基本诊断操作的实用程序
kcl2(7d)	kcl2 是为加密硬件驱动程序提供支持的核心模块。
apsslcfg(1m)	Apache Web Server 的配置实用程序
iplsslcfg(1m)	Sun ONE Web Server 的配置实用程序
pk11export(1m)	使用 PKCS#11 界面的密钥导出实用程序

附录 G

零置硬件

本附录介绍如何零置 Sun Crypto Accelerator 4000 板硬件，以将板还原为出厂状态。板还原为出厂状态时，处于 Failsafe 模式。

注意 – 仅在绝对必要时，才可执行硬件零置过程。如果仅需清除所有密钥资料，请使用 `vcaadm` 程序中的 `zeroize` 命令执行软件零置。有关 `zeroize` 命令的详情，请参阅第 74 页 “在板上执行软件零置”。另请参阅 `vcadiag` (4) 联机手册页，了解有关清除所有密钥资料的说明。

注 – 对板执行硬件零置会删除 Sun Crypto Accelerator 4000 固件。您必须重新安装 Sun Crypto Accelerator 4000 软件附带的固件。

将 Sun Crypto Accelerator 4000 硬件零置为原始出厂状态

某些情况下，可能需要将板还原为 `failsafe` 模式，并清除板的所有密钥资料和配置信息。只能使用标准 SCSI 硬件跳线 （并联）才能完成此项操作。

注 – 您可使用 `vcaadm` 程序中的 `zeroize` 命令来清除 Sun Crypto Accelerator 4000 板的所有密钥资料。不过，`zeroize` 命令会保持任何更新的固件完好无损。有关说明，请参阅第 74 页 “在板上执行软件零置”。另请参阅 `vcadiag`(4) 联机手册页。

▼ 使用硬件跳线零置 Sun Crypto Accelerator 4000 板

1. **关闭系统电源。**

注 – 对于某些系统，您可以根据需要在本过程中使用动态重配置功能 (DR) 来拆卸和装回板，而无需关闭系统电源。有关 DR 的正确过程，请参阅系统随附的文档。

注意 – 调节跳线时，此板不得接通任何电源。

---

2. **卸下计算机外壳，以便调节板中上部的跳线。**

3. **将跳线插在跳线块的插针 1 和 2 上。**

   插针 1 和 2 是距离支架最近的插针。共有四组插针 （每组两个）。将跳线插在插针 1 和 2 上，如图 G-1 中所示。

注意 – 跳线插在插针 1 和 2 上时，板不工作。

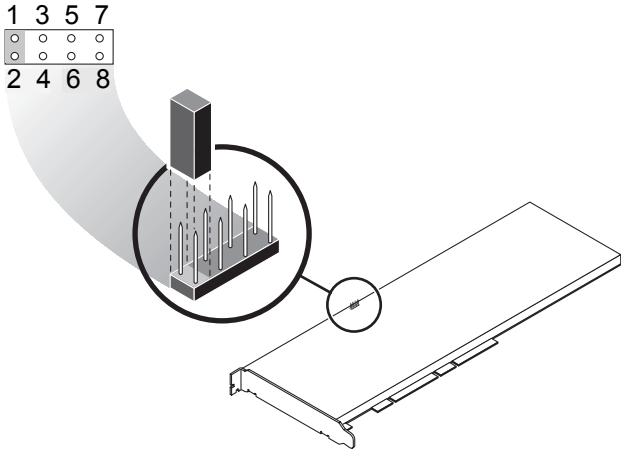

图 G-1 硬件跳线块插针

4. **打开系统电源。**

注意 – 在调整硬件跳线后打开系统电源时，将会删除所有固件、密钥资料及配置信息。本过程将板还原为原始出厂状态，并且将它置于 Failsafe 模式。

---

5. **关闭系统电源。**

6. **从跳线块的插针 1 和 2 上取下跳线，并放回原来的位置。**

7. **打开系统电源。**

8. **通过 `vcaadm` 连接到 Sun Crypto Accelerator 4000 板。**

   `vcaadm` 会提示您输入升级固件的路径。

9. **键入 `/opt/SUNWconn/cryptov2/firmware/sca4000fw` 作为安装固件的路径。**

   固件会自动安装，且 `vcaadm` 退出。

10. **通过 `vcaadm` 重新连接到 Sun Crypto Accelerator 4000 板。**

    `vcaadm` 会提示您初始化板以使用新的密钥库，或者初始化板以使用现有的密钥库。有关说明，请参阅第 62 页 “通过 `vcaadm` 初始化板”。

索引

A

B

C

D

F

G

H

J

K

L

M

P

Y

Z