Sun™ Crypto Accelerator 4000 보드 버전 1.1 설치 및 사용 설명서

Sun Microsystems, Inc.
www.sun.com

부품 번호: 817-5926-10
2004년 1월, 개정판 A

본 설명서에 대한 의견은 http://www.sun.com/hwdocs/feedback으로 보내주십시오.

재활용 가능

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。

목차

표

머리말

본 *Sun Crypto Accelerator 4000 보드 버전 1.1 설치 및 사용 설명서*에는 Sun Crypto Accelerator 4000 보드의 기능, 프로토콜 및 인터페이스에 대한 설명 및 보드를 시스템에 설치하고, 구성하고, 관리하는 방법이 나와 있습니다.

본 설명서는 Solaris 운영 환경, PCI I/O 카드가 내장된 Sun 플랫폼, Sun ONE 및 Apache Web Server, IPsec, SunVTS™ 소프트웨어, 인증 기관(CA) 획득 중 하나 이상에 대한 구성 경험이 있는 네트워크 관리자를 대상으로 합니다.

본 설명서의 구성

본 설명서는 다음과 같이 구성되어 있습니다.

- 1장은 Sun Crypto Accelerator 4000 보드의 제품 기능, 프로토콜, 인터페이스와 함께 하드웨어 및 소프트웨어 요구 사항을 설명합니다.
- 2장은 Sun Crypto Accelerator 4000의 하드웨어 및 소프트웨어 설치 및 제거 방법을 설명합니다.
- 3장은 Sun Crypto Accelerator 4000에서 설정 가능한 드라이버 매개 변수에 대한 정의와 `ndd` 유틸리티와 `vca.conf` 파일을 통해 이 매개 변수를 구성하는 방법을 설명합니다. 또한 OpenBoot™ PROM 인터페이스에서 자동 교섭 또는 강제 모드를 활성화하는 방법과 네트워크 `hosts` 파일 구성 방법을 설명합니다.
- 4장은 `vcaadm` 및 `vcadiag` 유틸리티를 통한 Sun Crypto Accelerator 4000 보드 구성과 키스토어 관리 방법을 설명합니다.
- 5장은 Sun ONE Web Server와 함께 사용하기 위한 Sun Crypto Accelerator 4000 보드 구성 방법을 설명합니다.
- 6장은 Apache Web Server와 함께 사용하기 위한 Sun Crypto Accelerator 4000 보드 구성 방법을 설명합니다.

- 7장은 SunVTS 진단 응용 프로그램 및 보드 상의 FCode 자가 테스트를 통한 Sun Crypto Accelerator 4000 보드 테스트 방법을 설명합니다. 또한 OpenBoot PROM 명령을 사용한 문제 해결 기법도 설명합니다.
- 8장은 PKCS#11 인터페이스에서의 여러 가지 보드 구성의 작동 방식을 설명합니다.
- 부록 A에는 Sun Crypto Accelerator 4000 보드의 사양이 나와 있습니다.
- 부록 B는 Sun Crypto Accelerator 4000 소프트웨어를 설치 스크립트 없이 수동으로 설치하는 방법을 설명합니다.
- 부록 C는 Sun Crypto Accelerator 4000 소프트웨어를 사용하여 Apache Web Server에 대한 SSL 지원을 구성하는 데 필요한 지시어를 설명합니다.
- 부록 D는 Sun Crypto Accelerator 4000 보드와 함께 제공되는 소프트웨어와 이 보드의 암호화 가속 기능을 활용하여 OpenSSL 호환 응용 프로그램을 구축하는 방법을 설명합니다.
- 부록 E에는 Sun Crypto Accelerator 4000 보드와 함께 사용되는 기타 소프트웨어의 사용에 대한 해당 소프트웨어 제작사의 공지 사항 및 라이센스 조항이 나와 있습니다.
- 부록 F에는 Sun Crypto Accelerator 4000 명령 설명과 각 명령에 대한 온라인 매뉴얼 페이지가 나와 있습니다.
- 부록 G는 Sun Crypto Accelerator 4000 보드를 보드의 failsafe 모드인 출하 시 상태로 초기화하는 방법을 설명합니다.

UNIX 명령 사용

이 설명서에는 시스템 종료, 시스템 부팅 및 장치 구성과 같은 기본 UNIX® 명령어 및 절차에 대한 정보는 나와 있지 않습니다.

이러한 정보는 다음을 참조하십시오.

- *Solaris 하드웨어 플랫폼 안내서*
- 다음 사이트에 있는 Solaris 운영 환경에 대한 온라인 설명서:
  `http://docs.sun.com`
- 시스템과 함께 제공된 기타 소프트웨어 설명서

쉘 프롬프트

쉘	프롬프트
C 쉘	*machine-name*%
C 쉘 수퍼유저	*machine-name*#
Bourne 쉘 및 Korn 쉘	$
Bourne 쉘 및 Korn 쉘 수퍼유저	#

활자체 규약

활자체	의미	예제
AaBbCc123	명령어, 파일 및 디렉토리의 이름과 컴퓨터 화면 상의 출력 내용	.login 파일을 편집하십시오. 모든 파일을 나열하려면 ls -a를 사용하십시오. % You have mail.
AaBbCc123	컴퓨터 화면 상의 출력 내용과 대조되는 사용자가 입력한 내용	% **su** Password:
AaBbCc123	문서 제목, 새로운 단어나 용어, 강조하는 단어	*사용 설명서*의 6장을 읽으십시오. 이들을 *클래스* 옵션이라고 합니다. 이 작업을 수행하려면 *반드시* 수퍼유저이어야 합니다.
	실제 이름이나 값으로 대체되는 명령행 변수	파일을 삭제하려면 rm *파일 이름*을 입력하십시오.

Sun 설명서 온라인 액세스

다음을 통해서 한글화된 버전을 비롯하여 Sun에서 제공하는 다양한 설명서를 보거나 인쇄 또는 구입할 수 있습니다.

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

Sun 기술 지원 문의

본 제품과 관련하여 설명서에 나와 있지 않은 기술적 의문 사항은 다음을 참조하십시오.

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

고객 의견

Sun은 설명서의 개선을 위해 항상 노력하고 있으며, 고객의 의견 및 제안을 언제나 환영합니다. 의견이 있으시면 다음 주소로 전자 메일을 보내 주십시오.

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

보내실 때는 다음과 같이 해당 설명서의 제목과 부품 번호를 표기해 주십시오.

Sun Crypto Accelerator 4000 보드 버전 1.1 설치 및 사용 설명서,
부품 번호: 817-5926-10

1 장

제품 개요

이 장에서는 Sun Crypto Accelerator 4000 보드의 개요를 설명하며 다음 항목으로 구성되어 있습니다.

제품 기능

Sun Crypto Accelerator 4000 보드는 Sun 서버에서 IPsec 및 SSL(대칭 및 비대칭 모두)에 대한 암호화 하드웨어 가속을 지원하는 기가비트 이더넷 기반의 네트워크 인터페이스 카드입니다. 암호화되지 않은 네트워크 트래픽을 위한 표준 기가비트 이더넷 네트워크 인터페이스로 운영될 뿐만 아니라, 보드에는 표준 소프트웨어 솔루션보다 더 많은 암호화된 IPsec 트래픽 처리량을 지원하는 암호화 하드웨어가 내장되어 있습니다.

보드를 설치하면 키스토어 및 사용자 정보를 관리하고 보드의 보안 레벨을 결정하는 `vcaadm` 유틸리티를 통해 초기화 및 구성됩니다. 키스토어 및 보안 관리자 계정을 구성하고 나면 `iplsslcfg` 및 `apsslcfg` 스크립트를 사용해 보드를 SSL 가속화에 사용하도록 Sun ONE Web Server 및 Application Server 또는 Apache Web Server를 구성할 수 있습니다. Sun ONE Directory, Messaging 및 Portal Server는 Sun ONE 관리 콘솔과 `modutil` 및 `certutil` 유틸리티를 사용해 보드를 SSL 가속화에 사용하도록 구성할 수도 있습니다. 또한 키스토어 및 암호화 서비스에 PKCS#11 인터페이스가 필요한 대부분의 응용 프로그램에서도 보드를 사용할 수 있습니다.

주요 프로토콜 및 인터페이스

Sun Crypto Accelerator 4000 보드는 표준 이더넷 최소/최대 프레임 크기(64~1,518바이트), 프레임 형식 및 다음의 표준과 프로토콜에 준수한다고 가정할 경우 기존의 이더넷 장비와 함께 운용할 수 있습니다.

- 전체 크기의 PCI 33/66Mhz, 32/64비트
- IEEE 802.3 CSMA/CD(이더넷)
- IEEE 802.2 논리적 연결 제어
- SNMP(국한된 MIB)
- 이중 및 반이중 기가비트 이더넷 인터페이스(IEEE 802.z)
- 일반 배전압 신호 방식(3.3V 및 5V)

주요 특징

- 구리 또는 파이버 인터페이스를 사용하는 기가비트 이더넷
- IPsec 및 SSL 암호화 기능 가속화
- 세션 설정 속도: 초당 최대 4,300회의 연산
- 대량 암호화율: 최대 800Mbps
- 최대 2,048비트 RSA 암호화 제공
- 최대 10배 빠른 3DES 대량 데이터 암호화 속도
- 보안 강화 및 키 관리 편의성을 위해 부정 조작 방지용 집중 보안 키와 Sun ONE Web Server용 인증서 관리
- FIPS 140-2 Level 3 인증서에 맞게 설계
- 낮은 CPU 사용률 — 서버 시스템 리소스 및 대역폭에 제약이 없음
- 보안 개인 키 저장 및 관리
- Sun의 미드프레임 및 하이 엔드 서버에서 동적 재구성(DR) 및 중복성/장애 조치를 지원
- 여러 CPU 간의 RX 패킷 부하 조절
- 완벽한 흐름 제어 지원(IEEE 802.3x)

Sun Crypto Accelerator 4000 보드는 FIPS(Federal Information Processing Standard) 140-2, Level 3에 규정된 암호화 모듈의 보안 요구 사항을 준수하도록 설계되었습니다.

지원되는 응용 프로그램

- Solaris 8 및 9 운영 환경(IPsec VPN)
- Sun ONE Web Server 4.1 및 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 및 2.x

지원되는 암호화 프로토콜

이 보드는 다음 프로토콜을 지원합니다.

- IPv4 및 IPv6용 IPsec(IKE 포함)
- SSLv2, SSLv3, TLSv1(전송층 보안)

이 보드는 다음 IPsec 기능을 가속화합니다.

- ESP(DES, 3DES) 암호화
- ESP(SHA1, MD5) 인증 *
- AH(SHA1, MD5) 인증 *

* 인라인 IPsec 가속화 용도로 구성하는 경우(5페이지의 "인라인 IPsec 하드웨어 가속화" 참조)

이 보드는 다음 SSL 기능을 가속화합니다.

- 클라이언트와 서버 간의 암호화 매개 변수 및 비밀 키 세트 보안 설정
- 보드에 보안 키 저장 — 보드를 벗어날 경우 키는 암호화됨

진단 지원

- OpenBoot PROM을 통한 사용자 실행 가능한 자가 테스트
- SunVTS 진단 테스트

암호화 알고리즘 가속화

이 보드는 하드웨어 및 소프트웨어 모두에서 암호화 알고리즘을 가속화합니다. 이와 같이 복잡한 이유는 암호화 알고리즘을 가속화하는 데 드는 비용이 모든 알고리즘에 대해 동일하지 않기 때문입니다. 일부 암호화 알고리즘은 하드웨어에서 구현되도록 특별히 설계된 반면 또다른 알고리즘은 소프트웨어에서 구현되도록 설계되었습니다. 하드웨어 가속화의 경우, 사용자 응용 프로그램에서 하드웨어 가속화 장치로 데이터를 이동하고 해당 결과를 다시 사용자 응용 프로그램으로 이동하는 데 추가 비용이 듭니다. 일부 암호화 알고리즘의 경우, 고도로 조정된 소프트웨어를 사용하면 전용 하드웨어의 수행 속도와 유사한 속도로 수행될 수 있습니다.

지원되는 암호화 알고리즘

Sun Crypto Accelerator 4000 드라이버(vca)는 각각의 암호화 요청을 검사하고 최대 처리량을 얻기 위해 가속화(호스트 프로세서 또는 Sun Crypto Accelerator 4000)를 위한 최적의 위치를 결정합니다. 부하 분산은 암호화 알고리즘, 현재 작업 부하 및 데이터 크기를 기반으로 이루어집니다.

이 보드는 다음 IPsec 알고리즘을 가속화합니다.

표 1-1 IPsec 암호화 알고리즘

유형	알고리즘
대칭형	DES, 3DES
해시*	MD5, SHA1

* 인라인 IPsec 가속화 용도로 구성하는 경우

이 보드는 다음 SSL 알고리즘을 가속화합니다.

표 1-2 SSL 암호화 알고리즘

유형	알고리즘
대칭형	DES, 3DES, ARCFOUR
비대칭형	Diffie-Hellman(Apache 전용) 및 RSA(최대 2,048비트 키), DSA
해시	MD5, SHA1

IPsec 가속화

이 보드는 대역 외(out-of-band) 및 인라인(in-line)의 두 IPsec 가속화 형식을 지원합니다. 이러한 두 구성을 통해 부하가 높은 암호화 작업을 SPARC® 프로세서에서 보드로 덜어낼 수 있습니다. 52페이지의 "IPsec 하드웨어 가속화 구성"을 참조하십시오.

표 1-3 가속화되는 IPsec 알고리즘

알고리즘	대역 외	인라인
DES	X	X
3DES	X	X
MD5		X
SHA1		X

대역 외 IPsec 하드웨어 가속화

보드를 대역 외 IPsec 가속화 용도로 구성하면 Solaris 9(또는 이상) 시스템에 설치된 하드웨어에서 지원되는 암호화 및 암호 해독 작업이 가속화됩니다. 모든 IPsec의 특정 패킷 처리는 호스트 Solaris IPsec 소프트웨어에서 수행됩니다. 53페이지의 "대역 외 IPsec 가속화 활성화"를 참조하십시오.

참고 – Solaris 9에서 대역 외 IPsec가속화를 위해 보드를 사용할 경우 IPsec 설정이나 튜닝이 필요하지 않습니다. Sun Crypto Accelerator 4000 패키지를 설치하고 재부팅하기만 하면 됩니다.

인라인 IPsec 하드웨어 가속화

보드를 인라인 IPsec 가속화 용도로 구성하면 Solaris 8 12/03(또는 이상) 시스템에 설치된 하드웨어에서 지원되는 암호화, 암호 해독 및 인증 작업이 가속화됩니다. IPsec 특정 패킷 처리의 일부가 보드에서 바로 수행됩니다. 인라인 IPsec 가속화를 위한 보드 구성 방법에 대한 지침은 53페이지의 "인라인 IPsec 가속화 활성화"를 참조하십시오.

SSL 가속화

표 1-4는 하드웨어로 이동 가능한 SSL 가속 알고리즘과 Sun ONE 및 Apache Web Server에 제공되는 소프트웨어 알고리즘을 나타냅니다.

표 1-4 지원되는 SSL 알고리즘

	Sun ONE Web Server		Apache Web Server	
알고리즘	**하드웨어**	**소프트웨어**	**하드웨어**	**소프트웨어**
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		

대량 암호화

Sun ONE 서버 소프트웨어를 위한 Sun Crypto Accelerator 4000 대량 암호화 기능은 기본적으로 비활성화되어 있습니다. 파일을 생성하고 Sun ONE 서버 소프트웨어를 재시작하여 이 기능을 수동으로 활성화해야 합니다.

보드에서 Sun ONE 서버 소프트웨어가 대량 암호화 기능을 사용할 수 있도록 하려면 `/etc/opt/SUNWconn/cryptov2/` 디렉토리에 `sslreg`이란 이름의 빈 파일을 생성한 후 서버 소프트웨어를 재시작합니다.

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

대량 암호화 기능을 비활성화하려면 `sslreg` 파일을 삭제한 후 서버 소프트웨어를 다시 시작해야 합니다.

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

Apache Web Server 소프트웨어의 대량 암호화 기능은 기본적으로 활성화되어 있으며 비활성화할 수 없습니다.

하드웨어 개요

Sun Crypto Accelerator 4000 하드웨어는 Sun 서버에서 IPsec 및 SSL의 성능을 향상시키는 전체 크기(10.67 × 31.198cm)의 암호화 가속기 PCI 기가비트 이더넷 어댑터입니다.

Sun Crypto Accelerator 4000 MMF 어댑터

Sun Crypto Accelerator 4000 MMF 어댑터는 단일 포트 기가비트 이더넷 광섬유 PCI 버스 카드입니다. 1,000Mbps 이더넷 네트워크에서만 운용됩니다.

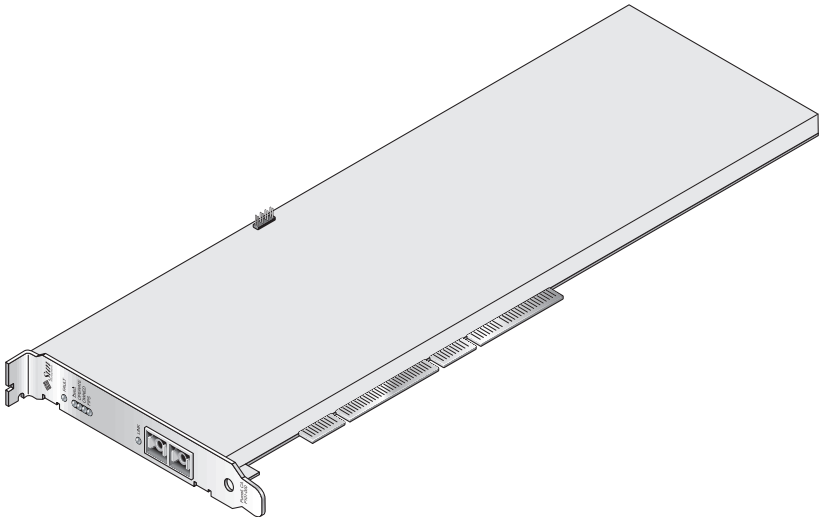

그림 1-1 Sun Crypto Accelerator 4000 MMF 어댑터

LED 디스플레이

표 1-5 MMF 어댑터의 전면 패널 디스플레이 LED

레이블	점등 조건	색상
FAULT	보드가 중단(치명적인 오류) 상태이거나 하위 수준 하드웨어 초기화에 실패한 경우 켜짐 부팅 중 오류가 발생하면 깜빡거림	적색
DIAG	POST, 진단, 장애 시 안전(업그레이드 안된 펌웨어) 상태에서 켜짐. 진단 실행 중 깜빡림	녹색
OPERATE	POST, 진단, 사용 불가(드라이버 없음) 상태에서 켜짐. 유휴, 작동, 장애 시 안전 상태에서 깜빡거림	녹색
INIT	보안 담당자가 `vcaadm`으로 보드를 초기화한 경우 켜짐. 64페이지의 "vcaadm을 통해 보드 초기화"를 참조하십시오. ZEROIZE 점퍼 존재 시 깜빡거림	녹색
FIPS	FIPS 140-2 level 3 인증 모드에서 작동 시 켜짐. FIPS 모드가 아닌 경우 꺼짐	녹색
LINK	연결되어 있을 때 켜짐	녹색

Sun Crypto Accelerator 4000 UTP 어댑터

Sun Crypto Accelerator 4000 UTP 어댑터는 단일 포트 기가비트 이더넷 구리 기반 PCI 버스입니다. 10, 100 및 1,000Mbps 이더넷 네트워크에서 작동하도록 설정할 수 있습니다.

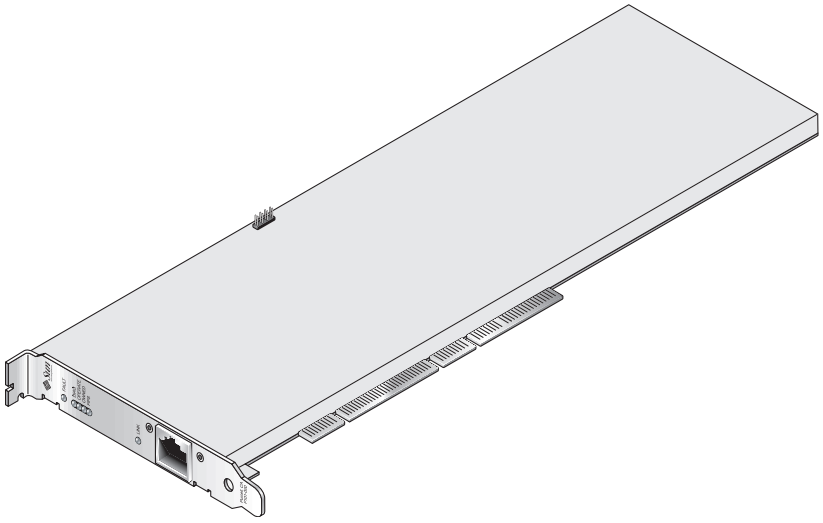

그림 1-2 Sun Crypto Accelerator 4000 UTP 어댑터

LED 디스플레이

표 1-6 UTP 어댑터용 전면 패널 디스플레이 LED

레이블	점등 조건	색상
FAULT	보드가 중단(치명적인 오류) 상태이거나 하위 수준 하드웨어 초기화에 실패한 경우 켜짐 부팅 중 오류가 발생하면 깜빡거림	적색
DIAG	POST, 진단, 장애 시 안전(업그레이드 안된 펌웨어) 상태에서 켜짐. 진단 실행 중 깜빡임	녹색
OPERATE	POST, 진단, 사용 불가(드라이버 없음) 상태에서 켜짐. 유휴, 작동, 장애 시 안전 상태에서 깜빡거림	녹색
INIT	보안 담당자가 `vcaadm`으로 보드를 초기화한 경우 켜짐. 64페이지의 "`vcaadm`을 통해 보드 초기화"를 참조하십시오. ZEROIZE 점퍼 존재 시 깜빡거림	녹색

표 1-6 UTP 어댑터용 전면 패널 디스플레이 LED*(계속)*

레이블	점등 조건	색상
FIPS	FIPS 140-2 level 3 인증 모드에서 작동 시 켜짐. FIPS 모드가 아닌 경우 꺼짐	녹색
1000	기가비트 이더넷 사용 시 켜짐	녹색
ACTIVITY(레이블 없음)	연결을 통해 전송 또는 수신 중일 때 켜짐	황색
LINK(레이블 없음)	연결되어 있을 때 켜짐	녹색

참고 – 서비스 팩 번호(SP9 또는 SP1)는 iPlanet 웹 서버 4.1 또는 6.0이 언급될 경우 항상 포함됩니다.

동적 재구성 및 고가용성

Sun Crypto Accelerator 4000 하드웨어 및 관련 소프트웨어는 동적 재구성(DR)과 핫 플러깅을 지원하며 Sun 플랫폼에서 효과적으로 작동합니다. DR 또는 핫 플러그 작동 중에 Sun Crypto Accelerator 4000 소프트웨어 계층은 자동으로 보드의 추가나 제거를 감지하고 일정 알고리즘을 조정하여 하드웨어 리소스의 변경 사항을 수용합니다.

고가용성(HA) 구성을 수행하려면, 시스템 또는 도메인에 여러 개의 Sun Crypto Accelerator 4000 보드를 설치하여 하드웨어 가속을 계속적으로 사용할 수 있습니다. Sun Crypto Accelerator 4000 하드웨어 장애가 발생할 경우, 소프트웨어 계층은 장애를 감지하고 사용 가능한 하드웨어 암호화 가속기 목록에서 이를 제거합니다. Sun Crypto Accelerator 4000 소프트웨어는 하드웨어 장애로 인한 리소스 감소를 일정 알고리즘을 조정하여 보완합니다. 그 이후의 암호와 요청은 나머지 보드로 넘어갑니다.

Sun Crypto Accelerator 4000 하드웨어는 장기 키 생성을 위한 고품질의 엔트로피 소스를 제공합니다. 도메인이나 시스템 내의 모든 Sun Crypto Accelerator 4000 보드가 제거된 경우 장기 키는 저품질 엔트로피로 생성됩니다.

부하 공유

Sun Crypto Accelerator 4000 소프트웨어는 Solaris 도메인 또는 시스템 내에 설치된 모든 보드로 부하를 분산시킵니다. 수신되는 암호화 요청은 정해진 길이의 작업 대기열에 기초하여 모든 보드에 걸쳐 분산됩니다. 암호화 요청은 첫 번째 보드로 전달되고, 해당 보드가 최대 용량으로 실행될 때까지 요청이 계속 전달됩니다. 첫 번째 보드가 최대 용량으로 실행되기 시작하면 추가 요청은 해당 유형의 요청을 수용 가능한 다음 보드의 대기열로 전달됩니다. 대기 메커니즘은 보드에서 요청의 결합을 통해 최적화하도록 설계되었습니다.

하드웨어 및 소프트웨어 요구 사항

표 1-7에는 Sun Crypto Accelerator 4000 어댑터에 대한 하드웨어 및 소프트웨어 요구 사항이 나와 있습니다.

표 1-7 하드웨어 및 소프트웨어 요구 사항

하드웨어 및 소프트웨어	요구 사항
하드웨어	Sun Fire™ V120, V210, V240, 280R, V480, V880, 4800, 4810, 6800, 12K, 15K; Netra™ 20 (lw4); Sun Blade™ 100, 150, 1000, 2000
운영 환경	Solaris 8 2/02 및 이후 호환 가능한 릴리스(IPsec 가속화에는 Solaris 9는 필수)

필수 패치

필수 패치에 대한 자세한 내용은 *Sun Crypto Accelerator 4000 보드 버전 1.1 릴리스 노트*를 참조하십시오.

다음은 시스템에서 Sun Crypto Accelerator 4000 보드를 실행하기 위해 필요한 패치입니다. Solaris 업데이트에 이전 릴리스에 대한 패치가 포함되어 있습니다. `showrev -p` 명령을 사용하여 나열된 패치가 설치되어 있는지 확인합니다.

다음 웹 사이트에서 다운로드할 수 있습니다.
`http://sunsolve.sun.com`

패치의 최신 버전을 설치합니다. 대시 번호(예: -01)는 패치의 새 버전이 나올 때마다 증가됩니다. 웹 사이트에 있는 버전이 아래 표에 표시되어 있는 버전보다 높으면 최신 버전이 됩니다.

필요한 패치가 SunSolve℠ 웹 사이트에 없는 경우에는 가까운 영업 센터 또는 서비스 담당자에게 문의하십시오.

Apache Web Server 패치

Apache Web Server와 Solaris 8을 함께 사용하려면 109234-09 패치를 설치한 후에 Sun Crypto Accelerator 4000 소프트웨어를 설치해야 합니다. `SUNWkcl2a` 패키지가 추가되면 시스템은 Apache Web Server mod_ssl 1.3.26로 구성됩니다.

Solaris 8 패치

표 1-8은 Sun Crypto Accelerator 4000 소프트웨어에 필요한 필수 Solaris 8 패치 목록입니다.

표 1-8 필수 Solaris 8 패치

패치 ID	설명
110383-01	`libnvpair`
108528-23	`KU-05`(`nvpair` 지원)
112438-01	`/dev/random`
110900-10	`pcifg`, SunFire 15K 지원 및 DR
110824-04	DR
110842-11	버스 속도 및 DR
110839-04	마이너 노드 및 DLPI 프로바이더 이름
109234-09	Apache 지원

Solaris 9 패치

표 1-9는 Sun Crypto Accelerator 4000 소프트웨어에 필요한 필수 Solaris 9 패치 목록입니다.

표 1-9 필수 Solaris 9 패치

패치 ID	설명
113068-04	버스 속도, Sun Fire 15K 지원 및 DR
112838-08	`pcicfg`, DR 및 Sun Fire 15K 지원
113218-08	기가비트 성능 및 `vca` 메모리 손실
112904-08	기가비트 성능
114758-01	마이너 노드 및 DLPI 프로바이더 이름
112233-08	(Solaris 9 9/04 이전의 Solaris 릴리스에만 필요함)

2 장

Sun Crypto Accelerator 4000 보드 설치

이 장에서는 Sun Crypto Accelerator 4000 하드웨어의 설치 방법과 자동 스크립트를 사용한 소프트웨어의 설치 및 제거 방법에 대해 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

보드의 하드웨어와 소프트웨어가 설치되면 구성 및 키스토어 정보로 보드를 초기화해야 합니다. 보드 초기화 방법에 대한 내용은 64페이지의 "vcaadm을 통해 보드 초기화"를 참조하십시오.

보드 사용법

각 보드는 특수 정전기 방지용 봉지에 포장되어 운반 또는 보관 기간 동안 보호됩니다. 보드에 내장된 정전기에 민감한 부품의 손상을 방지하려면 보드를 만지기 전에 다음 방법 중 한 가지를 사용하여 신체의 정전기를 감소시키십시오.

- 컴퓨터의 금속 프레임에 접촉합니다.
- 정전기 방지용 손목 띠를 손목 및 접지된 금속 표면에 부착합니다.

주의 – 보드에 내장된 민감한 부품의 손상을 방지하려면 보드를 다룰 때는 정전기 방지용 손목 띠를 착용하고, 보드를 들 때는 가장자리를 사용하며, 포장에 사용된 플라스틱 봉지와 같이 항상 정전기가 없는 장소에 놓아야 합니다.

보드 설치

Sun Crypto Accelerator 4000 보드 설치에는 시스템에 보드를 삽입하고 소프트웨어 도구를 로드하는 작업이 포함됩니다. 하드웨어 설치 지침에는 보드 설치에 대한 일반적인 단계만 포함됩니다. 특정 설치 지침에 대해서는 시스템과 함께 제공된 설명서를 참조하십시오.

▼ 하드웨어 설치

1. **수퍼유저로 로그인하고 시스템과 함께 제공된 지침에 따라 컴퓨터를 종료하고 전원을 끈 다음, 전원 코드를 분리하고 컴퓨터 덮개를 제거합니다.**
2. **사용하지 않은 PCI 슬롯(64비트, 66MHz 슬롯 권장)을 찾아봅니다.**
3. **정전기 방지용 손목 띠를 손목 및 접지된 금속 표면 끝에 부착합니다.**
4. **Phillips 헤드 나사 드라이버를 사용하여 PCI 슬롯 덮개에서 나사를 제거합니다.**

   5단계에서 브래킷을 고정할 수 있도록 나사를 보관합니다.
5. **Sun Crypto Accelerator 4000 보드의 가장자리를 잡고 비닐 봉지에서 꺼낸 다음 PCI 슬롯에 삽입하고 후면 브래킷의 나사를 고정시킵니다.**
6. **컴퓨터 덮개를 씌운 다음 전원 코드를 다시 연결하고 시스템 전원을 켭니다.**
7. **OpenBoot PROM** `ok` **프롬프트에서** `show-devs` **명령을 입력하여 보드가 올바르게 설치되었는지 확인합니다.**

```
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
.
```

위 예제에서 `/pci@8,600000/network@1`은 Sun Crypto Accelerator 4000 보드에 대한 장치 경로를 확인합니다. 시스템의 각 보드에 대해 이런 행이 하나씩 있습니다.

Sun Crypto Accelerator 4000 장치 속성이 올바르게 나열되는지 확인하려면 ok 프롬프트에서 장치 경로까지 이동한 후 .properties를 입력하여 속성 목록을 확인합니다.

```
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 04-03-03
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
```

Sun Crypto Accelerator 4000 소프트웨어 설치

Sun Crypto Accelerator 4000 소프트웨어는 Sun Crypto Accelerator 4000 CD에 포함되어 있습니다. SunSolve 웹 사이트에서 패치를 다운로드해야 할 경우도 있습니다. 자세한 내용은 10페이지의 "필수 패치"를 참조하십시오.

소프트웨어 설치는 수동 또는 `install` 스크립트를 사용하는 두 가지 방법이 있습니다. 이 항목에서는 `install` 스크립트로 소프트웨어를 설치하는 방법을 설명합니다. 소프트웨어를 수동으로 설치하려면 부록 B를 참조하십시오.

▼ 소프트웨어 설치

1. **시스템에 연결된 CD-ROM 드라이브에 Sun Crypto Accelerator 4000 CD를 넣습니다.**
   - 시스템이 Sun Enterprise Volume Manager™를 실행 중인 경우 CD-ROM이 `/cdrom/cdrom0` 디렉토리에 자동으로 마운트됩니다.
   - 시스템에 Sun Enterprise Volume Manager가 실행 중이 아닌 경우 다음을 입력하여 CD-ROM을 마운트합니다.

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

/cdrom/cdrom0 디렉토리에 다음 파일과 디렉토리가 표시됩니다.

표 2-1 /cdrom/cdrom0 디렉토리의 파일

파일 또는 디렉토리	내용	
Copyright	미국저작권 파일	
FR_Copyright	프랑스 저작권 파일	
install	Sun Crypto Accelerator 4000 소프트웨어 설치 스크립트	
remove	Sun Crypto Accelerator 4000 소프트웨어 제거 스크립트	
Docs	*Sun Crypto Accelerator 4000 보드 버전 1.1 설치 및 사용 설명서* *Sun Crypto Accelerator 4000 보드 릴리스 노트*	
Packages	다음 Sun Crypto Accelerator 4000 소프트웨어 패키지가 포함되어 있습니다.	
	SUNWkcl2r	암호화 커널 구성 요소
	SUNWkcl2u	암호화 관리 유틸리티 및 라이브러리
	SUNWkcl2a	Apache용 SSL 지원*(옵션)*
	SUNWkcl2m	암호화 관리 매뉴얼 페이지*(옵션)*
	SUNWvcar	VCA Crypto Accelerator(루트)
	SUNWvcau	VCA Crypto Accelerator(Usr)
	SUNWvcaa	VCA 관리
	SUNWvcafw	VCA 펌웨어
	SUNWvcamn	VCA Crypto Accelerator 매뉴얼 페이지*(옵션)*
	SUNWvcav	VCA Crypto Accelerator의 SunVTS 테스트*(옵션)*
	SUNWkcl2o	SSL 개발 도구 및 라이브러리*(옵션)*
	SUNWkcl2i.u	KCLv2 Crypto를 통한 IPsec 가속화*(옵션)*

이 설치 스크립트는 일정 순서에 따라 필수 패키지를 설치하며, 이러한 패키지를 설치한 후에 옵션 패키지를 설치해야 합니다. 필수 패키지가 설치되면 순서에 상관없이 옵션 패키지를 설치하고 제거할 수 있습니다.

옵션 SUNWkcl2a 패키지는 Apache를 웹 서버로 사용하려는 경우에만 설치합니다.

옵션 SUNWkcl2o 패키지는 Apache Web Server의 다른 버전으로 다시 연결하려는 경우에만 설치합니다.

옵션 SUNWvcav 패키지는 SunVTS 테스트를 수행하려는 경우에만 설치합니다. SUNWvcav 패키지를 설치하려면 SunVTS 4.4 이상에서 5.x까지의 버전이 설치되어 있어야 합니다.

참고 – 옵션 SUNWkcl2i.u 패키지는 Sun Crypto Accelerator 4000CD 상에서만 .u 확장자를 가지고 있습니다. 일단 패키지가 설치되면 이름이 SUNWkcl2i로 변경됩니다. CD에 있는 본 패키지의 .u 확장자는 패키지를 sun4u 아키텍처 전용으로 정의합니다.

2. **다음을 입력하여 필수 소프트웨어를 설치합니다.**

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

install 스크립트는 시스템을 분석하여 설치할 필수 패치를 파악하여 설치할 뿐만 아니라, 기본 소프트웨어를 설치하고 선택적으로 옵션 소프트웨어를 설치하기도 합니다. 예제:

참고 – 다음 예제에서는 저작권 및 라이센스 정보가 생략되었습니다. 저작권 및 소프트웨어 라이센스에 관한 내용은 부록 E를 참조하십시오.

```
# ./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.
```

설치할 옵션 패키지 선택

Apache Web Server 및 Sun Crypto Accelerator 4000 온라인 매뉴얼 페이지를 위한 SSL 지원을 제공하는 옵션 패키지만 설치하려면 SUNWkcl2a 및 SUNWkcl2m을 선택하십시오.

옵션 소프트웨어 패키지를 모두 설치하려면 SUNWkcl2a, SUNWkcl2m, SUNWvcamn, SUNWvcav, SUNWkcl2o 및 SUNWkcl2i.u를 선택하십시오.

이전 예제의 옵션 패키지 내용에 대한 설명은 표 2-1을 참조하십시오.

디렉토리 및 파일

표 2-2는 Sun Crypto Accelerator 4000 소프트웨어의 기본 설치 시 생성되는 디렉토리를 나타냅니다.

표 2-2 Sun Crypto Accelerator 4000 디렉토리

디렉토리	내용
/etc/opt/SUNWconn/vca/keydata	키스토어 데이터(암호화)
/opt/SUNWconn/cryptov2/bin	유틸리티
/opt/SUNWconn/cryptov2/lib	지원 라이브러리
/opt/SUNWconn/cryptov2/sbin	관리 명령

그림 2-1은 디렉토리 및 파일의 계층 구조를 설명합니다.

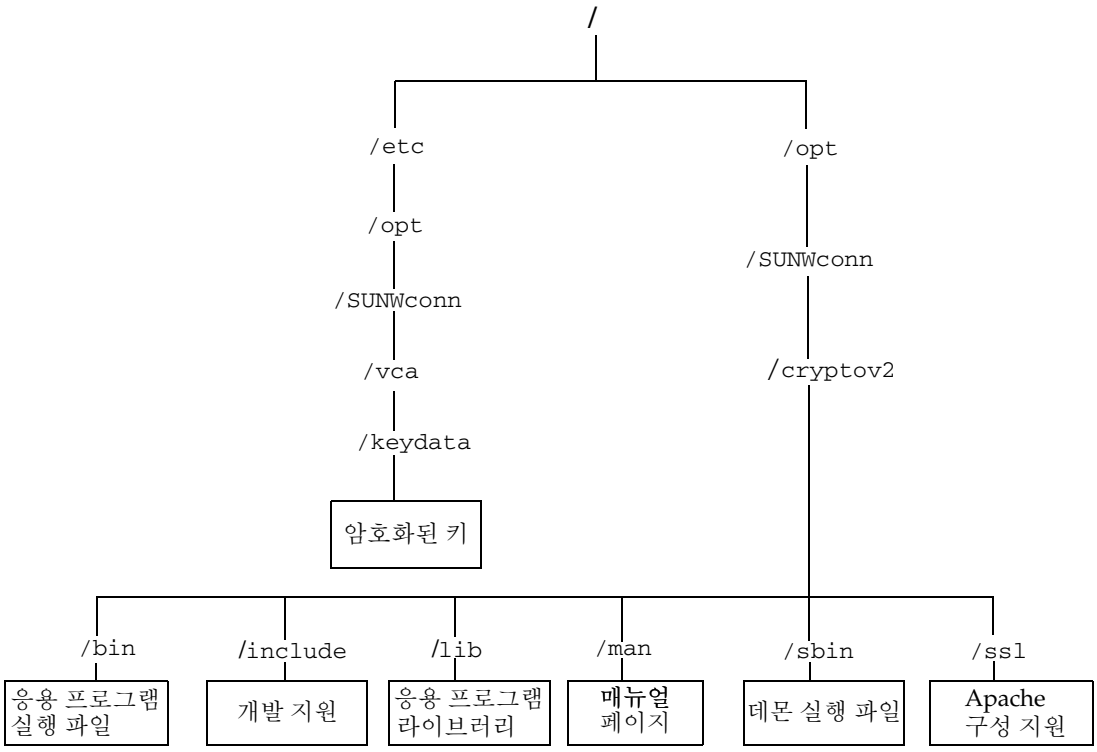

그림 2-1 Sun Crypto Accelerator 4000 디렉토리 및 파일

참고 – Sun Crypto Accelerator 4000 하드웨어 및 소프트웨어를 설치한 후에는 구성 및 키스토어 정보로 보드를 초기화해야 합니다. 보드 초기화 방법에 대한 내용은 64페이지의 "vcaadm을 통해 보드 초기화"를 참조하십시오.

Sun Crypto Accelerator 4000 소프트웨어 제거

소프트웨어를 제거하는 방법에는 CD-ROM의 `remove` 스크립트, 서버의 `/var/tmp/crypto_acc.remove` 스크립트 또는 `pkgrm` 명령을 사용하는 세 가지가 있습니다. 이 항목에서는 위의 두 가지 제거 스크립트를 사용하여 소프트웨어를 제거하는 방법에 대해 설명합니다. `pkgrm` 명령을 사용한 소프트웨어 제거 지침은 부록 B를 참조하십시오.

`install` 스크립트를 사용해 소프트웨어를 설치했으면 `remove` 스크립트를 사용해 소프트웨어를 제거합니다. 소프트웨어를 수동으로 설치했으면(부록 B) `/var/tmp/crypto_acc.remove` 스크립트를 사용합니다.

▼ `remove` 스크립트를 사용하여 소프트웨어 제거

- **Sun Crypto Accelerator 4000 CD-ROM을 삽입하고 다음을 입력합니다.**

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

▼ `/var/tmp/crypto_acc.remove` 스크립트를 사용하여 소프트웨어 제거

이 설치 로그는 아래 위치에 있습니다.

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

- **다음을 입력합니다.**

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

3 장

드라이버 매개 변수 구성

이 장에서는 Sun Crypto Accelerator 4000 UTP 및 MMF 이더넷 어댑터 모두에서 사용되는 vca 장치 드라이버 매개 변수의 구성 방법을 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

이더넷 장치 드라이버(vca) 매개 변수

vca 장치 드라이버는 Sun Crypto Accelerator 4000 UTP 및 MMF 이더넷 장치를 제어합니다. vca 드라이버는 Sun Crypto Accelerator 4000의 UNIX pci 이름 속성 pci108e,3de8에 첨부되어 있습니다(108e는 벤더 ID, 3de8는 PCI 장치 ID).

시스템의 각 Sun Crypto Accelerator 4000 장치를 사용자 정의하기 위해 vca 장치 드라이버 매개 변수를 수동으로 구성할 수 있습니다. 이 항목에서는 보드에 사용된 Sun Crypto Accelerator 4000 이더넷 장치의 기능에 대한 개요, 사용 가능한 vca 장치 드라이버 매개 변수 목록과 이런 매개 변수의 구성 방법을 설명합니다.

Sun Crypto Accelerator 4000 이더넷 UTP 및 MMF PCI 어댑터는 40페이지의 "OpenBoot PROM을 통한 링크 매개 변수에 대한 자동 교섭 모드 또는 강제 모드 활성화"에 나열되어 있는 운영 속도와 모드로 작동합니다. vca 장치는 기본적으로 speed, duplex, link-clock 매개 변수에 대한 일반 작동 모드를 선택할 때는 링크(링크 파트너)의 원격 끝을 통해 자동 교섭 모드로 작동합니다. link-clock 매개 변수는 보드가 1,000Mbps로 작동한 경우에만 적용할 수 있습니다. vca 장치는 또한 각각의 이런 매개 변수에 대해 강제 모드로 구성될 수도 있습니다.

주의 – 올바른 링크를 설정하려면 두 링크 파트너 모두가 speed, duplex, link-clock(1,000Mbps에서만 가능) 매개 변수 각각에 대해 자동 교섭 모드 또는 강제 모드로 작동 중이어야 합니다. 링크 파트너 중 하나라도 각각의 이런 매개 변수에 대해 동일한 모드로 작동하지 않는 경우 네트워크 오류가 발생하게 됩니다. 40페이지의 "OpenBoot PROM을 통한 링크 매개 변수에 대한 자동 교섭 모드 또는 강제 모드 활성화"를 참조하십시오.

드라이버 매개 변수 값 및 정의

표 3-1은 vca 장치 드라이버의 매개 변수와 설정을 설명합니다.

표 3-1 vca 드라이버 매개 변수, 상태 및 설명

매개 변수	상태	설명
instance	읽기 및 쓰기	장치 인스턴스
adv-autoneg-cap	읽기 및 쓰기	작동 모드 매개 변수
adv-1000fdx-cap	읽기 및 쓰기	작동 모드 매개 변수(MMF 어댑터 전용)
adv-1000hdx-cap	읽기 및 쓰기	작동 모드 매개 변수
adv-100fdx-cap	읽기 및 쓰기	작동 모드 매개 변수(UTP 어댑터 전용)
adv-100hdx-cap	읽기 및 쓰기	작동 모드 매개 변수(UTP 어댑터 전용)
adv-10fdx-cap	읽기 및 쓰기	작동 모드 매개 변수(UTP 어댑터 전용)
adv-10hdx-cap	읽기 및 쓰기	작동 모드 매개 변수(UTP 어댑터 전용)
adv-asmpause-cap	읽기 및 쓰기	흐름 제어 매개 변수
adv-pause-cap	읽기 및 쓰기	흐름 제어 매개 변수
pause-on-threshold	읽기 및 쓰기	흐름 제어 매개 변수
pause-off-threshold	읽기 및 쓰기	흐름 제어 매개 변수
link-master	읽기 및 쓰기	1Gbps 속도 강제 모드 매개 변수
enable-ipg0	읽기 및 쓰기	패킷 전송 전 추가 지연 활성화
ipg0	읽기 및 쓰기	패킷 전송 전 추가 지연
ipg1	읽기 및 쓰기	인터패킷 갭 매개 변수
ipg2	읽기 및 쓰기	인터패킷 갭 매개 변수
rx-intr-pkts	읽기 및 쓰기	인터럽트 블랭킹 값 수신
rx-intr-time	읽기 및 쓰기	인터럽트 블랭킹 값 수신
red-dv4to6k	읽기 및 쓰기	임의 조기 감지 및 패킷 드롭 백터

표 3-1 vca 드라이버 매개 변수, 상태 및 설명 *(계속)*

매개 변수	상태	설명
red-dv6to8k	읽기 및 쓰기	임의 조기 감지 및 패킷 드롭 백터
red-dv8to10k	읽기 및 쓰기	임의 조기 감지 및 패킷 드롭 백터
red-dv10to12k	읽기 및 쓰기	임의 조기 감지 및 패킷 드롭 백터
tx-dma-weight	읽기 및 쓰기	PCI 인터페이스 매개 변수
rx-dma-weight	읽기 및 쓰기	PCI 인터페이스 매개 변수
infinit-burst	읽기 및 쓰기	PCI 인터페이스 매개 변수
disable-64bit	읽기 및 쓰기	PCI 인터페이스 매개 변수

통지 링크 매개 변수

다음 매개 변수는 vca 드라이버가 해당 링크 파트너에게 통지할 speed 및 duplex 링크 매개 변수의 송수신을 결정합니다. 표 3-2는 작동 모드 매개 변수 및 해당 기본값을 설명합니다.

참고 – 매개 변수의 초기 설정이 0으로 설정된 경우 이를 변경할 수 없습니다. 초기 설정이 0인 설정을 변경해도 다시 0으로 복귀됩니다. 기본적으로, 이러한 매개 변수들은 vca 장치의 기능에 맞춰 설정됩니다.

Sun Crypto Accelerator 4000 UTP 어댑터의 통지 링크 매개 변수는 표 3-2에서 설명한 것과 같이 Sun Crypto Accelerator 4000 MMF 어댑터의 통지 링크 매개 변수와는 다릅니다.

표 3-2 작동 모드 매개 변수

매개 변수	설명	UTP 어댑터	MMF 어댑터
adv-autoneg-cap	하드웨어가 통지한 로컬 인터페이스 기능 0 = 강제 모드 1 = 자동 교섭(기본값)	X	X
adv-1000fdx-cap	하드웨어가 통지한 로컬 인터페이스 기능 0 = 1,000Mbps 전이중 불가 1 = 1000Mbps 전이중 가능(기본값)		X
adv-1000hdx-cap	하드웨어가 통지한 로컬 인터페이스 기능 0 = 1,000Mbps 반이중 불가 1 = 1,000Mbps 반이중 가능(기본값)	X	X

표 3-2 작동 모드 매개 변수 (*계속*)

매개 변수	설명	UTP 어댑터	MMF 어댑터
adv-100fdx-cap	하드웨어가 통지한 로컬 인터페이스 기능 0 = 100Mbps 전이중 불가 1 = 100Mbps 전이중 가능(기본값)	X	
adv-100hdx-cap	하드웨어가 통지한 로컬 인터페이스 기능 0 = 100Mbps 반이중 불가 1 = 100Mbps 반이중 가능(기본값)	X	
adv-10fdx-cap	하드웨어가 통지한 로컬 인터페이스 기능 0 = 10Mbps 전이중 불가 1 = 10Mbps 반이중 가능(기본값)	X	
adv-10hdx-cap	하드웨어가 통지한 로컬 인터페이스 기능 0 = 10Mbps 반이중 불가 1 = 10 Mbps 반이중 가능(기본값)	X	

표 3-2의 모든 매개 변수가 1로 설정된 경우 자동 교섭은 사용 가능한 최고 속도를 사용합니다. 위의 매개 변수가 모두 0으로 설정된 경우 다음 오류 메시지가 표시됩니다.

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

참고 – 위 예제에서 vca0은 모든 Sun Crypto Accelerator 4000 보드에 대해 문자열 vca가 사용되는 Sun Crypto Accelerator 4000 장치 이름입니다. 이 문자열의 바로 다음에는 항상 보드의 장치 인스턴스 번호가 따릅니다. 그러므로, vca0 보드의 장치 인스턴스 번호는 0입니다.

흐름 제어 매개 변수

vca 장치는 IEEE 802.3x Frame Based Link Level Flow Control Protocol(프레임 기반 링크 수준 흐름 제어 프로토콜)에 부합하는 휴지 프레임 송신(전송) 및 착신(수신)이 가능합니다. vca 장치는 수신한 흐름 제어 프레임에 답하여 자신의 전송률을 낮출 수 있습니다. 또한, vca 장치는 흐름 제어 프레임을 송신할 수 있어 링크 파트너가 이 기능을 지원하는 경우 링크 파트너에게 전송률을 낮출 것을 요청합니다. 기본적으로, 드라이버는 자동 교섭 중 전송과 수신 휴지 기능 모두를 통지합니다.

표 3-3은 흐름 제어 키워드와 기능을 설명합니다.

표 3-3 읽기-쓰기 흐름 제어 키워드 설명

키워드	설명		
adv-asmpause-cap	MMF 및 UTP 어댑터 모두 비대칭 휴지를 지원하므로 vca 장치는 한 방향으로만 휴지할 수 있습니다. 0=끔(기본값) 1=켬		
adv-pause-cap	이 매개 변수는 adv-asmpause-cap 값에 따라 두 가지 의미를 갖게 됩니다. (기본값=0)		
	매개 변수 값 +	**매개 변수 값 =**	**설명**
	adv-asmpause-cap=	adv-pause-cap=	
	1	1 또는 0	adv-pause-cap은 휴지 진행 방향을 결정합니다.
	1	1	휴지는 수신되지만 송신되지는 않습니다.
	1	0	휴지는 송신되지만 수신되지는 않습니다.
	0	1	휴지는 송수신됩니다.
	0	1 또는 0	adv-pause-cap은 휴지 기능의 활성 여부를 결정합니다.
pause-on-threshold	수신(RX) FIFO에서 64바이트 블록의 수를 정의하여 보드가 XON-PAUSE 프레임을 생성하도록 합니다.		
pause-off-threshold	RX FIFO에서 64바이트 블록의 수를 정의하여 보드가 XOFF-PAUSE 프레임을 생성하도록 합니다.		

기가비트 강제 모드 매개 변수

기가비트 링크에 대해서는, 이 매개 변수는 link-master를 결정합니다. 일반적으로, 스위치는 link-master로 활성화되며 이런 경우에는 이 매개 변수가 변경되지 않습니다. 그렇지 않은 경우에는 link-master 매개 변수가 vca 장치를 link-master로 활성화하기 위해 사용될 수 있습니다.

표 3-4 기가비트 강제 모드 매개 변수

매개 변수	설명
link-master	1로 설정된 경우 이 매개 변수는 링크 파트너를 슬레이브로 간주하고 마스터 작업을 활성화합니다. 0으로 설정된 경우 이 매개 변수는 링크 파트너를 마스터로 간주하고 슬레이브 작업을 활성화합니다(기본값).

인터패킷 갭 매개 변수

vca 장치는 enalble-ipg0이라는 프로그램 가능한 모드를 지원합니다.

enable-ipg0이 활성화된 패킷을 송신하기 전에, vca 장치는 추가 시간 지연을 설정합니다. ipg0 매개 변수로 설정된 이 지연은 ipg1 및 ipg2 매개 변수로 설정된 지연에 추가됩니다. 추가 ipg0 지연은 충돌을 줄입니다.

enable-ipg0이 비활성화된 경우, ipg0의 값은 무시되고 추가 지연은 설정되지 않습니다. ipg1 및 ipg2로 설정된 지연만 사용됩니다. 다른 시스템이 계속해서 대량의 연속 패킷을 전송하는 경우 enable-ipg0을 비활성화합니다. enable-ipg0이 활성화된 시스템은 네트워크 상에서 처리할 시간이 부족할 수도 있습니다. ipg0 매개 변수를 0에서 255까지 설정하여 지연을 추가할 수 있으며, 이는 매체 바이트 시간 지연입니다. 표 3-5는 enable-ipg0 및 ipg0 매개 변수에 대한 정의입니다.

표 3-5 enable-ipg0 및 ipg0을 정의하는 매개 변수

매개 변수	값	설명
enable-ipg0	0 1	enable-ipg0 활성화 enable-ipg0 비활성화(기본값=1)
ipg0	0에서 255	패킷 전송전(패킷 수신후) 추가 시간 지연(또는 갭)(기본값=8)

vca 장치는 프로그램 가능한 인터패킷 갭 매개 변수(IPG) ipg1 및 ipg2를 지원합니다. 총 IPG는 ipg1과 ipg2의 합계입니다. 1,000Mbps 링크 속도에 대한 총 IPG는 0.096마이크로초입니다.

표 3-6은 IPG 매개 변수에 대한 기본값과 허용되는 값의 목록입니다.

표 3-6 읽기-쓰기 인터패킷 갭 매개 변수 값 및 설명

매개 변수	값 (바이트-시간)	설명
ipg1	0에서 255	인터패킷 갭 1(기본값=8)
ipg2	0에서 255	인터패킷 갭 2(기본값=4)

드라이버는 기본적으로 ipg1을 8바이트 시간으로, ipg2를 4바이트 시간으로 설정하며, 이는 표준값이 됩니다(바이트 시간은 1,000Mbps의 링크 속도 설정에서 링크 상에 1바이트를 전송하는 데 소요되는 시간을 말합니다).

네트워크 상에 이보다 긴 IPG(ipg1 및 ipg2의 합)를 사용하는 시스템이 있고 이런 시스템에 대한 네트워크 액세스가 느린 경우 ipg1 및 ipg2의 값을 늘려 다른 시스템의 긴 IPG와 일치하도록 합니다.

인터럽트 매개 변수

표 3-7은 수신 인터럽트 블랭킹 값을 설명합니다.

표 3-7 RX 별칭 읽기용 블랭킹 레지스터

필드 이름	값	설명
rx-intr-pkts	0에서 511	최종 패킷 서비스 이후부터 해당 패킷 수가 도착한 후 인터럽트합니다. 0은 패킷 블랭킹이 없음을 의미합니다 (기본값=3).
rx-intr-time	0에서 524,287	최종 패킷 서비스 이후 4.5마이크로초(usecs)가 경과한 후 인터럽트합니다. 0은 시간 블랭킹이 없음을 의미합니다 (기본값=3).

임의 조기 드롭 매개 변수

이 매개 변수는 수신 FIFO의 용량 상태에 따른 패킷 드롭 기능을 제공합니다. 이 기능은 기본적으로 비활성화되어 있습니다. FIFO 점유율이 일정 범위에 도달하면 패킷은 사전 설정된 확률에 따라 드롭됩니다. FIFO 수준이 증가할 때 확률도 증가해야 합니다. 제어 패킷은 드롭되지 않으며 통계에서 제외됩니다.

표 3-8 RX 임의 조기 감지 8비트 벡터

필드 이름	값	설명
red-dv4to6k	0에서 255	FIFO 임계값이 4,096바이트 이상, 6,144바이트 이하인 경우의 임의 조기 감지 및 패킷 드롭 벡터입니다. 드롭 확률은 12.5퍼센트 단위로 세분화하여 프로그램할 수 있습니다. 예를 들어, 비트 0이 설정된 경우 각 8개 패킷 중 최초 패킷은 이 범주에서 드롭됩니다(기본값=0).
red-dv6to8k	0에서 255	FIFO 임계값이 6,144바이트 이상, 8,192바이트 이하인 경우의 임의 조기 감지 및 패킷 드롭 벡터입니다. 드롭 확률은 12.5퍼센트 단위로 세분화하여 프로그램할 수 있습니다. 예를 들어, 비트 8이 설정된 경우 각 8개 패킷 중 최초 패킷은 이 범주에서 드롭됩니다(기본값=0).
red-dv8to10k	0에서 255	FIFO 임계값이 8,192바이트 이상, 10,240바이트 이하인 경우의 임의 조기 감지 및 패킷 드롭 벡터입니다. 드롭 확률은 12.5퍼센트 단위로 세분화하여 프로그램할 수 있습니다. 예를 들어, 비트 16이 설정된 경우 각 8개 패킷 중 최초 패킷은 이 범주에서 드롭됩니다(기본값=0).
red-dv10to12k	0에서 255	FIFO 임계값이 10,240바이트 이상, 12,288바이트 이하인 경우의 임의 조기 감지 및 패킷 드롭 벡터입니다. 드롭 확률은 12.5퍼센트 단위로 세분화하여 프로그램할 수 있습니다. 예를 들어, 비트 24가 설정된 경우 각 8개 패킷 중 최초 패킷은 이 범주에서 드롭됩니다(기본값=0).

PCI 버스 인터페이스 매개 변수

이 매개 변수를 통해 PCI 인터페이스 특성을 수정하여 특정 응용 프로그램에 대해 보다 향상된 PCI 성능을 얻을 수 있습니다.

표 3-9 PCI 버스 인터페이스 매개 변수

매개 변수	설명
tx-dma-weight	가중된 라운드 로빈 조정이 실시되는 동안 전송(TX) 측에 크레디트를 부여하는 중복 계수를 결정합니다. 이 값은 0에서 3 사이입니다(기본값=0). 0은 별도의 가중이 없음을 뜻합니다. 다른 값은 가중 트래픽에 대해 2의 지수를 사용합니다. 예를 들어, tx-dma-weight = 0이고 rx-dma-weight = 3인 경우 RX 트래픽이 지속적으로 수신되는 동안 RX 트래픽의 우선 순위는 PCI에 액세스하는 트래픽의 우선 순위보다 8배 더 큽니다.
rx-dma-weight	가중된 라운드 로빈 조정이 실시되는 동안 전송(TX) 측에 크레디트를 부여하는 중복 계수를 결정합니다. 0에서 3사이의 값입니다(기본값=0).
infinite-burst	이 매개 변수가 활성화되면 무한 버스트를 지원하는 시스템에서 무한 버스트 기능을 사용할 수 있습니다. 어댑터는 버스를 통해 전체 패킷이 전송될 때까지 버스를 계속 사용합니다. 값은 0 또는 1입니다(기본값=0).
disable-64bit	어댑터의 64비트 기능을 끕니다. 참고: UltraSPARC® III 기반 플랫폼에서 이 매개 변수는 기본적으로 1로 설정될 수 있습니다. UltraSPARC II 기반 플랫폼에서 기본값은 0입니다. 값은 0 또는 1입니다(기본값=0,64비트 기능 활성화).

vca 드라이버 매개 변수 설정

vca 장치 드라이버를 다음 두 가지 방법으로 설정할 수 있습니다.

- ndd 유틸리티 사용
- vca.conf 파일 사용

ndd 유틸리티를 사용한 경우 매개 변수는 시스템을 재부팅할 때까지만 유효합니다. 이 방법은 매개 변수 설정을 테스트할 때 적합합니다.

매개 변수 설정이 시스템을 재부팅한 후에도 유효하도록 하려면 /kernel/drv/vca.conf 파일을 생성하고 시스템 내의 어떤 장치에 대해 특정 매개 변수를 설정할 필요가 있을 때 매개 변수 값을 이 파일에 추가합니다. 자세한 내용은 37페이지의 "vca.conf 파일을 사용한 드라이버 매개 변수 설정"을 참조하십시오.

ndd 유틸리티를 사용한 매개 변수 설정

ndd 유틸리티를 사용하여 시스템을 재부팅하기 전까지만 유효한 매개 변수를 설정합니다.

다음 항목은 vca 드라이버와 ndd 유틸리티를 사용하여 각 vca 장치의 매개 변수를 수정(-set 옵션으로) 또는 표시(-set 옵션 없이)하는 방법을 설명합니다.

▼ ndd 유틸리티용 장치 인스턴스 지정

vca 장치에 대한 매개 변수를 얻거나 설정하기 위해 ndd 유틸리티를 사용하기 전에는 유틸리티에 해당하는 장치 인스턴스를 지정해야 합니다.

1. **특정 장치와 관련된 인스턴스 번호를 확인하려면** /etc/path_to_inst **파일을 확인합니다.** path_to_inst**(4)에 대한 내용은 온라인 매뉴얼 페이지를 참조하십시오.**

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

위의 예제에서 세 가지 Sun Crypto Accelerator 4000 이더넷 인스턴스는 설치한 어댑터에서 기인합니다. 인스턴스 번호는 0과 1입니다.

2. 인스턴스 번호를 사용하여 장치를 선택합니다.

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

참고 – 본 설명서에 포함된 예제에서 *N*은 장치의 인스턴스 번호를 의미합니다.

선택을 변경할 때까지 장치는 선택된 상태로 남아있습니다.

비대화형 및 대화형 모드

ndd 유틸리티를 두 가지 모드로 사용할 수 있습니다:

- 비대화형
- 대화형

비대화형 모드에서 특정 명령을 실행하기 위해 유틸리티를 가동합니다. 일단 명령이 실행되면 유틸리티를 빠져 나갑니다. 대화형 모드에서는 유틸리티를 사용하여 하나 이상의 매개 변수 값을 얻거나 설정할 수 있습니다. 자세한 내용은 ndd(1M) 온라인 매뉴얼 페이지를 참조하십시오.

비대화형 모드에서 ndd *유틸리티 사용*

이 항목에서는 매개 변수 값을 변경하고 표시하는 방법을 설명합니다.

- **매개 변수 값을 수정하려면** -set **옵션을 사용합니다.**

  ndd 유틸리티를 -set 옵션으로 호출한 경우 유틸리티는 *value*를 전달하며 이 value는 /dev/vca 드라이버 인스턴스의 이름으로 지정되어야 하며, 이 값을 매개 변수에 할당합니다.

```
# ndd -set /dev/vcaN 매개 변수 값
```

adv 매개 변수를 변경하면 다음과 유사한 메시지가 나타납니다.

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

- **매개 변수 값을 표시하려면 매개 변수 이름을 명시하고 값을 생략합니다.**

  -set 옵션을 생략하면 이를 질의 작업으로 간주하여 유틸리티는 지정된 드라이버 인스턴스를 질의한 후 지정된 매개 변수와 관련된 값을 검색하고 출력합니다.

```
# ndd /dev/vcaN 매개 변수
```

참고 – 이전 예제에서 *N*은 vca 장치의 인스턴스 번호입니다. 이 번호는 kstat 명령을 실행하는 보드의 인스턴스 번호를 반영해야 합니다.

대화형 모드에서 ndd *유틸리티 사용*

- **대화형 모드에서 매개 변수 값을 수정하려면 다음과 같이** ndd /dev/vca*N***을 지정합니다.**

  그러면 ndd 유틸리티가 매개 변수 이름 입력을 위한 프롬프트를 표시합니다.

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

참고 – 이전 예제에서 *N*은 vca 장치의 인스턴스 번호입니다. 이 번호는 kstat 명령을 실행하는 보드의 인스턴스 번호를 반영해야 합니다.

매개 변수 이름이 입력되면 ndd 유틸리티는 매개 변수 값을 묻는 프롬프트를 표시합니다(표 3-1에서 표 3-9까지 참조).

- **vca 드라이버가 지원하는 모든 매개 변수를 나열하려면** ndd /dev/vca*N*을 **입력합니다.**

  (매개 변수 설명은 표 3-1에서 표 3-9까지 참조)

```
# 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 ?
#
```

참고 – 이전 예제에서 *N*은 vca 장치의 인스턴스 번호입니다. 이 번호는 kstat 명령을 실행하는 보드의 인스턴스 번호를 반영해야 합니다.

자동 교섭 또는 강제 모드 설정

다음 링크 매개 변수를 자동 교섭 또는 강제 모드로 작동하도록 설정할 수 있습니다.

- speed
- duplex
- link-clock

기본적으로, 이 링크 매개 변수에는 자동 교섭 모드가 활성화됩니다. 매개 변수 중 어느 하나가 자동 교섭 모드에 있는 경우 vca 장치는 호환값과 흐름 제어 기능을 교섭하기 위해 링크 파트너와 통신합니다. 이런 매개 변수 중 어느 하나라도 auto이외의 값으로 설정된 경우 교섭은 수행되지 않고 링크 매개 변수가 강제 모드로 구성됩니다. 강제 모드에서는 speed 매개 변수 값이 링크 파트너 간에 일치해야 합니다. 40페이지의 "OpenBoot PROM을 통한 링크 매개 변수에 대한 자동 교섭 모드 또는 강제 모드 활성화"를 참조하십시오.

▼ 자동 교섭 모드 비활성화

네트워크 장비가 자동 교섭을 지원하지 않거나 네트워크 speed, duplex 및 link-clock 매개 변수를 강제로 설정하려면 vca 장치 상에서 자동 교섭 모드를 비활성화할 수 있습니다.

1. **링크 파트너 장치와 함께 제공된 설명서에서 수록된 값으로 다음 드라이버 매개 변수를 설정합니다(예, 스위치).**
   - adv-1000fdx-cap
   - adv-1000hdx-cap
   - adv-100fdx-cap
   - adv-100hdx-cap
   - adv-10fdx-cap
   - adv-10hdx-cap
   - adv-asmpause-cap
   - adv-pause-cap

   이런 매개 변수에 대한 설명과 설정 가능한 값은 표 3-2를 참조하십시오.

2. adv-autoneg-cap **매개 변수를** 0**으로 설정합니다.**

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

ndd 연결 매개 변수를 변경하면 다음과 유사한 메시지가 나타납니다.

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

참고 – 자동 교섭을 비활성화한 경우 speed, duplex 및 link-clock(1,000Mbps에서만 가능) 매개 변수가 강제 모드에서 작동하도록 활성화해야 합니다. 해당 지침은 40페이지의 "OpenBoot PROM을 통한 링크 매개 변수에 대한 자동 교섭 모드 또는 강제 모드 활성화"를 참조 하십시오.

vca.conf 파일을 사용한 매개 변수 설정

/kernel/drv 디렉토리의 vca.conf 파일에 항목을 추가하여 드라이버 매개 변수 속성을 지정할 수도 있습니다. 매개 변수 이름은 24페이지의 "드라이버 매개 변수 값 및 정의"에 나열된 이름과 같습니다.

주의 – /kernel/drv/vca.conf 파일의 그 어떠한 기본 항목을 삭제하지 마십시오.

prtconf(1) 및 driver.conf(4) 온라인 매뉴얼 페이지에는 이에 대한 추가 정보를 제공합니다. 다음 절차는 vca.conf 파일에서 매개 변수를 설정하는 예를 설명합니다.

이전 항목에서 정의된 변수는 시스템에서 이미 알려진 장치에 적용됩니다. vca.conf 파일로 Sun Crypto Accelerator 4000 보드에 대한 변수를 설정하려면 해당 장치에 대해 다음 세 가지 정보를 알고 있어야 합니다. 즉, 장치 이름, 장치 부모, 장치 단위 주소입니다.

▼ vca.conf 파일을 사용한 드라이버 매개 변수 설정

1. **장치 트리에서 해당** vca **장치에 대한 하드웨어 경로 이름을 획득합니다.**

   a. **특정 장치와 관련된 이름을 검색하려면** /etc/driver_aliases **파일을 확인합니다.**

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

   위 예제에서 Sun Crypto Accelerator 4000 소프트웨어 드라이버(vca)와 관련된 장치 이름은 "pci108e,3de8"입니다.

   b. /etc/path_to_inst **파일에서 장치 부모 이름과 장치 단위 주소를 검색합니다.**

   path_to_inst(4)에 대한 내용은 온라인 매뉴얼 페이지를 참조하십시오.

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

위 예제에서 장치 경로 이름, 인스턴스 번호, 소프트웨어 드라이버 이름이란 세 개의 열이 출력됩니다.

위 예제에서 첫 행의 장치 경로 이름은 "/pci@8,600000/network@1"입니다. 장치 경로 이름은 장치 부모 이름, 장치 노드 이름, 장치 단위 주소란 세 부분으로 구성되어 있습니다. 표 3-10을 참조하십시오.

표 3-10 장치 경로 이름

전체 장치 경로 이름	부모 이름 부분	노드 이름 부분	단위 주소 부분
"/pci@8,600000/network@1"	/pci@8,600000	network	1
"/pci@8,700000/network@1"	/pci@8,700000	network	1

vca.conf 파일에서 PCI 장치를 명확하게 식별하려면 전체 장치 경로 이름을 사용합니다(부모 이름, 노드 이름, 단위 주소). PCI 장치 사양에 대한 자세한 내용은 pci(4) 온라인 매뉴얼 페이지를 참조하십시오.

2. **/kernel/drv/vca.conf 파일에서 vca 장치에 대한 매개 변수를 설정합니다.**

   다음 항목에서 특정 Sun Crypto Accelerator 4000 이더넷 장치에 대하여 adv-autoneg-cap 매개 변수가 비활성화됩니다 .

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

3. **vca.conf 파일을 저장합니다.**
4. **모든 파일과 프로그램을 저장하고 종료한 후 창 기능 시스템을 빠져 나갑니다.**
5. **시스템을 종료하고 재부팅합니다.**

vca.conf 파일로 모든 Sun Crypto Accelerator 4000 vca 장치의 매개 변수 설정

장치 경로 이름을 생략한 경우(부모 이름, 노드 이름, 단위 주소) 모든 Sun Crypto Accelerator 4000 이더넷 장치의 모든 인스턴스에 대한 변수가 설정됩니다.

▼ vca.conf 파일로 모든 Sun Crypto Accelerator 4000 vca 장치의 매개 변수 설정

1. **매개** *변수=값;***을 입력하여 모든 인스턴스에 대한 매개 변수 값을 변경할 수 있도록** vca.conf **파일에 행 하나를 추가합니다.**

   다음 예제에서는 모든 Sun Crypto Accelerator 4000 이더넷 장치의 모든 인스턴스에 대해 adv-autoneg-cap 매개 변수를 1로 설정합니다.

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

vca.conf 파일 예제

다음은 vca.conf 파일 예제입니다.

```
#
# Copyright 2003 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
#ident  "@(#)vca.conf   1.3     13-03-10 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;
```

OpenBoot PROM을 통한 링크 매개 변수에 대한 자동 교섭 모드 또는 강제 모드 활성화

OpenBoot PROM 인터페이스에서 다음 매개 변수가 자동 교섭 또는 강제 모드에서 작동되도록 설정할 수 있습니다.

표 3-11 로컬 링크 네트워크 장치 매개 변수

매개 변수	설명
speed	이 매개 변수는 auto, 1000, 100 또는 10으로 설정할 수 있으며, 구문은 다음과 같습니다. • speed=auto(기본값) • speed=1000 • speed=100 • speed=10
duplex	이 매개 변수는 auto, full 또는 half으로 설정할 수 있으며, 구문은 다음과 같습니다. • duplex=auto(기본값) • duplex=full • duplex=half
link-clock	이 매개 변수는 speed 매개 변수가 1000으로 설정되어 있거나 1,000Mbps MMF Sun Crypto Accelerator 4000 보드를 사용하는 경우에만 적용할 수 있습니다. 이 매개 변수의 값은 링크 파트너의 값과 일치해야 합니다 — 예를 들어, 로컬 링크의 값이 master인 경우 링크 파트너는 slave 값을 가져야 합니다. 이 매개 변수는 master, slave 또는 auto로 설정할 수 있으며, 구문은 다음과 같습니다. • link-clock=auto(기본값) • link-clock=master • link-clock=slave

적절한 링크를 설정하려면 로컬 링크와 링크 파트너 간의 speed, duplex 및 link-clock(1,000Mbps에서만 가능) 매개 변수가 올바르게 구성되어야 합니다. 두 링크 파트너 모두가 speed, duplex, link-clock(1,000Mbps에서만 가능) 매개 변수 각각에 대해 자동 교섭 모드 또는 강제 모드로 작동 중이어야 합니다. 이 매개 변수 중 하나에 auto 값이 설정되면 해당 매개 변수의 링크가 자동 교섭 모드로 작동됩니다. OpenBoot ok 프롬프트에서 매개 변수가 없으면 해당 매개 변수가 기본값인 auto를 갖도록 구성합니다. auto 이외의 값은 해당 매개 변수에 대한 로컬 링크가 강제 모드에서 작동하도록 구성합니다.

로컬 링크가 100Mbps 미만의 속도 및 전이중과 반이중에서 speed 및 duplex 매개 변수에 대해 자동 교섭 모드로 작동하게 되면 링크 파트너는 전이중과 반이중 하나에서 100Mps 또는 10Mbps 속도를 사용합니다.

speed 매개 변수가 강제 모드에서 작동하는 경우 이 값은 링크 파트너의 speed 값과 일치해야 합니다. 로컬 링크와 링크 파트너 간의 duplex 매개 변수가 일치하지 않은 경우 링크는 활성화되지만 트래픽 충돌이 발생하게 됩니다.

로컬 링크 speed 매개 변수가 자동 교섭으로, 링크 파트너 speed 매개 변수가 강제로 설정되면 로컬 링크와 링크 파트너 간의 speed 값 교섭 가능 여부에 따라 링크가 활성화됩니다. 자동 교섭 모드의 인터페이스는 언제나 반이중으로 링크(속도가 일치하는 경우) 활성화를 시도합니다. 두 인터페이스 중 하나가 자동 교섭 모드가 아니기 때문에 자동 교섭 모드의 인터페이스는 speed 매개 변수만을 감지합니다. 이중 매개 변수는 감지되지 않습니다. 이런 기법을 병렬 감지라고 합니다.

주의 – 이중 충돌로 링크를 활성화하게 되면 항상 트래픽 충돌이 발생합니다.

로컬 링크 매개 변수가 강제 모드에서 작동하려면 매개 변수는 auto 이외의 값을 가져야 합니다. 예를 들어, 반이중으로 100Mbps에서 강제 모드 링크를 활성화하려면 OpenBoot PROM ok 프롬프트에서 다음을 입력합니다.

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

참고 – 이 항목의 예제에서는 net은 기본적인 통합 네트워크 인터페이스 장치 경로의 별칭입니다. net 외의 장치 경로 이름을 지정하여 다른 네트워크 장치를 구성할 수 있습니다.

클럭 마스터인 반이중 1,000Mbps에서 강제 모드를 활성화하려면 OpenBoot PROM ok 프롬프트에서 다음 명령을 입력합니다.

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

참고 – link-clock 매개 변수의 값은 링크 파트너의 link-clock 값과 상응해야 합니다. 예를 들어, 로컬 링크의 link-clock 값이 master로 설정된 경우 링크 파트너의 link-clock 값은 slave로 설정되어야 합니다.

10Mbps 속도에는 강제 모드를 설정하고 이중에는 자동 교섭 모드를 설정하려면 OpenBoot PROM ok 프롬프트에서 다음을 입력합니다.

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

또한 OpenBoot PROM ok 프롬프트에서 다음을 입력하여 이전 예제와 동일한 로컬 링크 매개 변수를 설정할 수 있습니다.

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

자세한 내용은 IEEE 802.3 설명서를 참조하십시오.

암호화 및 이더넷 드라이버 운영 통계

이 항목에서는 kstat(1M) 명령이 제공하는 통계에 대해 설명합니다.

암호화 드라이버 통계

표 3-12는 암호화 드라이버 통계를 설명합니다.

표 3-12 암호화 드라이버 통계

매개 변수	설명	안정 여부
vs-mode	값은 FIPS, standard 또는 unitialized입니다. FIPS는 보드가 FIPS 모드에 있다는 것을 의미합니다. standard는 보드가 FIPS 모드에 있지 않다는 것을 의미합니다. unitialized는 보드가 초기화되지 않았다는 것을 의미합니다.	안정
vs-status	값은 ready, faulted 또는 failsafe입니다. ready는 보드가 정상적으로 작동하고 있다는 것을 의미합니다. faulted는 보드가 작동하지 않고 있다는 것을 의미합니다. failsafe는 보드의 출하 시 상태인 failsafe 모드를 의미합니다.	안정

이더넷 드라이버 통계

표 3-13은 이더넷 드라이버 통계를 설명합니다.

표 3-13 이더넷 드라이버 통계

매개 변수	설명	안정 여부
ipackets	인바운드 패킷 수	안정
ipackets64	ipackets의 64비트 버전	안정
ierrors	오류를 포함하고 있어 처리할 수 없는 총 수신 패킷(장기)	안정
opackets	인터페이스에 전송 요청된 총 패킷	안정
opackets64	인터페이스에 전송 요청된 총 패킷(64비트)	안정
oerrors	오류로 인해 성공적으로 전송할 수 없었던 총 패킷(장기)	안정
rbytes	인터페이스에서 성공적으로 수신한 총 바이트	안정
rbytes64	인터페이스에서 성공적으로 수신한 총 바이트(64비트)	안정
obytes	인터페이스에 전송 요청된 총 바이트	안정
obytes64	인터페이스에 전송 요청된 총 바이트(64비트)	안정
multircv	그룹 및 기능적 주소를 포함하여 성공적으로 수신된 멀티캐스트 패킷(장기)	안정
multixmt	그룹 및 기능적 주소를 포함하여 전송 요청된 멀티캐스트 패킷(장기)	안정
brdcstrcv	성공적으로 수신된 동보 패킷(장기)	안정
brdcstxmt	전송 요청된 동보 패킷(장기)	안정
norcvbuf	수신용 패킷을 위한 버퍼가 할당되지 않아 유효한 수신 패킷이 취소된 횟수(장기)	안정
noxmtbuf	송신 버퍼가 작업 중이었거나 송신 버퍼가 할당되지 않아 출력 시 폐기된 패킷(장기)	안정

표 3-14는 송수신 MAC 카운터를 설명합니다.

표 3-14 TX 및 RX MAC 카운터

매개 변수	설명	안정 여부
tx-collisions	충돌을 일으킨 모든 프레임 전송 시도에 대한 16비트 로드 가능한 카운터 증분치	안정
tx-first-collisions	최초 시도에서 충돌이 있었지만 다음 시도에서 성공적으로 전송된 매 프레임에 대한 16비트 로드 가능한 카운터 증분치	불안정
tx-excessive-collisions	시도 수 제한값을 초과한 매 프레임 전송에 대한 16비트 로드 가능한 카운터 증분치	불안정
tx-late-collisions	충돌이 있었던 매 프레임 전송에 대한 16비트 로드 가능한 카운터 증분치. 이 매개변수는 적어도 최소 프레임 크기 바이트 수를 전송한 후 발생한 충돌로 인하여 TxMAC가 드롭한 프레임의 수를 표시합니다. 보통, 네트워크의 최대 허용 폭을 준수하지 않은 스테이션이 네트워크상에 적어도 하나가 있다는 것을 의미합니다.	불안정
tx-defer-timer	프레임 전송 시도 시 TxMAC가 네트워크의 트래픽으로 미루고 있는 16비트 로드 가능한 타이머 증분치. 타이머 기준 시간은 256으로 나눈 매체 바이트 시각입니다.	불안정
tx-peak-attempts	8비트 레지스터는 본 레지스터가 마지막으로 읽은 이후의 성공적으로 전송된 프레임 당 최대 연속 충돌 수를 표시합니다. 이 레지스터가 구할 수 있는 최대값은 255입니다. 성공적으로 전송된 프레임 당 연속 충돌 수가 255를 넘는 경우 소프트웨어에 마스크 가능한 인터럽트가 생성됩니다. 읽기가 완료되면 이 레지스터는 자동으로 0이 됩니다.	불안정
tx-underrun	네트워크에서 유효 프레임을 수신한 후의 16비트 로드 가능한 카운터 증분치	불안정
rx-length-err	네트워크에서 프로그램된 최대 프레임 크기 레지스터보다 긴 프레임을 수신한 후의 16비트 로드 가능한 카운터 증분치	불안정

표 3-14 TX 및 RX MAC 카운터*(계속)*

매개 변수	설명	안정 여부
rx-alignment-err	수신 프레임에서 정렬 오류 감지 할 때 16비트 로드 가능한 카운터 증분치. 수신 프레임이 CRC(Cyclic Redundancy Checksum) 알고리즘에 실패하고 해당 프레임에 정수값이 아닌 바이트 수가 포함될 때(즉, 비트 단위의 프레임 크기가 0이 아닌 경우) 정렬 오류가 보고됩니다.	불안정
rx-crc-err	수신 프레임이 CRC 확인 알고리즘에 실패하고 해당 프레임에 정수값의 바이트 수가 포함되어 있을 때(즉, 8비트 모듈의 프레임 크기가 0인 경우) 16비트 로드 가능한 카운터 증분치	불안정
rx-code-violations	프레임을 수신하는 동안 MII 상에서 XCVR이 Rx_Err 지시를 생성할 때 16비트 로드 가능한 카운터 증분치. 이 지시는 송수신기가 수신한 데이터 스트림에서 부적절한 코드를 감지했을 때 생성됩니다. 수신 코드 위반은 FCS 또는 정렬 오류로 카운트되지 않습니다.	불안정
rx-overflows	자원 부족으로 드롭된 이더넷 프레임 수	불안정
rx-no-buf	수신 버퍼 공간이 부족하여 하드웨어가 데이터를 수신하지 못한 횟수	불안정
rx-no-comp-wb	하드웨어가 수신한 데이터에 대한 완료 항목 입력을 수행하지 못한 횟수	불안정
rx-len-mismatch	표시된 길이가 실제 프레임 길이와 맞지 않는 상태에서 수신된 프레임 수	불안정

다음 이더넷 속성(표 3-15)은 장치 특성과 링크 파트너 특성을 논리곱하여 도출된 것입니다.

표 3-15 현재 이더넷 링크 속성

매개 변수	설명	안정 여부
ifspeed	1000, 100 또는 10Mbps	안정
link-duplex	0=반, 1=전	안정
link-pause	링크에 대한 현재 휴지 설정(26페이지의 "흐름 제어 매개 변수" 참조)	안정
link-asmpause	링크에 대한 현재 휴지 설정(26페이지의 "흐름 제어 매개 변수" 참조)	안정

표 3-15 현재 이더넷 링크 속성*(계속)*

매개 변수	설명	안정 여부
link-up	1=활성, 0=비활성	안정
link-status	1=활성, 0=비활성	안정
xcvr-inuse	사용 중인 송수신기 종류: 1=내부 MII, 2=외부 MII, 3=외부 PCS	안정

표 3-16은 읽기 전용 매체 독립 인터페이스(MII)의 기능을 설명합니다. 이 매개 변수는 하드웨어의 기능을 정의합니다. 기가비트 매체 독립 인터페이스(GMII)는 다음 기능을 모두 지원합니다.

표 3-16 읽기 전용 vca 장치 기능

매개 변수	설명	안정 여부
cap-autoneg	0 = 자동 교섭 불가 1 = 자동 교섭 가능	안정
cap-1000fdx	로컬 인터페이스 전이중 가능 여부 0 = 1,000Mbps 전이중 불가 1 = 1,000Mbps 전이중 가능	안정
cap-1000hdx	로컬 인터페이스 반이중 가능 여부 0 = 1,000Mbps 반이중 불가 1 = 1,000Mbps 반이중 가능	안정
cap-100fdx	로컬 인터페이스 전이중 가능 여부 0 = 100Mbps 전이중 불가 1 = 100Mbps 전이중 가능	안정
cap-100hdx	로컬 인터페이스 반이중 가능 여부 0 = 100Mbps 반이중 불가 1 = 100Mbps 반이중 가능	안정
cap-10fdx	로컬 인터페이스 전이중 가능 여부 0 = 10Mbps 전이중 불가 1 = 10Mbps 전이중 가능	안정
cap-10hdx	로컬 인터페이스 반이중 가능 여부 0 = 10Mbps 반이중 불가 1 = 10Mbps 반이중 가능	안정
cap-asm-pause	로컬 인터페이스 흐름 제어 가능 여부 0 = 비대칭 휴지 불가 1 = 비대칭 휴지(로컬 장치로부터) 가능(26페이지의 "흐름 제어 매개 변수" 참조)	안정
cap-pause	로컬 인터페이스 흐름 제어 가능 여부 0 = 대칭 휴지 불가 1 = 대칭 휴지 가능(26페이지의 "흐름 제어 매개 변수" 참조)	안정

링크 파트너 기능 보고

표 3-17은 읽기 전용 링크 파트너의 기능을 설명합니다.

표 3-17 읽기 전용 링크 파트너 기능

매개 변수	설명	안정 여부
lp-cap-autoneg	0 = 자동 교섭 불가 1 = 자동 교섭	안정
lp-cap-1000fdx	0 = 1,000Mbps 전이중 전송 불가 1 = 1,000Mbps 전이중	안정
lp-cap-1000hdx	0 = 1,000Mbps 반이중 전송 불가 1 = 100Mbps 반이중 전송	안정
lp-cap-100fdx	0 = 100Mbps 전이중 전송 불가 1 = 100Mbps 전이중	안정
lp-cap-100hdx	0 = 100Mbps 반이중 전송 불가 1 = 100Mbps 반이중	안정
lp-cap-10fdx	0 = 10Mbps 전이중 전송 불가 1 = 10Mbps 전이중 전송	안정
lp-cap-10hdx	0 = 10Mbps 반이중 전송 불가 1 = 10Mbps 반이중 전송	안정
lp-cap-asm-pause	0 = 비대칭 휴지 불가 1 = 링크 파트너 기능에 대한 비대칭 휴지 (26페이지의 "흐름 제어 매개 변수" 참조)	안정
lp-cap-pause	0 = 대칭 휴지 불가 1 = 대칭 휴지 가능(26페이지의 "흐름 제어 매개 변수" 참조)	안정

링크 파트너가 자동 교섭이 불가능한 경우(lp-cap-autoneg이 0일 때) 표 3-17에 설명된 나머지 내용은 이와 연관이 없어지며, 매개 변수 값은 0입니다.

링크 파트너가 자동 교섭이 가능한 경우(lp-cap-autoneg이 1일 때) 자동 교섭과 링크 파트너 기능을 사용하면 속도와 모드 정보가 표시됩니다.

표 3-18은 드라이버의 고유 매개 변수를 설명합니다.

표 3-18 드라이버 고유 매개 변수

매개 변수	설명	안정 여부
lb-mode	해당되는 경우, 장치가 속한 루프백 모드 복사	불안정
promisc	활성화된 경우, 장치는 자유 모드입니다. 비활성화된 경우, 장치는 자유 모드가 아닙니다.	불안정
이더넷 전송 카운터		
tx-wsrv	전송 링이 가득 찬 횟수 카운트	불안정
tx-msgdup-fail	패킷 복제 시도 실패	불안정
tx-allocb-fail	메모리 할당 시도 실패	불안정
tx-queue0	최초 하드웨어 전송 대기열에서 전송 대기 중인 패킷 수	불안정
tx-queue1	두 번째 하드웨어 전송 대기열에서 전송 대기 중인 패킷 수	불안정
tx-queue2	세 번째 하드웨어 전송 대기열에서 전송 대기 중인 패킷 수	불안정
tx-queue3	네 번째 하드웨어 전송 대기열에서 전송 대기 중인 패킷 수	불안정
이더넷 수신 카운터		
rx-hdr-pkts	256바이트 이하로 수신된 패킷 수	불안정
rx-mtu-pkts	256바이트 이상, 1,514바이트 이하로 수신된 패킷 수	불안정
rx-split-pkts	두 페이지로 분할된 패킷 수	불안정
rx-nocanput	IP 스택으로의 전달 실패로 인해 드롭된 패킷 수	불안정
rx-msgdup-fail	복제가 불가능했던 패킷 수	불안정
rx-allocb-fail	불록 할당이 실패한 수	불안정
rx-new-pages	수신 중 대체된 페이지 수	불안정
rx-new-hdr-pages	수신 중 대체된 256바이트 이하의 패킷으로 채워진 페이지 수	불안정
rx-new-mtu-pages	수신 중 대체된 256바이트 이상, 1,514 이하의 패킷으로 채워진 페이지 수	불안정
rx-new-nxt-pages	수신 중 대체된 페이지별로 분할된 패킷을 포함한 페이지 수	불안정

표 3-18 드라이버 고유 매개 변수*(계속)*

매개 변수	설명	안정 여부
rx-page-alloc-fail	페이지 할당이 실패한 수	불안정
rx-mtu-drops	드라이버가 페이지를 대체하기 위해 신규 페이지를 맵하는 것이 불가능하여 256바이트보다 크고 1,514보다 작은 패킷의 전체 페이지가 드롭된 횟수	불안정
rx-hdr-drops	드라이버가 페이지를 대체하기 위해 신규 페이지를 맵하는 것이 불가능하여 256바이트 이하인 패킷의 전체 페이지가 드롭된 횟수	불안정
rx-nxt-drops	드라이버가 페이지를 대체하기 위해 신규 페이지를 맵하는 것이 불가능하여 분할 패킷이 담긴 페이지가 드롭된 횟수	불안정
rx-rel-flow	드라이버가 흐름 해제를 요청받은 횟수	불안정
이더넷 PCI 속성		
rev-id	필드에서 사용 중인 장치를 인식하는 데 유용한 Sun Crypto Accelerator 4000 이더넷 장치의 개정 ID	불안정
pci-err	모든 PCI 오류의 합계	불안정
pci-rta-err	수신된 대상 중단 수	불안정
pci-rma-err	수신된 마스터 중단 수	불안정
pci-parity-err	감지된 PCI 패리티 오류 수	불안정
pci-drto-err	지연된 트랜잭션의 재시도 시간 초과 횟수	불안정
dma-mode	Sun Crypto Accelerator 4000 드라이버에 의해 사용(vca)	불안정

▼ 링크 파트너 설정 확인

- **수퍼유저 권한으로** `kstat vca:`*N* **명령을 입력합니다.**

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

여기서 *N*은 vca 장치의 인스턴스 번호입니다. 이 번호는 kstat 명령을 실행하는 보드의 인스턴스 번호를 반영해야 합니다.

IPsec 인라인 가속화 통계

표 3-19는 보드를 인라인 IPsec 하드웨어 가속화 용도로 구성할 때 증가하는 커널 통계에 대해 설명합니다. 인라인 IPsec 설정을 사용하기 위한 보드 구성 방법에 대한 지침은 53페이지의 "인라인 IPsec 가속화 활성화"를 참조하십시오.

표 3-19 인라인 IPsec 가속화를 위한 암호화 드라이버 통계

매개 변수	설명	안정 여부
ipsec_ierrrors	오류를 포함하고 있어 처리할 수 없는 총 수신 IPsec 패킷(장기)	안정
ipsec_ipackets	인바운드 IPsec 패킷 수	안정
ipsec_ipackets64	인바운드 IPsec 패킷 수(64비트)	안정
ipsec_obytes	인터페이스에 전송 요청된 총 IPsec 바이트	안정
ipsec_obytes64	인터페이스에 전송 요청된 총 IPsect 바이트(64비트)	안정
ipsec_oerrors	오류로 인해 성공적으로 전송하지 못한 총 IPsec 패킷(장기)	안정
ipsec_opackets	인터페이스에 전송 요청된 총 IPsec 패킷	안정
ipsec_opackets64	인터페이스에 전송 요청된 총 IPsec 패킷(64비트)	안정
ipsec_rbytes	인터페이스에서 성공적으로 수신한 총 IPsec 바이트	안정
ipsec_rbytes64	인터페이스에서 성공적으로 수신한 총 IPsec 바이트(64비트)	안정
sadb_cache_misses	펌웨어 캐시 누락 수	안정
sadb_cache_overflows	펌웨어 캐시 오버플로 수	안정
sadb_entries	SADB 드라이버의 항목 수	안정
sadb_operations	Solaris IPsec에서 드라이버로 보낸 SADB 작업 수	안정

참고 – 표 3-19에 나열된 IPsec 커널 통계는 하드웨어에서 실제로 인라인으로 처리되는 IPsec 패킷에 대해서만 증가합니다. 256바이트 이하의 수신 패킷은 인라인으로 처리되지 않으며 IPsec 커널 통계는 이러한 패킷에 대해 증가하지 않습니다. 위의 커널 통계는 또한 대역 외 IPsec 트래픽에는 적용되지 않습니다(52페이지의 "IPsec 하드웨어 가속화 구성" 참조). `snoop`이 활성화되면 위의 카운터가 증가하지 않습니다. 대역 외 패킷은 일정한 네트워크 커널 통계와 `3desbytes` 및 `3desjobs` 같은 해당되는 모든 암호화 통계를 증가시킵니다.

네트워크 구성

이 항목은 시스템에 어댑터를 설치한 후 네트워크 호스트 파일을 편집하는 방법을 설명합니다.

네트워크 호스트 파일 구성

드라이버 소프트웨어를 설치한 후 어댑터의 이더넷 인터페이스를 위한 `hostname.vca`*N* 파일을 생성해야 합니다. 파일 이름 `hostname.vca`*N*에서 *N*은 사용할 `vca` 인터페이스의 인스턴스 번호에 해당합니다. 또한, `/etc/hosts` 파일에 해당 이더넷 인터페이스에 대해 IP 주소와 호스트 이름을 생성해야 합니다.

1. `/etc/path_to_inst` **파일에서 적절한** `vca` **인터페이스와 인스턴스 번호를 검색합니다.**

   `path_to_inst`(4)에 대한 내용은 온라인 매뉴얼 페이지를 참조하십시오.

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

   위 예제에서 인스턴스 번호는 0입니다.

2. `ifconfig`**(1M) 명령을 사용하여 어댑터의** `vca` **인터페이스를 설정합니다.**

   `ifconfig` 명령을 사용하여 네트워크 인터페이스에 IP 주소를 할당합니다. 명령행에서 다음을 입력하여 *ip 주소*를 어댑터의 IP 주소로 대체합니다.

   ```
   # ifconfig vcaN plumb ip 주소 up
   ```

   자세한 내용은 `ifconfig`(1M) 매뉴얼 페이지와 Solaris 설명서를 참조하십시오.

   - 재부팅 후에도 설정을 그대로 유지하려면 `/etc/`*hostname*`.vca`*N* 파일을 생성합니다. 여기서 *N*은 사용할 `vca` 인터페이스의 인스턴스 번호에 해당합니다.

     1 단계에 있는 예제의 `vca` 인터페이스를 사용하려면 `/etc/`*hostname*`.vca`*N* 파일을 생성합니다 . 여기서 *N* 은 본 예제에서 0 인 장치의 인스턴스 번호에 해당합니다 . 인스턴스 번호가 1 인 경우 파일 이름은 `/etc/`*hostname*`.vca1` 가 됩니다 .
   - 사용하지 않을 Sun Crypto Accelerator 4000 인터페이스를 위한 `/etc/`*hostname*`.vca`*N* 파일을 생성하지 마십시오.
   - `/etc/`*hostname*`.vca`*N* 파일은 적절한 `vca` 인터페이스에 대한 호스트 이름을 포함하고 있어야 합니다.

- 호스트 이름은 IP 주소를 가지고 있어야 하며 /etc/hosts 파일에 나열되어 있어야 합니다.
- 호스트 이름은 다른 어떤 인터페이스의 호스트 이름과 달라야 합니다. 예를 들어, /etc/*hostname*.vca0 및 /etc/*hostname*.vca1은 동일한 호스트 이름을 공유할 수 없습니다.

다음 예제는 Sun Crypto Accelerator 4000 보드를 가진 zardoz라는 시스템에 필요한 etc/*hostname*.vca*N* 파일을 보여줍니다(zardoz-11).

```
# cat /etc/ 호스트 이름 .hme0
zardoz
# cat /etc/ 호스트 이름 .vca0
zardoz-11
```

3. **각각의 활성화된** vca **인터페이스에 대해** /etc/hosts **파일에 적절한 항목을 생성합니다.**

예제:

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

IPsec 하드웨어 가속화 구성

이 보드에는 인라인과 대역 외의 두 가지 IPsec 하드웨어 가속화 구성이 있습니다. 두 구성 모두 IPsec 암호화 작업을 가속화합니다. 하지만 각 구성에 따라 이점이 다르므로 적절한 구성을 결정하려면 전체적인 시스템 요구 사항을 평가해야 합니다.

참고 – IPsec 가속화는 Solaris 9 이상에서 지원되며 Solaris 8에서는 지원되지 않습니다. 인라인 IPsec 가속화는 Solaris 9 12/03 이상에서만 지원됩니다(표 3-20 참조).

표 3-20 IPsec 가속화를 위한 Solaris 릴리스 요구 사항

Solaris 버전	대역 외 가속화	인라인 가속화
모든 Solaris 8 릴리스	지원되지 않음	지원되지 않음
Solaris 9에서 Solaris 9 8/03	지원됨	지원되지 않음
Solaris 9 12/03 이상	지원됨	지원됨

대역 외는 기본 IPsec 구성이며 멀티프로세서 시스템에서 성능이 최적화됩니다. 이 구성은 DES 및 3DES 암호화 작업을 보드로 덜어주며 호스트 처리 성능이 그다지 중요하지 않은 멀티프로세서 시스템에서 주로 사용되는 구성입니다.

인라인 IPsec 구성은 인증 지원(MD5 및 SHA1)을 통해 대역 외 기능을 증가시키며 호스트 패킷 처리의 일부를 보드로 덜어줍니다. 보드가 추가 패킷 처리를 담당하므로 호스트 CPU의 사용률을 크게 줄여줍니다.

참고 – 대역 외 구성은 DES나 3DES 암호화 알고리즘만 필요한 멀티프로세서 시스템의 인라인보다 IPsec 처리량이 높을 수 있습니다.

대역 외 IPsec 가속화 활성화

Solaris 9 이상이 필요합니다. 대역 외는 보드의 기본 구성입니다. Solaris 9에서 대역 외 IPsec 가속화를 위해 보드를 사용할 경우 IPsec 설정이나 튜닝이 필요하지 않습니다. Sun Crypto Accelerator 4000 패키지를 설치하고 재부팅하기만 하면 됩니다.

인라인 IPsec 가속화 활성화

Solaris 9 12/03 이상이 필요합니다. 인라인 가속화를 구성하려면 Solaris 소프트웨어 및 `vca` 드라이버의 구성 파일을 모두 변경해야 합니다.

▼ 인라인 IPsec 하드웨어 가속화 활성화

1. **Solaris 소프트웨어에서 인라인 가속화를 활성화하려면 다음 항목을** `/etc/system` **구성 파일에 추가합니다.**

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

`/etc/system` 파일의 변경 내용을 적용하려면 시스템을 재부팅해야 합니다.

2. **다음 항목을 `/kernel/drv/vca.conf` 구성 파일에 추가하여 `vca` 드라이버에서 인라인 가속화를 활성화합니다.**

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

`/kernel/drv/vca.conf` 파일의 변경 내용을 적용하려면 시스템을 재부팅하거나 `vca` 드라이버를 언로드하여 재로드해야 합니다.

참고 – Solaris 소프트웨어에 인라인 가속화가 활성화되어 있지 않으면 IPsec 이외의 기능의 성능을 저하시킬 수 있으므로 드라이버에서도 인라인 가속화를 활성화하지 않는 것이 좋습니다.

인라인 가속화를 활성화한 후에는 표준 IPsec 설정 절차에 따라 인터페이스에 Solaris 소프트웨어의 IPsec 정책을 설정할 수 있습니다. Solaris에서의 IPsec 정책 설정에 관한 내용은 `http://docs.sun.com`에서 *IPsec and IKE Administration Guide*를 참조하십시오.

인라인 가속화를 사용하면 AH 및 ESP 알고리즘을 모두 가속화할 수 있지만, 다중 중첩 변환(AH+ESP 포함)은 보드에서 수행할 수 없습니다. 다중 변환을 적용하면 인라인에서는 가장 외부에 있는 변환만 수행되며, 나머지 변환은 Solaris IPsec 구성에 의해 수행됩니다. Solaris 9 시스템에 KCL IPsec 가속화(`SUNWkcl2i.u`) 패키지가 설치되어 있으면 하드웨어(대역 외)에서도 위의 변환을 수행할 수 있습니다.

보드를 IPsec 인라인 가속화 용도로 구성하면 `kstat`(1M) 명령에서 제공하는 추가 통계가 증가합니다. IPsec 인라인 가속화 `kstat` 통계에 대한 설명은 표 3-19를 참조하십시오.

4 장

Sun Crypto Accelerator 4000 보드 관리

이 장에서는 vcaadm, vcad, vcadiag, pk11export 유틸리티를 사용하여 보드를 관리하는 방법을 간략하게 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

vcaadm 유틸리티 사용

vcaadm 유틸리티는 Sun Crypto Accelerator 4000 보드에 대한 명령행 인터페이스를 제공합니다. 보안 관리자로 지정된 사용자만 vcaadm 유틸리티를 사용할 수 있습니다. vcaadm으로 처음 Sun Crypto Accelerator 4000 보드에 연결하게 되면 초기 보안 관리자와 암호를 만드는 화면이 나타납니다.

vcaadm 유틸리티에 쉽게 액세스하려면 검색 경로 내에 다음 예제와 같이 Sun Crypto Accelerator 4000 도구 디렉토리를 넣습니다.

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

vcaadm 명령행 구문은 다음과 같습니다.

- vcaadm [-H]
- vcaadm [-y] [-h *호스트 이름*] [-p *port*] [-d vca*N*] [-f *파일 이름*]
- vcaadm [-y] [-h *호스트 이름*] [-p *port*] [-d vca*N*] [-s *보안 관리자*] *명령*

참고 – -d 속성을 사용하는 경우, vca*N*은 보드의 장치 이름이며 여기서 *N*은 Sun Crypto Accelerator 4000 장치 인스턴스 번호에 해당합니다.

표 4-1은 vcaadm 유틸리티의 옵션을 설명합니다.

표 4-1 vcaadm 옵션

옵션	의미
-H	vcaadm 명령에 대한 도움말 파일을 표시한 후 종료합니다.
-d vca*N*	드라이버 인스턴스 번호가 *N*인 Sun Crypto Accelerator 4000 보드에 연결합니다. 예를 들어, -d vca1은 장치 vca1에 연결되며, 여기서 vca는 보드 장치 이름에 있는 문자열이고 1은 장치의 인스턴스 번호입니다. 이 값의 기본값은 vca0이고 반드시 vca*N* 형식이어야 합니다. 여기서 *N*은 장치 인스턴스 번호에 해당합니다.
-f *파일 이름*	*파일 이름*에 있는 하나 이상의 명령을 해석한 후 종료합니다.
-h *호스트 이름*	*호스트 이름*에 있는 Sun Crypto Accelerator 4000 보드에 연결합니다. *호스트*의 값은 호스트 이름 또는 IP 주소가 될 수 있으며, 기본값은 루프백 주소입니다.
-p *포트*	*포트*의 Sun Crypto Accelerator 4000 보드에 연결합니다. *포트*의 기본값은 6870입니다.
-s *보안 관리자*	*보안 관리자*라는 이름의 보안 관리자로 로그인합니다.
-y	확인이 필요한 모든 프롬프트에 대해 '예'라고 답합니다.

참고 – *보안 관리자* 이름은 이 사용 설명서 전체에서 보안 관리자 이름의 예제로 사용됩니다.

작동 모드

vcaadm은 다음 세 가지 모드에서 실행될 수 있습니다. 이런 모드는 vcaadm에 전달되는 명령의 방법에 따라 달라집니다. 세 가지 모드는 단일 명령 모드, 파일 모드 및 대화형 모드입니다.

참고 – vcaadm을 사용하려면 보안 관리자 인증을 받아야 합니다. 보안 관리자 인증을 받아야 하는 횟수는 사용 중인 운영 모드에 따라 결정됩니다.

단일 명령 모드

단일 명령 모드에서는 모든 명령에 대해 보안 관리자 인증을 받아야 합니다. 명령이 실행되면 vcaadm에서 로그 아웃하게 됩니다.

단일 명령 모드에서 명령을 입력하는 경우에는 모든 명령행 스위치가 지정된 후 실행할 명령을 지정하게 됩니다. 예를 들어, 단일 명령 모드에서 다음 명령을 실행하면 지정된 키스토어 내의 모든 사용자를 표시하고 해당 사용자를 명령 쉘 프롬프트로 반환합니다.

```
$ vcaadm show user
Security Officer Name: 보안 관리자
Security Officer Password:
```

다음 명령은 보안 관리자인 *보안 관리자*로 로그인을 수행하고 키스토어에 사용자 *웹 관리자*를 생성합니다.

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

참고 – 첫 번째 암호는 보안 관리자용이고 그 다음은 새로운 사용자 *웹 관리자*의 암호 및 암호 확인입니다.

단일 명령 모드의 모든 출력은 표준 출력 스트림으로 이동합니다. 표준 UNIX 쉘 기반 방법으로 이 출력을 재지정할 수 있습니다.

파일 모드

파일 모드에서는 실행되는 각 파일에 대해 보안 관리자 인증을 받아야 합니다. 명령 파일의 명령이 실행된 후 사용자는 vcaadm에서 로그아웃됩니다.

파일 모드에서 명령을 입력하려면 vcaadm이 하나 이상의 명령을 읽어오는 파일을 지정합니다. 파일은 각 행마다 하나의 명령으로 구성된 ASCII 코드의 텍스트여야 합니다. 각 코멘트는 "#" 문자로 시작합니다. 파일 모드 옵션이 설정된 경우 vcaadm은 최종 옵션 이후의 모든 명령행 인수를 무시합니다. 다음 예제는 deluser.scr 파일에 있는 명령을 실행하고 모든 프롬프트에 "y"로 응답합니다.

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

대화형 모드

대화형 모드에서는 보드에 연결할 때마다 보안 관리자 인증을 받아야 합니다. 이것은 vcaadm의 기본적인 운영 모드입니다. 대화형 모드의 vcaadm에서 로그아웃하려면 logout명령을 사용합니다. 58페이지의 "vcaadm을 통한 로그인 및 로그아웃"을 참조하십시오.

대화형 모드는 한 번에 하나의 명령을 입력할 수 있는 ftp(1)와 유사한 인터페이스를 제공합니다. 대화형 모드에서는 -y 옵션이 지원되지 않습니다.

vcaadm을 통한 로그인 및 로그아웃

명령행에서 vcaadm을 사용하여 각각 -h, -p, -d 속성으로 *호스트*, *포트*, *장치*를 지정하게 되면, 네트워크 연결이 올바르게 수행된 경우 즉시 보안 관리자로 로그인하는 프롬프트가 나타납니다.

vcaadm 유틸리티는 특정 보드에서 실행 중인 vcaadm 응용 프로그램과 Sun Crypto Accelerator 4000 펌웨어 간에 암호화된 네트워크 연결(채널)을 설정합니다.

암호화된 채널을 설정하는 동안 보드는 하드웨어 이더넷 주소와 RSA 공개 키를 통해 서로 식별합니다. vcaadm이 처음 보드에 연결되면 트러스트 데이터베이스 ($HOME/.vcaadm/trustdb)가 생성됩니다. 이 파일에는 해당 보안 관리자에 의해 현재 트러스트 연결이 되어 있는 모든 보드가 포함됩니다.

vcaadm을 통해 보드에 로그인

보안 관리자가 새 보드에 연결하면 vcaadm은 보안 관리자에게 이를 통보하고 다음 옵션을 표시합니다.

```
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)
```

보안 관리자가 만일 원격 액세스 키가 변경된 보드에 연결한 경우 vcaadm은 보안 관리자에게 이를 통지하고 다음과 같이 세 가지 옵션을 표시합니다.

```
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
```

새 보드에 로그인

참고 – 이 장의 나머지 예제들은 대화형 모드의 vcaadm으로 작성되었습니다.

새 보드에 연결하면 vcaadm은 트러스트 데이터베이스에 새 항목을 생성해야 합니다. 다음은 새 보드에 로그인하는 예제입니다.

```
# vcaadm -h 호스트 이름
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 -->
```

변경된 원격 액세스 키가 있는 보드에 로그인

변경된 원격 액세스 키가 있는 보드에 연결하는 경우, vcaadm은 트러스트 데이터베이스에서 보드에 해당하는 항목을 변경해야 합니다. 다음은 변경된 원격 액세스 키가 있는 보드에 로그인하는 예제입니다.

```
# vcaadm -h 호스트 이름
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 *프롬프트*

대화형 모드에서 vcaadm 프롬프트는 다음과 같이 나타납니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> 명령
```

다음 표는 vcaadm 프롬프트 변수에 대한 설명입니다.

표 4-2 vcaadm 프롬프트 변수 정의

프롬프트 변수	정의
vca*N*	vca는 Sun Crypto Accelerator 4000 보드를 표시하는 문자열입니다. *N*은 보드의 장치 경로 이름에 속한 장치 인스턴스 번호(단위 주소)입니다. 장치의 인스턴스 번호를 확인하는 자세한 내용은 37페이지의 "vca.conf 파일을 사용한 드라이버 매개 변수 설정"을 참조하십시오.
호스트 이름	Sun Crypto Accelerator 4000 보드가 물리적으로 연결된 호스트 이름입니다. *호스트 이름*을 물리적 호스트의 IP 주소로 대체할 수 있습니다.
보안 관리자	보드에 현재 로그인되어 있는 보안 관리자의 이름입니다.

vcaadm을 통해 보드에서 로그아웃

대화형 모드에서 작업하는 경우, vcaadm을 완전히 종료하지 않은 상태에서 한 보드의 연결을 끊고 다른 보드에 연결할 수 있습니다. 보드의 연결을 종료하고 로그아웃한 후에도 대화형 모드를 지속하려면 logout 명령을 사용합니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> logout
vcaadm>
```

위 예제에서 vcaadm> 프롬프트에 더 이상 장치 인스턴스 번호, 호스트 이름 또는 보안 관리자 이름이 표시되지 않습니다. 다른 장치에 로그인하려면 다음 매개 변수 옵션과 함께 connect 명령을 입력합니다.

표 4-3 connect 명령 매개 변수 옵션

매개 변수	의미
dev vca*N*	드라이버 인스턴스 번호가 *N*인 Sun Crypto Accelerator 4000 보드에 연결합니다. 예를 들어, -d vca1은 장치 vca1에 연결하며, 기본값은 장치 vca0입니다.
host *호스트 이름*	*호스트 이름*에 있는 Sun Crypto Accelerator 4000 보드에 연결합니다 (기본값은 루프백 주소). *호스트 이름*을 물리적 호스트의 IP 주소로 대체할 수도 있습니다.
port *포트*	port *포트*의 Sun Crypto Accelerator 4000 보드에 연결합니다 (기본값은 6870).

예제

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> logout
vcaadm> connect host 호스트 이름 dev vca2
Security Officer Login: 보안 관리자
Security Officer Password:
vcaadm{vcaN@ 호스트 이름, 보안 관리자 }>
```

이미 Sun Crypto Accelerator 4000 보드에 연결되어 있는 경우 vcaadm에서 connect 명령을 실행할 수 없습니다. 먼저 로그아웃한 후 connect 명령을 실행해야 합니다.

새 연결이 활성화될 때마다 vcaadm과 대상 Sun Crypto Accelerator 4000 펌웨어는 전송되는 관리 데이터를 보호하기 위해 새로운 세션 키 재교섭을 수행합니다.

vcaadm을 통한 명령 입력

vcaadm 유틸리티에는 Sun Crypto Accelerator 4000 보드와 대화하는 데 사용해야 하는 명령 언어가 들어 있습니다. 명령은 명령의 전체 또는 일부(확실한 식별이 가능할 정도)를 사용하여 입력합니다. show 대신 sh를 사용하여 입력할 수 있으나, re만 입력할 경우에는 reset 또는 rekey에 모두 해당될 수 있으므로 의미가 모호합니다.

다음은 전체 단어를 사용하여 명령을 입력하는 예제입니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> show user
User                                              Status
------------------------------------------------------
web-admin                                        enabled
Tom                                               enabled
------------------------------------------------------
```

sh us와 같이 명령의 일부를 명령으로 사용해도 위 예제와 동일한 정보를 얻을 수 있습니다.

모호한 명령을 입력하면 다음과 같이 설명 메시지가 표시됩니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> re
Ambiguous command: re
```

명령어에 대한 도움말 보기

vcaadm에는 도움말 기능이 내장되어 있습니다. 도움말을 보려면 도움말이 필요한 명령어 다음에 물음표(?) 문자를 입력합니다. 전체 명령어를 입력하고 해당 행의 아무 곳에나 "?"를 입력하면, 아래 예제와 같이 명령어에 대한 구문이 표시됩니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> create ?
Sub-Command                       Description
------------------------------------------------------
so                                Create a new security officer
user                              Create a new user

vcaadm{vcaN@ 호스트 이름, 보안 관리자}> create user ?
Usage: create user [<username>]

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

vcaadm 프롬프트에서 물음표를 입력하여 다음 예제와 같이 모든 vcaadm 명령의 목록과 설명을 표시할 수 있습니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> ?
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
```

vcaadm 대화형 모드가 아닌 경우 "?" 문자는 현재 작업 중인 쉘에 의해 해석될 수 있습니다. 이런 경우에는 물음표를 입력하기 전에 반드시 명령 쉘 이스케이프 문자를 입력해야 합니다.

대화형 모드에서 vcaadm 유틸리티 종료

quit 및 exit 두 명령을 통해 vcaadm을 종료할 수 있습니다. Ctrl-D 키를 눌러도 vcaadm이 종료됩니다.

vcaadm을 통해 보드 초기화

Sun Crypto Accelerator 4000 보드 구성의 첫 번째 단계는 보드를 초기화하는 것입니다. 보드를 초기화할 때는 키스토어를 생성해야 합니다(참조100페이지의 "개념 및 용어"). vcaadm을 통해 처음 Sun Crypto Accelerator 4000 보드에 연결하면 새로운 키스토어 또는 백업 파일에 저장된 기존 키스토어를 사용하여 보드를 초기화하라는 메시지가 표시됩니다. vcaadm은 보드 초기화 형식에 상관 없이 이에 필요한 모든 정보를 묻습니다.

▼ 새 키스토어를 사용하여 보드 초기화

1. 보드가 설치된 시스템의 명령 프롬프트에서 vcaadm을 입력하거나, 원격 시스템인 경우 vcaadm -h *호스트 이름*을 입력한 후 1을 선택하여 보드를 초기화합니다.

```
# vcaadm -h 호스트 이름
Please select an action:

1. Abort this connection
2. Trust the board for this session only.
3. Replace the 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. 키스토어 이름을 생성합니다(68페이지의 "명명 요구 사항" 참조).

```
Keystore Name: 키스토어 이름
```

3. FIPS 140-2 모드 또는 비 FIPS 모드를 선택합니다.

FIPS 모드에서 보드는 FIPS 140-2, level 3을 준수합니다. FIPS 140-2는 사용자 조작 방지 및 강력한 데이터 무결성과 보안을 필요로 하는 미국 정보 처리 표준입니다. 다음 웹 사이트에서 FIPS 140-2 관련 문서를 참조하십시오.
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

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

4. **초기 보안 관리자 이름 및 암호를 생성합니다(68페이지의 "명명 요구 사항" 참조).**

```
Initial Security Officer Name: 보안 관리자
Initial Security Officer Password:
Confirm Password:
```

참고 – 필수 매개 변수를 삭제 또는 변경하거나, 예상치 못한 결과를 가져올 수도 있는 명령을 실행하기 전에 vcaadm은 사용자에게 Y, Yes, N 또는 No를 입력하여 확인하도록 합니다. 이 값은 대/소문자를 구분하지 않으며, 기본값은 No입니다.

5. **구성 정보를 확인합니다.**

```
Board initialization parameters:
-----------------------------------------------------
Initial Security Officer Name: 보안 관리자
Keystore name: 키스토어 이름
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.
```

기존 키스토어를 사용하여 보드 초기화

단일 키스토어에 여러 보드를 추가할 경우 모든 보드가 동일한 키스토어 정보를 사용하도록 초기화할 수 있습니다. 또한, Sun Crypto Accelerator 4000 보드를 원래의 키스토어 구성으로 복원할 수도 있습니다. 이 항목에서는 백업 파일에 저장된 기존 키스토어를 사용하여 보드를 초기화하는 방법을 설명합니다.

이 절차를 수행하기에 앞서 기존 보드 구성에 대한 백업 파일을 먼저 생성해야 합니다. 백업 파일을 생성하고 복원하려면 백업 파일의 데이터를 암호화하고 해독할 암호가 필요합니다(73페이지의 "마스터 키 백업" 참조).

▼ 기존 키스토어를 사용하여 보드 초기화

1. **Sun Crypto Accelerator 4000 보드가 설치된 시스템의 명령 프롬프트에서** vcaadm**을 입력하거나 원격 시스템인 경우** vcaadm -h *호스트 이름*을 **입력한 후 2를 선택하여 백업에서 보드를 복원합니다.**

```
# vcaadm -h 호스트 이름
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. **백업 파일의 경로와 암호를 입력합니다.**

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

3. **구성 정보를 확인합니다.**

```
Board restore parameters:
-----------------------------------------------------
Path to backup file: /tmp/board-backup
Keystore name: 키스토어 이름
-----------------------------------------------------

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

vcaadm을 통한 키스토어 관리

키스토어는 키 구성 요소의 리포지터리입니다. 키스토어는 보안 관리자 및 사용자와 연관되어 있습니다. 키스토어는 스토리지를 제공할 뿐만 아니라 사용자 계정이 키 객체를 소유할 수 있는 수단을 제공합니다. 키스토어를 이용하면 소유자로 인증되지 않은 응용 프로그램에서 키를 숨길 수 있습니다. 키스토어에는 세 가지 구성 요소가 있습니다.

- **키 객체 –** Sun ONE Web Server와 같은 응용 프로그램을 위해 저장된 장기 키
- **사용자 계정 –** 응용 프로그램이 특정 키를 인증하고 액세스하는 수단 제공
- **보안 관리자 계정 –** `vcaadm`을 통해 키 관리 기능에 액세스하는 수단 제공

참고 – 한 Sun Crypto Accelerator 4000 보드는 반드시 하나의 키스토어를 가지고 있어야 합니다. 추가 성능과 장애 허용을 위해 여러 보드가 같은 키스토어를 사용하도록 구성할 수 있습니다.

명명 요구 사항

보안 관리자 이름, 사용자 이름, 키스토어 이름은 다음 요구 사항을 만족해야 합니다.

표 4-4 보안 관리자 이름, 사용자 이름 및 키스토어 이름 요구 사항

이름 요구 사항	설명
최소 길이	최소 1자
최대 길이	사용자 이름 63자, 키스토어 이름 32자
유효 문자	영숫자, 밑줄(_), 대시(-), 마침표(.)
시작 문자	반드시 알파벳이어야 함

암호 요구 사항

암호 요구 사항은 `set passreq`의 현재 설정(`low`, `med`, `high`)에 따라 달라집니다.

암호 요구 사항 설정

`set passreq` 명령을 사용하여 Sun Crypto Accelerator 4000 보드에 대한 암호 요구 사항을 설정합니다. 이 명령은 `vcaadm`이 표시하는 모든 암호 프롬프트의 암호 문자 요구 사항을 설정합니다. 다음 표와 같이 암호 요구 사항 설정에는 세 가지가 있습니다.

표 4-5 암호 요구 사항 설정

암호 설정	요구 사항
`low`	암호 제한이 없습니다. 보드가 FIPS 모드에 있지 않은 경우의 기본값입니다.
`med`	최소 6자가 필요하며, 이 중 3자는 반드시 알파벳이고 1자는 알파벳이 아니어야 합니다. 이 설정은 보드가 FIPS 140-2 모드인 경우의 기본 설정으로, FIPS 140-2 모드에서 허용하는 최소 암호 요구 사항입니다.
`high`	최소 8자가 필요하며, 이 중 3자는 반드시 알파벳이고 1자는 알파벳이 아니어야 합니다. 이 설정은 기본값이 아니므로 수동으로 구성해야 합니다.

암호 요구 사항을 변경하려면 `set passreq` 명령을 입력한 다음 `low`, `med` 또는 `high`를 이어서 입력합니다. 다음 명령은 Sun Crypto Accelerator 4000 보드에 대한 암호 요구 사항을 `high`로 설정합니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> set passreq high

vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> set passreq
Password security level (low/med/high): high
```

키스토어에 보안 관리자 배치

하나의 키스토어에 대해 하나 이상의 보안 관리자가 있을 수 있습니다. 보안 관리자 이름은 Sun Crypto Accelerator 4000 보드 도메인 내에서만 인식되며 호스트 시스템의 사용자 이름과 같을 필요는 없습니다.

보안 관리자를 생성할 때 명령행에서 이름 매개 변수는 선택 사항입니다. 보안 관리자 이름을 생략하면 vcaadm은 해당 이름을 묻습니다(68페이지의 "명명 요구 사항" 참조).

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> create so 별칭
Enter new security officer password:
Confirm password:
Security Officer Alice created successfully.

vcaadm{vcaN@ 호스트 이름, 보안 관리자}> create so
New security officer name: Bob
Enter new security officer password:
Confirm password:
Security Officer Bob created successfully.
```

키스토어에 사용자 배치

이 사용자 이름은 Sun Crypto Accelerator 4000 보드의 도메인 내에서만 인식되며 웹 서버 프로세스를 실제로 실행할 UNIX 사용자 이름과 같을 필요는 없습니다.

사용자를 생성할 때 명령행에서 사용자 이름 매개 변수는 선택 사항입니다. 사용자 이름을 생략하면 vcaadm은 해당 사용자 이름을 묻습니다(68페이지의 "명명 요구 사항" 참조).

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> create user 웹 관리자
Enter new user password:
Confirm password:
User web-admin created successfully.

vcaadm{vcaN@ 호스트 이름, 보안 관리자}> create user
New user name: Tom
Enter new user password:
Confirm password:
User Tom created successfully.
```

사용자는 웹 서버 시작 시 인증할 때 이 암호를 사용해야 합니다.

주의 – 키에 액세스하려면 암호를 기억하고 있어야 합니다. 잊은 암호를 찾을 수 있는 방법은 없습니다.

참고 – 5분 이상 명령 입력이 없으면 사용자 계정은 로그아웃됩니다. 이 옵션은 변경이 가능합니다. 자세한 내용은 74페이지의 "자동 로그아웃 시간 설정"을 참조하십시오.

사용자 및 보안 관리자 목록 표시

키스토어와 연관된 사용자나 보안 관리자를 나열하려면 `show user` 또는 `show so` 명령을 입력합니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> show user
User                                            Status
------------------------------------------------------
web-admin                                       Enabled
Tom                                             Enabled
------------------------------------------------------


vcaadm{vcaN@ 호스트 이름, 보안 관리자}> show so
Security Officer
------------------------------------------------------
sec-officer
Alice
Bob
------------------------------------------------------
```

암호 변경

보안 관리자 암호만 `vcaadm`을 사용하여 변경할 수 있습니다. 보안 관리자는 자신의 암호를 직접 변경할 수 있습니다. `set password` 명령을 사용하여 보안 관리자 암호를 변경합니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> set password
Enter new security officer password:
Confirm password:
Security Officer password has been set.
```

사용자 암호는 Sun ONE Web Server `modutil` 유틸리티를 사용하여 PKCS#11 인터페이스를 통해 변경할 수 있습니다. 자세한 내용은 Sun ONE Web Server 설명서를 참조하십시오.

사용자 활성화 또는 비활성화

참고 – 보안 관리자는 비활성화할 수 없습니다. 일단 보안 관리자가 생성되면 삭제될 때까지 활성화된 상태를 유지합니다.

모든 사용자는 기본적으로 활성화 상태로 생성됩니다. 사용자는 비활성화할 수 있습니다. 비활성화된 사용자는 PKCS#11 인터페이스를 통해 키 구성 요소에 액세스할 수 없습니다. 비활성화된 사용자를 활성화하면 해당 사용자의 모든 키 요소에 대한 액세스가 복원됩니다.

사용자를 활성화하거나 비활성화할 때 명령행에서 사용자 이름 매개 변수는 선택 사항입니다. 사용자 이름을 생략하면 vcaadm은 해당 사용자 이름을 묻습니다사용자 계정을

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> disable user Tom
User Tom disabled.
vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> disable user
User name: 웹 관리자
User web-admin disabled.
```

비활성화하려면 disable user 명령을 입력합니다.

계정을 활성화하려면 enable user 명령을 입력합니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> enable user Tom
User Tom enabled.

vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> enable user
User name: 웹 관리자
User web-admin enabled.
```

사용자 삭제

delete user 명령을 실행하고 삭제할 사용자를 지정합니다. 사용자를 삭제할 때 명령행에서 사용자 이름 매개 변수는 선택 사항입니다. 사용자 이름을 생략하면 vcaadm은 해당 사용자 이름을 묻습니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> delete user 웹 관리자
Delete user web-admin? (Y/Yes/N/No) [No]: y
User web-admin deleted successfully.

vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> delete user
User name: Tom
Delete user Tom? (Y/Yes/N/No) [No]: y
User Tom deleted successfully.
```

보안 관리자 삭제

delete so 명령을 실행하고 삭제할 보안 관리자를 지정합니다. 보안 관리자를 삭제할 때 명령행에서 보안 관리자 이름 매개 변수는 선택 사항입니다. 보안 관리자 이름을 생략하면 vcaadm은 해당 보안 관리자 이름을 묻습니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> delete so Bob
Delete Security Officer Bob? (Y/Yes/N/No) [No]: y
Security Officer Bob deleted.

vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> delete so
Security Officer name: 별칭
Delete Security Officer Alice? (Y/Yes/N/No) [No]: y
Security Officer Alice deleted.
```

마스터 키 백업

키스토어는 디스크에 저장되고 마스터 키로 암호화됩니다. 마스터 키는 Sun Crypto Accelerator 4000 펌웨어에 저장되며 보안 관리자는 이를 백업할 수 있습니다.

마스터 키를 백업하려면 backup 명령을 사용합니다. backup 명령에는 백업이 저장될 백업 파일의 경로 이름이 있어야 합니다. 이 경로 이름은 명령행에 넣을 수 있으며, 생략할 경우 vcaadm에서 해당 경로 이름을 묻습니다.

백업 데이터에 대한 암호를 설정해야 합니다. 이 암호는 백업 파일에 있는 마스터 키를 암호화하기 위해 사용됩니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> 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.
```

주의 – 이 암호는 키스토어의 마스터 키를 보호하므로 백업 파일을 만들 때는 짐작하기 어려운 암호를 선택하는 것이 좋습니다. 입력한 암호도 반드시 기억해야 합니다. 암호가 없으면 마스터 키 백업 파일에 액세스할 수 없습니다. 잊은 암호를 찾을 수 있는 방법은 없습니다.

백업 방지를 위한 키스토어 잠금

보안 방침이 엄격한 사이트에서는 Sun Crypto Accelerator 4000 보드의 마스터 키가 하드웨어에서 추출되지 못하도록 할 수 있습니다. `set lock` 명령을 통해 이를 강제로 수행할 수 있습니다.

주의 – 이 명령을 실행한 후에는 모든 마스터 키 백업 시도가 실패하게 됩니다. 마스터 키를 다시 생성해도 잠금 상태는 지속됩니다. 이 설정을 취소하는 유일한 방법은 `zeroize` 명령으로 Sun Crypto Accelerator 4000 보드를 초기화하는 것입니다(78페이지의 "보드에서 소프트웨어 초기화 수행" 참조).

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> 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.
```

vcaadm을 통한 보드 관리

이 항목에서는 vcaadm 유틸리티로 Sun Crypto Accelerator 4000 보드를 관리하는 방법을 설명합니다.

자동 로그아웃 시간 설정

보안 관리자가 자동으로 보드에서 로그아웃되는 시간을 사용자 정의하려면 `set timeout` 명령을 사용합니다. 자동 로그아웃 시간을 변경하려면 `set timeout` 명령과 함께 보안 관리자가 자동으로 로그아웃되는 시간을 분 단위로 환산한 숫자를 입력합니다. 값이 0인 경우 자동 로그아웃 기능이 비활성화됩니다. 최대 대기값은 1,440분(1일)입니다. 새로 초기화된 보드는 기본값이 5분입니다.

다음 명령은 보안 관리자의 자동 로그아웃 시간을 10분으로 변경합니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> set timeout 10
```

보드 상태 표시

Sun Crypto Accelerator 4000 보드의 현재 상태를 확인하려면 `show status` 명령을 실행합니다. 이 명령은 보드의 하드웨어 및 펌웨어 버전, 네트워크 인터페이스의 MAC 주소 및 상태(활성/비활성, 속도, 이중 및 기타) 및 키스토어 이름과 ID를 표시합니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> 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: 키스토어 이름
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
----------------------------------------------------------------
```

FIPS 140-2 모드에서의 보드 작동 여부 확인

Sun Crypto Accelerator 4000 보드가 FIPS 140-2 모드에서 작동하고 있는 경우, `show status` 명령을 실행하면 다음 메시지가 표시됩니다.

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

보드가 FIPS 140-2 모드에서 작동하고 있지 않은 경우, `show status` 명령을 실행하면 FIPS 140-2 모드를 명시하는 메시지가 표시되지 않습니다.

또한 `kstat`(1M) 유틸리티를 사용해도 보드가 FIPS 140-2 모드에서 작동 중인지 확인할 수 있습니다. 보드가 FIPS 140-2 모드에서 작동 중인 경우 `kstat`(1M) 매개 변수인 `vs-mode`를 실행하면 `FIPS` 값을 반환합니다. 42페이지의 "암호화 및 이더넷 드라이버 운영 통계" 및 온라인 매뉴얼 페이지에서 `kstat`(1M)에 대한 내용을 참조하십시오.

새 펌웨어 로드

새 기능이 추가되면 Sun Crypto Accelerator 4000 보드의 펌웨어를 업데이트하여 이를 반영할 수 있습니다. 펌웨어를 로드하려면 `loadfw` 명령을 실행하고 펌웨어 파일에 대한 경로를 입력합니다.

펌웨어를 올바르게 업데이트하려면 `reset` 명령을 사용하여 보드를 수동으로 재설정해야 합니다. 보드를 재설정하게 되면 현재 로그인되어 있는 보안 관리자는 로그아웃됩니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> loadfw /opt/SUNWconn/cryptov2/firmware/sca4000fw
Security Officer Login: 보안 관리자
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
```

보드 재설정

특정 상황에서는 보드를 재설정해야 할 수도 있습니다. 이런 경우에는 `reset` 명령을 실행해야 합니다. 이 명령을 실행하면 사용자에게 작업 확인 메시지를 표시합니다. Sun Crypto Accelerator 4000 보드를 재설정하게 되면, 해당 보드의 작업을 대신 수행할 다른 활성화된 Sun Crypto Accelerator 4000 보드가 없을 경우 시스템의 암호화 가속화가 일시적으로 중단될 수 있습니다. 또한, 이 명령이 실행되면 vcaadm에서 자동으로 로그아웃되기 때문에 장치 관리를 계속 하려면 vcaadm에 다시 로그인하고 해당 장치에 다시 연결해야 합니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> 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.
```

보드 키 재생성

보안 방침이 바뀌면 마스터 키 또는 원격 액세스 키를 새 키로 교체하여 사용해야 합니다. rekey 명령을 통해 이러한 키 중 하나 또는 두 개 모두를 재생성할 수 있습니다.

마스터 키를 재생성하면 키스토어가 새 키로 재암호화되어 새 키스토어 파일로 이전의 백업 마스터 키 파일을 무효화시킵니다. 키를 재생성할 때마다 마스터 키를 백업합니다. 여러 Sun Crypto Accelerator 4000 보드가 동일한 키스토어를 사용하고 있는 경우에는 새 마스터 키를 백업하고 이를 다른 보드로 복원해야 합니다.

원격 액세스 키를 재생성하면 보안 관리자는 로그아웃되고 새 원격 액세스 키로 다시 연결해야 합니다.

rekey 명령을 실행할 때 세 가지 키 유형 중 하나를 지정할 수 있습니다.

표 4-6 키 유형

키 유형	작업
master	마스터 키를 재생성합니다.
remote	원격 액세스 키를 재생성합니다. 보안 관리자가 로그아웃됩니다.
all	마스터 키와 원격 액세스 키를 모두 재생성합니다.

다음 예제는 rekey 명령을 사용하여 all 유형의 키를 입력하는 것입니다.

```
vcaadm{vcaN@ 호스트 이름,보안 관리자}> 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.
```

보드에서 소프트웨어 초기화 수행

보드에서 모든 키 구성 요소를 제거하는 데는 두 가지 방법이 있습니다. 첫 번째 방법은 하드웨어 점퍼를 사용하는 것입니다. 이 방법은 보드를 출하 시 상태로 복원합니다 (failsafe 모드)(243페이지의 "Sun Crypto Accelerator 4000 하드웨어를 출하 시 상태로 초기화" 참조). 두 번째 방법은 `zeroize` 명령을 사용하는 것입니다.

참고 – `zeroize` 명령은 키 구성 요소만 삭제하고 업데이트된 펌웨어는 그대로 보존합니다. 이 명령은 또한 작업이 성공적으로 완료되면 보안 관리자가 로그아웃됩니다.

`zeroize` 명령으로 보드에서 소프트웨어를 초기화하려면 이 명령을 입력하고 확인합니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> 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.
```

vcaadm diagnostics 명령 사용

`vcaadm` 유틸리티 및 SunVTS 소프트웨어에서 진단을 수행할 수 있습니다. `vcaadm`에 있는 `diagnostics` 명령은 Sun Crypto Accelerator 4000 하드웨어의 세 가지 주요 항목인 일반 하드웨어, 암호화 하위 시스템 및 네트워크 하위 시스템을 진단합니다. 일반 하드웨어 테스트는 DRAM, 플래시 메모리, PCI 버스, DMA 컨트롤러 및 기타 내장 하드웨어를 테스트합니다. 암호화 하위 시스템 테스트는 난수 발생기와 암호화 가속기를 테스트합니다. 네트워크 하위 시스템 테스트는 `vca` 장치를 테스트합니다.

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자}> diagnostics
Performing diagnostic tests...Done.
Diagnostic Results
-----------------------------------------------------
General Hardware:                PASS
Cryptographic Subsystem:         PASS
Network Subsystem:               PASS
-----------------------------------------------------
```

vcad 명령 사용

vcad 명령은 vcad 데몬을 구성하고 시작하며, 이는 vcaadm(1M) 및 기타 암호화 응용 프로그램을 위한 암호화 키스토어 서비스를 제공합니다. 또한 vcad 데몬은 드라이버와 하드웨어의 키스토어 데이터 읽기 및 쓰기를 처리합니다.

vcad 명령에 쉽게 액세스하려면 검색 경로 내에 다음 예제와 같이 Sun Crypto Accelerator 4000 도구 디렉토리를 넣습니다.

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

vcad 명령의 명령행 구문은 다음과 같습니다.

/opt/SUNWconn/cryptov2/sbin/vcad [-dFlV] [-f *구성 파일*] [-h *호스트 주소*] [-k *키스토어 디렉토리*] [-L *로그 파일*] [-p *포트*] [-s *최대 크기*] [-t *초*][-u *사용자 이름*]

표 4-7은 vcad 명령에서 지원되는 옵션에 대한 설명입니다.

표 4-7 vcad 명령 옵션

옵션	설명
-d	디버깅 기능을 켭니다. 각 메시지에는 실제 메시지 내용과 함께 vcad의 프로세스 ID, 현재 스레드 ID 및 메시지 범주가 포함됩니다. -d 옵션을 여러 개 사용하면 로그의 표시 수준이 높아집니다(최대 2개). -d 옵션을 여러 개 사용할 경우, -d 하나는 구성 파일의 DebugLevel 매개 변수를 INFO로 설정하는 것과 동일하며 -dd는 DEBUG로 설정하는 것과 동일합니다.
-f *구성 파일*	구성 파일의 위치를 지정합니다. 구성 파일의 기본 위치는 /etc/opt/SUNWconn/vca/vcad.conf입니다. 이 옵션을 사용하여 파일이 열리지 않으면, vcad가 시작되지 않습니다.
-F	포그라운드에서 vcad를 수행하고 로그 출력을 stderr로 보냅니다. 이 동작은 -L 플래그로 선택한 *로그파일*을 덮어씁니다.
-h *호스트 주소*	vcad에서 바인딩할 호스트 IPv4 또는 IPv6 주소를 지정하고 수신 연결 요청을 수신 대기합니다. -h 옵션을 추가하여 둘 이상의 호스트 또는 IP 주소를 지정할 수 있습니다. -h 옵션을 사용하지 않으면 vcad는 사용 가능한 모든 인터페이스에서 수신 연결 요청을 수신 대기합니다. 바인딩할 특정 호스트 또는 IP 주소를 지정하면 이 주소와 localhost에 응답하는 인터페이스에만 연결이 설정됩니다. -h 플래그로 지정한 주소나 호스트는 모두 -l 옵션에 의해 무시됩니다.

표 4-7 vcad 명령 옵션*(계속)*

옵션	설명
-k *키스토어 디렉토리*	*키스토어 디렉토리*를 모든 키스토어 데이터의 디렉토리로 사용합니다. 수퍼유저가 아닌 데몬이 실행되는 경우, 키스토어 데이터 파일처럼 이 디렉토리도 해당 사용자가 읽고 쓸 수 있어야 합니다. 키스토어 데이터의 기본 디렉토리는 /etc/opt/SUNWconn/vca/keydata입니다.
-l	로컬 호스트상의 관리 클라이언트에서 보낸 수신 연결 요청만 수락합니다. 이 옵션은 다른 모든 인터페이스에서 데몬을 수신 대기하게 설정하는 명령행 또는 .conf 파일의 지시어보다 우선합니다.
-L *로그 파일*	로깅 출력을 시스템 로그의 표준 위치가 아닌 *로그 파일*로 보냅니다.
-p *포트*	수신 연결을 위해 *포트*를 사용하여 바인딩합니다. 기본 포트는 6870입니다.
-s *최대 크기*	데이터 길이가 최대 *최대 크기* 바이트인 명령을 Sun Crypto Accelerator에 전달할 수 있도록 합니다. 관리자는 이 기능을 사용하여 단일 명령으로 대량의 데이터가 커널을 통해 전송되는 것을 방지할 수 있습니다. 단일 명령 최대 크기의 기본값은 4MB(4194304 바이트)입니다.
-t *초*	vcad가 클라이언트에서 보내는 데이터를 기다리는 시간을 *초* 단위 수로 설정합니다. 이 시간을 초과하면 vcad와 클라이언트 간의 연결이 종료됩니다.
-u *사용자 이름*	vcad를 *사용자 이름*으로 수행합니다. 사용자 이름을 지정하지 않으면 vcad는 vcad를 시작한 사용자로 실행합니다. 사용자 이름을 지정했으나 해당 사용자 이름을 시스템에서 찾을 수 없는 경우에는 vcad가 시작되지 않습니다. vcad를 수퍼유저나 사용자 ID가 0인 다른 계정으로 실행하면 vcad가 경고 메시지를 표시합니다. 수퍼유저가 아닌 사용자로 vcad를 실행하는 것에 관한 권장 사항은 82페이지의 "vcad 데몬 보안"을 참조하십시오.
-V	vcad의 버전 정보를 표시합니다.

vcad 구성 파일

vcad 데몬은 구성 파일에서 운영 매개 변수를 가져옵니다. vcad 데몬을 실행하면 기본적으로 데몬은 /etc/opt/SUNWconn/vca/vcad.conf에서 구성 파일을 찾지만 다른 파일은 vcad 명령의 -f 플래그로 지정할 수도 있습니다. -f 플래그를 사용하지 않아 기본 구성 파일을 찾거나 읽을 수 없으면 vcad 데몬은 기본값을 모두 사용하여 시작하려 합니다. 이 경우 표준 오류 출력으로 경고 메시지가 전달됩니다.

구성 파일은 행 당 하나의 지시어를 포함합니다. 각 명령은 해당 명령과 연관된 값을 가져야 합니다. 코멘트를 사용할 수 있으며 반드시 # 문자로 시작해야 합니다. 지시어 이름은 대/소문자를 구분하지 않지만 지시어의 값은 대/소문자를 구분합니다. 자세한 내용은 표 4-8에서 각 지시어에 대한 설명을 참조하십시오.

구성 파일 지시어는 동일한 운영 매개 변수에 대해 명령행 옵션을 사용하는 것으로 대체될 수 있습니다. 예를 들어, "Port" 구성 파일 지시어는 -p 옵션으로 대체할 수 있습니다. 명령행 옵션 또는 구성 파일 지시어로 지정되지 않은 운영 매개 변수는 기본값을 사용합니다. 표 4-8은 vcad 명령에서 지원되는 명령행 지시어에 대한 설명입니다.

표 4-8 vcad 명령의 명령행 지시어

지시어	설명
DebugLevel *수준*	구성 파일에 세 가지 디버그 수준 중 하나를 설정할 수 있습니다. 세 가지 수준은 간략한 것에서 상세한 것의 순으로 알림, 정보 및 디버그입니다. 기본값은 알림 수준입니다.
HostBind *호스트 /IP*	vcad가 바인딩하고 수신 대기할 IPv4나 IPv6 주소 또는 호스트에서 확인할 대상 IP 주소를 지정합니다. 여러 HostBind 지시어를 사용하면 vcad가 하나 이상의 주소에서 수신 대기할 수 있습니다. 구성 파일에 HostBind 항목이 없으면 모든 인터페이스에서 연결을 수신 대기합니다. -l 명령행 플래그는 모든 HostBind 항목에 우선합니다.
KeyStoreDir *디렉토리*	관리자가 키스토어 파일을 저장할 대체 디렉토리를 선택할 수 있습니다. vcad를 실행할 사용자는 이 디렉토리에 대해 읽기 및 쓰기 권한이 있어야 합니다(사용자 지시어 참조). 키스토어 디렉토리의 기본 위치는 /etc/opt/SUNWconn/vca/keydata입니다.
LogFile *로그 파일*	*로그 파일*에 모든 로깅 데이터를 작성합니다. 기본적으로 로깅 데이터는 syslog에 작성됩니다. -F(포그라운드에서 실행) 명령행 플래그를 사용하면 이 지시어를 무시하고 vcad 로깅 데이터를 표준 오류 장치로 보냅니다.
MaxData *크기*	단일 명령으로 전송되는 데이터의 최대 허용 크기를 바이트 단위로 설정합니다. 기본적으로 이 값은 4MB(4194304 바이트)입니다. 전송 데이터가 이 값을 초과하면 vcad는 클라이언트에 오류를 반환하고 연결을 닫습니다.
Port *포트*	수신 대기 포트를 설정합니다. vcad가 수신 대기하는 기본 포트는 6870입니다. 관리자가 vcad를 권한을 부여받은 포트(보통 1024 미만의 포트)에서 수신 대기하도록 하려면 수퍼유저 권한을 가진 사용자로 vcad를 실행해야 합니다. 보안 관련 사항은 82페이지의 "vcad 데몬 보안"을 참조하십시오.
Timeout *초*	관리자가 명령 데이터의 첫 번째 바이트를 받은 이후의 해당 데이터의 시간 제한 값을 설정할 수 있습니다. 이 시간 제한 값은 읽기가 지연되었을 때 특정 카드에 대한 액세스가 잠기는 것을 막아줍니다. 이 시간 제한은 vcad가 연결된 클라이언트의 새 명령을 기다리고 있을 때는 적용되지 않습니다. 펌웨어 시간 제한 값에서 이 문제를 다룹니다(74페이지의 "자동 로그아웃 시간 설정" 참조). 기본 시간 제한은 300초(5분)입니다.
User *사용자 이름*	vcad를 username으로 실행하도록 설정합니다. 이 데몬은 실제 사용자 ID를 사용자 이름과 관련된 UID로 설정하려고 합니다. 이 지시어의 기본값은 vcad 프로세스를 시작한 사용자입니다.

vcad 데몬 보안

vcad 데몬은 TCP 포트에서 수신 대기하므로 특정 보안 권장 사항을 고려해야 합니다.

vcad를 실행할 때 수퍼유저 권한이 없는 사용자 ID 즉, UID0 계정이 아닌 다른 계정으로 실행해야 합니다. 네트워크에서 이 사용자 계정으로 직접 로그인해서는 안 됩니다. 이 계정은 암호가 없거나 암호가 잠금 상태여야 하고 로그인 쉘도 없어야 합니다. 이 계정에 대한 /etc/shadow 파일의 항목에는 NP 또는 *LK*를 갖게 됩니다.

기본적으로 vcad 데몬은 데몬 사용자 계정으로 시작하게 됩니다. 이 계정이 비활성화되어 있더라도 vcad 데몬은 올바르게 시작되지만 시스템에는 이 계정이 존재해야 합니다. 다른 사용자 이름으로 vcad를 실행하도록 수동으로 구성하려면 다음 단계를 수행합니다.

▼ 다른 사용자 이름으로 vcad 데몬을 실행하기 위한 구성

1. /dev/vcactl에 대한 읽기/쓰기 액세스를 설정합니다.

vcad 데몬은 /dev/vcactl와 직접 통신하여 명령 데이터를 전달하고 Sun Crypto Accelerator 4000 펌웨어에서 키스토어 I/O 명령을 가져옵니다. 권한과 소유권은 vcad가 실행되는 사용자 계정만 /dev/vcactl를 읽고 쓸 수 있게 설정해야 합니다. 기본적으로 소유자 읽기/쓰기 권한이 있는 데몬만 마이너 노드를 소유하도록 vcactl 모듈을 추가합니다. 이 권한을 변경하는 가장 안전한 방법은 rem_drv(1m) 및 add_drv(1m)를 사용하여 vcactl 모듈을 다시 등록하는 것입니다.

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

USER 및 GROUP 자리 표시자에는 장치 마이너 노드에 필요한 사용자 및 그룹 소유권을 포함시켜야 합니다. MODE는 장치의 마이너 노드에 사용할 파일 모드입니다. 0600은 vcactl 모듈의 권장 모드입니다. 자세한 내용은 add_drv(1m) 매뉴얼 페이지를 참조하십시오.

2. 키스토어에 대한 읽기/쓰기 액세스를 구성합니다.

vcad 데몬이 키스토어 I/O 동작을 수행하려면 데몬의 구성에서 지정된 키스토어 디렉토리에 액세스할 수 있어야 합니다. 키스토어 디렉토리의 읽기/쓰기/실행 권한은 vcad를 실행하는 사용자 계정만 사용할 수 있어야 합니다. 이 디렉토리의 키스토어 파일은 해당 사용자에게 읽기/쓰기 권한만 허용해야 합니다.

3. 권한이 없는 TCP 포트에서 vcad 데몬을 실행합니다.

vcad 데몬을 수퍼유저 권한으로 실행하지 않으면 권한이 있는 포트에 데몬을 바인딩할 수 없습니다. 일반적으로 1024 이상인 포트는 권한이 없는 포트입니다. 해당 시스템에서 tcp_smallest_nonpriv_port 매개 변수의 값이 1024가 아닌 경우 ndd를 사용하여 이 값을 결정합니다. 기본적으로 vcad 데몬은 6870 포트를 사용합니다.

예제

예제 1: vcad 데몬을 시작하고 5525 포트에서 수신 대기합니다.

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

예제 2: 추가 디버깅 정보와 함께 vcad 데몬을 시작하여 디버깅 정보를 화면에 내보냅니다.

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

이 방법으로 시작하면 데몬 시작 시 다음과 같은 출력이 생성됩니다.

```
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
```

vcad 데몬은 또한 두 가지 수준의 디버그 출력과 함께 실행될 때 연결이 새로 이뤄지거나 종료되면 이를 알려 줍니다.

예제 3: vcad 데몬을 시작하고 대체 구성 파일을 사용합니다.

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

vcadiag 유틸리티 사용

vcadiag 유틸리티는 수퍼유저가 보안 관리자 인증을 받지 않고 관리 업무를 수행할 수 있도록 Sun Crypto Accelerator 4000 보드에 대한 명령행 인터페이스를 제공합니다. 명령행 옵션은 vcadiag가 수행하는 작업을 결정합니다.

vcadiag 유틸리티에 쉽게 액세스하려면 검색 경로 내에 다음 예제와 같이 Sun Crypto Accelerator 4000 도구 디렉토리를 넣습니다.

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

vcadiag 명령행 구문은 다음과 같습니다.

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

참고 – [-DFKRZ] 옵션을 사용할 경우 vca*N*은 보드의 장치 이름이며, 여기서 *N*은 Sun Crypto Accelerator 4000 장치 인스턴스 번호에 해당합니다.

표 4-9 는 vcadiag 유틸리티에 지원되는 옵션입니다.

표 4-9 vcadiag 옵션

옵션	의미
-D vca*N*	Sun Crypto Accelerator 4000 보드에 진단을 수행합니다.
-F vca*N*	관리 세션을 보호하기 위해 Sun Crypto Accelerator 4000 보드가 사용하는 공개 키 지문을 표시합니다.
-K vca*N*	관리 세션을 보호하기 위해 Sun Crypto Accelerator 4000 보드가 사용하는 공개 키 및 공개 키 지문을 표시합니다.
-Q	Sun Crypto Accelerator 4000 장치 및 소프트웨어 구성 요소에 대한 정보를 제공합니다. 다음의 정보를 콜론으로 구분한 목록 형식으로 출력됩니다. • 장치 • 내부 기능 • 키스토어 이름 • 키스토어 일련 번호 • 키스토어 참조 횟수 이 옵션을 사용하여 장치와 키스토어 간의 관계를 확인할 수 있습니다.
-R vca*N*	보드를 재설정합니다.
-Z vca*N*	보드를 초기화합니다.

다음은 -D 옵션의 예제입니다.

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

다음은 -F 옵션의 예제입니다.

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

다음은 -K 옵션의 예제입니다.

```
# 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
```

다음은 -Q 옵션의 예제입니다.

```
# 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
```

다음은 -R 옵션의 예제입니다.

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

다음은 -Z 옵션의 예제입니다.

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

pk11export 유틸리티 사용

pk11export 유틸리티는 키 데이터베이스에서 키와 인증서를 추출해 PKCS#12에서 불러 올 수 있는 형식으로 저장합니다. 이 유틸리티에서는 개체를 추출한 다음 키와 인증서를 PKCS#12 파일에 저장하기 위해 PKCS#11 인터페이스가 필요합니다. 키와 인증서는 한 번에 한 쌍씩만 추출할 수 있습니다.

이 유틸리티는 동적 라이브러리 내에 해당 인터페이스가 들어 있는 경우 다른 PKCS#11 프로바이더에서도 작동합니다. pk11export 유틸리티는 다음 요구 사항이 충족되는 경우 PKCS#11 프로바이더를 통해 키를 내보냅니다.

- PKCS#11 인터페이스는 C_WrapKey PKCS#11 기능을 구현해야 합니다.
- PKCS#11 인터페이스는 CKM_DES3_CBC_PAD 및 CKM_SHA_1 PKCS#11 메커니즘을 구현해야 합니다.
- 내보낼 키에는 CKA_EXTRACTABLE 속성 집합이 있어야 합니다.

pk11export의 명령행 구문은 다음과 같습니다.

- /opt/SUNWconn/cryptov2/bin/pk11export -V
- /opt/SUNWconn/cryptov2/bin/pk11export -l [-p *pkcs11-라이브러리*]
- /opt/SUNWconn/cryptov2/bin/pk11export [-n *별칭*] [-o *파일 이름*] [-p *pkcs11-라이브러리*] *토큰 이름*

표 4-10은 pk11export 유틸리티에 지원되는 옵션입니다.

표 4-10 pk11export 옵션

옵션	설명
-l	해당 PKCS#11 라이브러리가 인식되는 사용 가능한 모든 토큰 목록을 나열합니다.
-n *별칭*	내보낼 키/인증서 쌍을 지정합니다. *별칭*은 문자열 값입니다.

표 4-10 pk11export 옵션*(계속)*

옵션	설명
-o *파일 이름*	내보내기 결과 생성된 PKCS#12 파일을 *파일 이름* 파일에 저장합니다. 출력 *파일 이름*을 지정하지 않으면 PKCS#12 파일은 pkcs12file이라는 파일 이름으로 현재 디렉토리에 저장됩니다.
-p *pkcs11-라이브러리*	키와 인증서를 추출할 PKCS#11 라이브러리를 지정합니다. 이 옵션에는 *pkcs11-라이브러리* 변수에 들어 있는 동적 라이브러리의 전체 경로를 입력해야 합니다. 기본적으로 pk11export는 Sun Crypto Accelerator 1000 PKCS#11 라이브러리 (/opt/SUNWconn/crypto/lib/libpkcs11.so)를 사용하지만, 모든 PKCS#11 라이브러리는 이 옵션에서 *pkcs11-라이브러리* 변수로 지정할 수 있습니다.
-V	pk11export의 버전 정보를 표시합니다.

예제

예제 1: PKCS#11 구현에 필요한 토큰을 나열합니다.

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

예제 2: PKCS#11 토큰 nobody@webserv에서 Server-Cert 인증서를 내보내 /tmp/webserv-export.p12 파일에 저장합니다.

```
example% pk11export -o /tmp/webserv-export.p12 nobody@webserv
Enter password for nobody@webserv:
Enter password for pkcs12 file:
Re-enter password for pkcs12 file:
/tmp/webserv-export.p12 was created successfully
```

iplssl cfg 스크립트 사용

iplssl cfg 스크립트의 옵션 1과 2는 모듈을 설치하여 보드를 구성하고 Sun ONE Web Server와 Application Server 소프트웨어에 보드를 등록합니다. 스크립트 옵션 3과 4는 Sun ONE Web Server 키를 PKCS#12 형식으로 내보내고 가져옵니다.

▼ Sun ONE Web Server 4.1의 iplssl cfg 스크립트 옵션 1 사용

- **108페이지의 "Sun ONE Web Server 4.1 구성"을 참조하십시오.**

▼ Sun ONE Web Server 6.0의 iplssl cfg 스크립트 옵션 1 사용

- **118페이지의 "Sun ONE Web Server 6.0 구성"을 참조하십시오.**

▼ iplssl cfg 스크립트 옵션 2 사용

1. **다음을 입력하여** iplssl cfg **스크립트를 실행합니다.**

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

2. **Sun ONE Application Server의 경우** 2**를 입력하고 바이너리 및 도메인 경로를 입력합니다.**

```
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. **0을 입력하여 종료합니다.**

▼ iplsslcfg 스크립트 옵션 3 사용

이 옵션은 Sun ONE Web Server 내부 데이터베이스에서 SSL 인증서와 키를 PKCS#12 형식으로 내보냅니다. 그런 다음 Sun Crypto Accelerator 4000 모듈로 다시 이 인증서를 가져올 수 있습니다.

1. **다음을 입력하여** `iplsslcfg` **스크립트를 실행합니다.**

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

2. **Sun ONE Web Server 키를 PKCS#12 형식으로 내보려면 3을 입력한 다음 [Return]을 누릅니다.**

```
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. **Sun ONE Server 디렉토리의 경로를 입력합니다.**

   iplsslcfg 유틸리티는 키를 내보낼 수 있는 인증서/키 데이터베이스를 모두 검색합니다.

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

4. **표시된 목록에서 이름을 선택하여 입력합니다.**

```
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. **내보낼 서버 인증서에 대한 별칭을 입력합니다.**

   이 이름은 기본적으로 Server-Cert입니다.

```
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. **PKCS#12 파일의 경로와 파일 이름을 지정합니다.**

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

7. **암호를 입력합니다.**

   인증이 성공적으로 완료되면 PKCS#12 파일의 암호를 설정하라는 메시지가 표시됩니다. 암호를 생성하면 PKCS#12 파일은 6단계에서 선택한 파일 이름으로 작성됩니다.

```
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. **0을 입력하여 종료합니다.**

▼ iplsslcfg 스크립트 옵션 4 사용

이 옵션은 PKCS#12 형식으로 키와 인증서를 보드로 가져옵니다.

1. **다음을 입력하여** iplsslcfg **스크립트를 실행합니다.**

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

2. **Sun ONE Web Server의 PKCS#12 형식에서 키를 가져오려면 4를 입력한 다음 [Return]을 누릅니다.**

```
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. **Sun ONE Server 디렉토리의 경로를 입력합니다.**

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

4. **가져올 PKCS#12 파일의 경로를 입력합니다.**

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

5. **다음 질문에 yes로 답합니다.**

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

6. **초기화 시 구성한 보드가 사용할 키스토어 이름을 입력합니다.**

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

7. ***사용자 이름*:*암호* 문자열을 입력하여 인증을 받습니다.** 표 5-1**을 참조하십시오.**

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

8. **PKCS#12 파일을 보호하기 위해 사용할 암호를 입력합니다.**

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

<Press ENTER to continue>
```

apsslcfg 스크립트 사용

apsslcfg 스크립트 옵션 1은 SSL용 Apache Web Server를 구성합니다. 옵션 2는 Apache Web Server의 키를 구성합니다.

참고 – apsslcfg 스크립트는 Apache Web Server 1.3.26만 지원합니다.

▼ apsslcfg 스크립트 옵션 1 사용

- **170페이지의 "Apache Web Server 1.3x 구성"을 참조하십시오.**

apsslcfg 스크립트 옵션 2 사용

옵션 2에는 다음 세 가지 하위 옵션이 있습니다.

1. Apache용 키 쌍 생성 및 인증서 요청
2. Apache(PEM으로 인코딩된 X.509) 키를 PKCS#12 형식으로 내보내기
3. PKCS#12 형식에서 Apache(PEM으로 인코딩된 X.509)로 키를 가져오기

▼ Apache용 키 쌍 생성 및 인증서 요청

이 옵션은 RSA 키 및 인증 기관(CA)에 제출할 인증서 요청을 작성합니다.

1. **1을 입력하여 옵션을 선택합니다.**
2. **바이너리와 Apache 모듈의 경로 및 구성 파일의 경로를 입력합니다.**

```
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. **키의 경로를 입력합니다.**

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

4. **키 및 인증서 요청 파일의 기본 이름을 입력합니다.**

   이 이름은 파일 이름에 덧붙여집니다. 예를 들어, `cert1`을 선택하면 키 파일 이름은 `cert1-key.pem`, 인증서 요청 파일 이름은 `cert1-certreq.pem`이 됩니다.

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

5. **생성할 RSA 키의 크기를 선택합니다.**

   비트 크기를 선택하면 RSA 키가 생성됩니다.

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

6. **키 파일을 암호화할 암호를 입력합니다.**

   암호는 되도록 어려운 암호를 사용하고 잊어버리지 않도록 합니다.

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

7. **인증서 요청에 필요한 인증서 이름을 입력합니다.**

인증서 요청은 인증 기관(CA)에 보낼 파일에 작성됩니다.

```
-----
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) []: 회사
Organizational Unit Name (eg, section) []: 부서
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>
```

▼ Apache(PEM으로 인코디된 X.509) 키를 PKCS#12 형식으로 내보내기

이 옵션을 사용하면 Apache Web Server 키와 인증서를 PKCS#12 파일에 저장할 수 있습니다.

1. **이 옵션을 선택하려면 2를 입력합니다.**
2. **키와 인증서 파일의 경로를 입력합니다.**

   키와 인증서 파일이 서로 동일하면 같은 경로를 두 번 입력합니다.

참고 – 키와 인증서 데이터는 동일한 파일에 저장할 수도 있고 다른 파일에 저장할 수도 있습니다. 하지만 다른 파일에 저장하더라도 파일 이름은 같아야 합니다.

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

3. **PKCS#12 출력 파일의 경로를 입력합니다.**

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

4. **인증서에 대한 별칭을 입력합니다.**
   이 이름은 인증서/키 쌍을 고유하게 식별합니다.

```
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. **PCKS#12 파일에 저장될 키를 보호할 암호를 입력합니다.**

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

6. **PKCS#12 파일의 키 데이터를 보호할 암호를 입력합니다.**
   PKCS#12 파일은 위에서 지정한 파일에 작성됩니다.

```
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>
```

▼ PKCS#12 형식에서 Apache(PEM으로 인코딩된 X.509)로 키 가져오기

이 옵션을 사용하면 PKCS#12 파일에서 키와 인증서를 추출하여 Apache Web Server에서 사용할 수 있습니다.

1. **3을 입력하여 옵션을 선택합니다.**

2. **PKCS#12 파일의 경로와 파일 이름을 입력합니다.**

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

3. **추출된 키와 인증서의 경로를 입력합니다.**

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

4. **키와 인증서 파일의 파일 이름을 입력합니다.**

   암호화된 키와 인증서는 모두 동일한 파일에 저장됩니다.

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

5. **PKCS#12 파일을 보호하기 위해 사용할 암호를 입력합니다.**

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

6. **Apache에서 읽을 수 있는 형식으로 추출된 키 파일을 보호할 새 암호를 입력합니다.**

   키와 인증서 데이터는 4단계에서 지정한 파일에 작성됩니다.

```
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>
```

같은 서버에 설치된 여러 보드에 다른 MAC 주소 할당

한 서버의 여러 보드에 다른 MAC 주소를 할당하는 방법은 두 가지가 있습니다. 첫 번째 방법은 운영 체제 수준에서, 두 번째는 OpenBoot PROM(OBP) 수준에서 수행합니다.

▼ 터미널 창에서 다른 MAC 주소 할당

1. **다음 명령을 입력합니다.**

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

참고 – `local-mac-address?` 매개 변수가 `true`로 설정된 경우 모든 비통합 네트워크 인터페이스 장치는 출하 시 제품에 할당된 로컬 MAC 주소를 사용합니다.

2. **시스템을 재부팅합니다.**

▼ OpenBoot PROM 수준에서 다른 MAC 주소 할당

1. **OpenBoot PROM** `ok` **프롬프트에서 다음 명령을 입력합니다.**

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

참고 – `local-mac-address?` 매개 변수가 `true`로 설정된 경우 모든 비통합 네트워크 인터페이스 장치는 출하 시 제품에 할당된 로컬 MAC 주소를 사용합니다.

2. **운영 체제를 부팅합니다.**

5 장

Sun ONE 서버 소프트웨어 설치 및 구성

이 장에서는 Sun ONE 서버와 함께 사용하기 위한 Sun Crypto Accelerator 4000 보드의 구성 방법을 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

참고 – 본 설명서에서 설명하는 Sun ONE 서버의 이전 이름은 iPlanet™ 서버였습니다.

Sun ONE Web Server를 위한 보안 관리

이 항목에서는 Sun ONE Web Server로 관리할 경우 Sun Crypto Accelerator 4000 보드의 보안 기능에 대한 개요를 설명합니다.

참고 – 키스토어를 관리하려면 해당 시스템에 대한 관리자 권한이 있는 관리자 계정을 가지고 있어야 합니다.

개념 및 용어

Sun ONE Web Server와 같은 PKCS#11 인터페이스를 통해 Sun Crypto Accelerator 4000 보드와 통신하는 응용 프로그램이 사용할 키스토어와 사용자를 생성해야 합니다.

참고 – Apache Web Server(6장)는 이 장에서 설명하는 키스토어 또는 사용자 계정 기능을 사용하지 않습니다.

Sun Crypto Accelerator 4000 보드 컨텍스트 내에서는 암호화 키 생성 요소를 사용자가 소유합니다. 각 키는 한 명의 사용자만 소유할 수 있으며, 각 사용자는 다수의 키를 소유할 수 있습니다. 사용자는 `production` 키와 `development` 키 같이 (사용자가 지원하는 소속 기관에 따라)서로 다른 구성에 사용할 여러 개의 키를 소유할 수 있습니다.

참고 – *사용자* 또는 *사용자 계정*이라는 용어는 `vcaadm`에서 생성된 Sun Crypto Accelerator 4000 사용자를 말하며, 일반적인 UNIX 사용자 계정을 의미하지 않습니다. UNIX 사용자 이름과 Sun Crypto Accelerator 4000 사용자 이름은 상호 관련이 없습니다.

키스토어는 키 구성 요소의 리포지터리입니다. 키스토어는 보안 관리자 및 사용자와 연관되어 있습니다. 키스토어는 스토리지를 제공할 뿐만 아니라 사용자 계정이 키 객체를 소유할 수 있는 수단을 제공합니다. 키스토어를 이용하면 소유자로 인증되지 않은 응용 프로그램에서 키를 숨길 수 있습니다. 키스토어에는 세 가지 구성 요소가 있습니다.

- **키 객체 –** Sun ONE Web Server와 같은 응용 프로그램을 위해 저장된 장기 키
- **사용자 계정 –** 응용 프로그램이 특정 키를 인증하고 액세스하는 수단 제공
- **보안 관리자 계정 –** `vcaadm`을 통해 키 관리 기능에 액세스하는 수단 제공

참고 – 한 Sun Crypto Accelerator 4000 보드는 반드시 하나의 키스토어를 가지고 있어야 합니다. 추가 성능과 장애 허용 기능을 위해 여러 Sun Crypto Accelerator 4000 보드가 같은 키스토어를 사용하도록 구성할 수 있습니다.

일반적인 설치에서는 세 명의 사용자를 가진 단일 키스토어를 포함하고 있습니다. 예를 들어, 이와 같은 구성에서는 *sca4000-ks-1*이라는 단일 키스토어가 포함될 수 있으며 이 키스토어에는 *webserv*, *dirserv* 및 *mailserv*라는 세 명의 사용자가 들어 있을 수 있습니다. 이를 통해서 이 세 명의 사용자는 이 키스토어 내에서 자신들의 서버 키에 대한 액세스 제어 권한을 소유하고 제어할 수 있게 됩니다. 그림 5-1은 일반적인 설치의 개요를 나타냅니다.

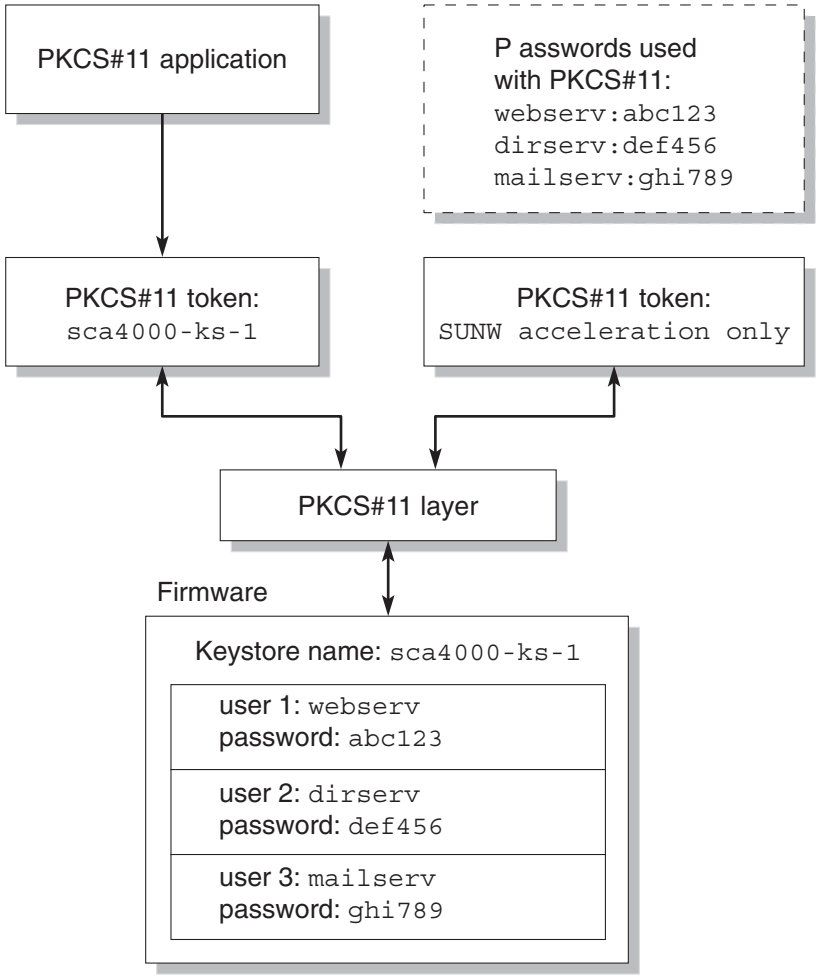

그림 5-1 키스토어 및 사용자 개요

관리 도구인 vcaadm은 Sun Crypto Accelerator 4000 키스토어와 사용자를 관리하기 위해 사용됩니다. 67페이지의 "vcaadm을 통한 키스토어 관리"를 참조하십시오.

토큰 및 토큰 파일

Sun ONE Web Server에서는 *키스토어*가 *토큰*으로 나타납니다. 토큰 파일은 Sun Crypto Accelerator 4000 관리자가 해당 응용 프로그램에 특정 토큰을 선택적으로 제공할 수 있게 해줍니다.

예제

만일 세 개의 키스토어 *engineering*, *finance* 및 *legal*을 생성하면 Sun ONE Web Server에는 기본적으로 다음과 같이 세 개의 토큰을 제공합니다.

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

토큰 파일

기본 설정을 덮어쓰려면 토큰 파일이 있어야 합니다. 일부 응용 프로그램은 여러 토큰을 취급할 수 없습니다. 토큰 파일은 각 행별로 하나 이상의 토큰 이름을 포함한 텍스트 파일입니다.

참고 – 토큰 이름과 키스토어 이름은 같습니다.

Sun ONE Web Server는 토큰 파일에 나열된 토큰만 제공합니다. 토큰 파일을 지정하는 방법은 다음과 같습니다(순서대로).

1. 환경 변수 `SUNW_PKCS11_TOKEN_FILE`에 명명된 파일

   일부 응용 프로그램 소프트웨어에서는 환경 변수가 숨겨져 있습니다 . 이러한 경우에는 이 방법을 사용할 수 없습니다 .

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

   이 파일은 Sun ONE Web Server 를 실행하는 UNIX 사용자의 홈 디렉토리에 있어야 합니다 . 홈 디렉토리가 없는 UNIX 사용자로 Sun ONE Web Server 가 실행되는 경우에는 이 방법을 사용할 수 없습니다 .

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

토큰 파일이 없는 경우 Sun Crypto Accelerator 4000 소프트웨어는 Sun ONE Web Server에 모든 토큰을 제공합니다.

다음은 토큰 파일의 예제입니다.

```
================================
# 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.

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

참고 – 주석은 샵(#) 표시로 시작되며 빈 행도 가능합니다.

위의 파일이 없는 경우에는 102페이지의 "토큰 및 토큰 파일"에 설명된 기본 방법이 사용됩니다.

대량 암호화 활성화 및 비활성화

SunONE 소프트웨어의 대량 암호화 기능은 기본적으로 비활성화되어 있습니다. 대용량 파일을 안전하게 전송하기 위해 이 기능을 활성화할 수도 있습니다.

Sun Crypto Accelerator 4000 보드에서 Sun ONE 서버 소프트웨어가 대량 암호화 기능을 사용할 수 있도록 하려면 `/etc/opt/SUNWconn/cryptov2/` 디렉토리에 `sslreg`이란 이름의 빈 파일을 생성한 후 서버 소프트웨어를 재시작합니다.

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

대량 암호화 기능을 비활성화하려면 `sslreg` 파일을 삭제한 후 서버 소프트웨어를 다시 시작해야 합니다.

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

Sun ONE Web Server 구성

이 항목에서는 다음을 설명합니다.

암호

Sun ONE Web Server를 작동하는 과정에서 여러 암호를 입력하도록 요청을 받게 됩니다. 표 5-1에 각 암호에 대한 설명이 나와 있습니다. 이러한 암호는 이 장 전체에서 언급됩니다.

표 5-1 Sun ONE Web Server에 필요한 암호

암호 유형	설명
Sun ONE Web Server 관리 서버	Sun ONE Web Server 관리 서버를 시작하는 데 필요합니다. 이 암호는 Sun ONE Web Server를 설정하는 과정에서 할당됩니다.
Web Server 트러스트 데이터베이스	보안 모드에서 실행할 경우 내부 암호화 모듈을 시작하는 데 필요합니다. 이 암호는 Sun ONE Web Server 관리 서버를 통해 트러스트 데이터베이스를 작성할 때 할당됩니다. 이 암호는 또한 인증서를 요청하고 이를 내부 암호화 모듈에 설치할 경우에도 필요합니다.
보안 관리자	`vcaadm` 권한이 있는 작업 수행 시 필요합니다.
사용자 이름:암호	보안 모드에서 실행할 경우 Sun Crypto Accelerator 4000 모듈을 시작하는 데 필요합니다. 이 암호는 또한 인증서를 요청하고 이를 내부 암호화 모듈에 설치할 경우에도 필요합니다(*keystore_name*). 암호는 `vcaadm`에서 생성된 키스토어 사용자의 *사용자 이름*과 *암호*로 구성됩니다. 키스토어 *사용자 이름*과 *암호*는 콜론(:)으로 구분합니다.

키스토어 배치

Sun ONE Web Server와 함께 사용하기 위해 보드를 활성화하기 전에 먼저 보드를 초기화하고 보드의 키스토어에 적어도 한 명의 사용자를 배치해야 합니다. 보드의 키스토어는 초기화 과정 중 생성됩니다. 기존 키스토어를 사용하도록 Sun Crypto Accelerator 4000 보드를 초기화할 수도 있습니다. 64페이지의 "`vcaadm`을 통해 보드 초기화"를 참조하십시오.

참고 – Sun Crypto Accelerator 4000 보드 당 하나의 키스토어만 구성할 수 있으며 보드 당 하나의 키스토어를 구성해야 합니다. 추가 성능과 장애 허용을 위해 여러 Sun Crypto Accelerator 4000 보드가 같은 키스토어를 사용하도록 구성할 수 있습니다.

▼ 키스토어 배치

1. **다음 예와 같이 Sun Crypto Accelerator 4000 도구 디렉토리를 검색 경로 내에 넣습니다 (넣지 않은 경우).**

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

2. **vcaadm 명령을 사용하여 vcaadm 유틸리티에 액세스하거나 vcaadm -h *호스트 이름* 을 입력하여 vcaadm을 원격 호스트에 있는 보드에 연결합니다.**

   55페이지의 "vcaadm 유틸리티 사용"을 참조하십시오.

```
$ vcaadm -h 호스트 이름
```

3. **보드 키스토어에 사용자를 배치합니다.**

   이 사용자 이름은 Sun Crypto Accelerator 4000 보드의 도메인 내에서만 인식되며 웹 서버 프로세스를 실제로 실행할 UNIX 사용자 이름과 같을 필요는 없습니다. 사용자를 생성하기 전에 반드시 vcaadm 보안 관리자로 로그인해야 합니다.

4. **create user 명령으로 사용자를 생성합니다.**

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> create user 사용자 이름
Initial password:
Confirm password:
User username created successfully.
```

   여기서 생성된 *사용자 이름*과 *암호*는 합해져서 *사용자 이름:암호*가 됩니다(표 5-1 참조). 사용자는 웹 서버 시작 시 인증할 때 이 암호를 사용해야 합니다. 이 암호는 단일 사용자의 키스토어 암호입니다.

주의 – 사용자는 반드시 이 *사용자 이름:암호*를 기억해야 합니다. 이 암호가 없으면 해당 키에 액세스할 수 없습니다. 잊은 암호를 찾을 수 있는 방법은 없습니다.

5. vcaadm**을 종료합니다.**

```
vcaadm{vcaN@ 호스트 이름, 보안 관리자 }> exit
```

Sun ONE Web Server 활성화 개요

Sun ONE Web Server를 활성화하려면 다음 절차를 완료해야 합니다. 이에 대한 자세한 내용은 다음 항목에서 설명합니다.

1. Sun ONE Web Server 설치
2. 트러스트 데이터베이스 생성
3. 인증서 요청
4. 인증서 설치
5. Sun ONE Web Server 구성

주의 – 위의 절차는 반드시 순서대로 수행해야 합니다. 그렇지 않으면 구성이 잘못될 수 있습니다.

- Sun ONE Web Server 4.1을 사용하는 경우 107페이지의 "Sun ONE Web Server 4.1 설치 및 구성"을 참조하십시오.
- Sun ONE Web Server 6.0을 사용하는 경우 117페이지의 "Sun ONE Web Server 6.0 설치 및 구성"을 참조하십시오.

재부팅 시 무인 시작되도록 Sun ONE Web Server 구성

암호화된 키를 사용하여 Sun ONE Web Server가 재부팅 될 때 사용자의 개입 없이 자동으로 시작되도록 구성할 수 있습니다.

▼ 재부팅 시 Sun ONE Web Server의 자동 시작을 위한 암호화 키 생성

1. Sun ONE Web Server 인스턴스의 config **하위 디렉토리로 이동합니다 (예:** /usr/iplanet/servers/https-*webserver 인스턴스 이름*/config**).**

2. **다음 행만을 포함한** `password.conf` **파일을 생성합니다(암호 정의는** 표 5-1 **참조).**

```
internal: 트러스트 데이터베이스 암호
키스토어 이름: 사용자 이름: 암호
```

3. **암호 파일의 파일 소유권을 서버가 운영하는 UNIX 사용자 ID로 설정하고 파일 소유자만이 읽을 수 있도록 권한을 설정합니다.**

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

Sun ONE Web Server 4.1 설치 및 구성

이 항목에서는 Sun ONE Web Server 4.1이 보드를 사용하도록 하기 위해 소프트웨어를 설치 및 구성하는 방법에 대해 설명합니다. 절차는 반드시 순서대로 수행해야 합니다. Sun ONE Web Server 설치 및 사용 방법에 대한 자세한 내용은 Sun ONE Web Server 설명서를 참조하십시오. 이 항목은 다음 절차를 설명합니다.

▼ Sun ONE Web Server 4.1 설치

1. **Sun ONE Web Server 4.1 소프트웨어를 다운로드합니다.**

   웹 서버 소프트웨어는 다음 URL에서 다운받을 수 있습니다.
   `http://www.sun.com/`

2. **설치 디렉토리로 변경하고 웹 서버 소프트웨어를 추출합니다.**

3. **명령행에서** `setup` **스크립트를 사용해 웹 서버를 설치합니다.**

   이 서버의 기본 경로 이름은 `/usr/netscape/server4`입니다.

   이 장에서는 이 기본 경로를 사용합니다. 웹 서버 소프트웨어를 다른 위치에 설치하려면 설치한 위치를 기록해 두는 것이 좋습니다.

```
# ./setup
```

4. **설치 스크립트의 프롬프트에 응답합니다.**

   다음 프롬프트 이외에는 기본값을 그대로 사용할 수 있습니다.

   a. `yes`**를 입력하여 라이센스 약관에 동의합니다.**

   b. **정식 도메인 이름을 입력합니다.**

   c. **Sun ONE Web Server 4.1 관리 서버 암호를 두 번 입력합니다.**

   d. **프롬프트가 나타나면 [Return]을 누릅니다.**

Sun ONE Web Server 4.1 구성

다음은 웹 서버 인스턴스에 대한 트러스트 데이터베이스를 생성하고 웹 서버로 보드를 등록하며 서버 인증서를 생성 및 설치할 뿐 아니라, SSL을 위해 웹 서버를 구성하는 절차입니다.

Sun ONE Web Server 관리 서버는 구성 프로세스 중에 반드시 실행 중이어야 합니다.

▼ 트러스트 데이터베이스 생성

1. **Sun ONE Web Server 4.1 관리 서버를 시작합니다.**

   `setup` 요청에 따라 `startconsole`을 실행하지 말고 다음 명령을 사용하여 Sun ONE Web Server 4.1 관리 서버를 시작합니다.

```
# /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
```

   서버에 연결하기 위한 URL이 응답으로 제공됩니다.

2. **웹 브라우저를 열고 다음을 입력하여 관리 GUI(Graphical User Interface)를 시작합니다.**

   http:// *호스트 이름.도메인:관리 포트*

   인증 대화 상자에서 `setup` 실행 중 선택한 Sun ONE Web Server 4.1 관리 서버의 사용자 이름과 암호를 입력합니다.

   참고 – Sun ONE Web Server 설치 시 기본 설정을 사용한 경우 사용자 ID 또는 Sun ONE Web Server 4.1 관리 서버 사용자 이름에 **admin**을 입력합니다.

   ---

3. **[OK(확인)]를 선택합니다.**

   Sun ONE Web Server 4.1 관리 서버 창이 나타납니다.

4. **웹 서버 인스턴스에 대한 트러스트 데이터베이스를 생성합니다.**

   a. **Sun ONE Web Server 4.1 관리 서버 창에서 [Servers(서버)] 탭을 누릅니다.**

   b. **서버를 선택한 다음 [Manage(관리)] 단추를 누릅니다.**

   c. **페이지의 상단 부분에 있는 [Security(보안)] 탭을 누르고 [Create Database(데이터베이스 생성)] 링크를 선택합니다.**

   d. **두 개의 대화 상자에 암호(웹 서버 트러스트 데이터베이스,** 표 5-1 **참조)를 입력하고 [OK(확인)]를 선택합니다.**

      8개 이상의 문자로 된 암호를 선택합니다. Sun ONE Web Server를 보안 모드로 실행할 경우 이 암호를 사용하여 내부 암호화 모듈을 시작합니다.

      하나 이상의 웹 서버 인스턴스에 대해 보안을 활성화할 수 있습니다. 이 경우에는 각 웹 서버 인스턴스에 대해 1단계 ~ 4단계를 반복합니다.

   참고 – Sun ONE Web Server 4.1 관리 서버에서 SSL(Secure Socket Layer)을 실행하는 경우에도 트러스트 데이터베이스의 설정 절차는 유사합니다. 자세한 내용은 `http://docs.sun.com`에서 *iPlanet Web Server, Enterprise Edition Administrator's Guide*를 참조하십시오.

▼ Web Server에 보드 등록

1. **다음 스크립트를 실행하여 Web Server에 보드를 등록합니다.**

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

이 스크립트는 웹 서버를 선택하고 선택한 Sun ONE 서버를 위한 Sun Crypto Accelerator 4000 암호화 모듈을 설치하라는 메시지를 표시합니다. 그런 다음 스크립트는 구성 파일을 업데이트하여 보드를 활성화합니다.

2. **Sun ONE Web Server가 SSL을 사용할 수 있도록 구성하려면 1을 입력한 다음 [Return]을 누릅니다.**

참고 – 여기서는 이 프롬프트에서 1 옵션을 선택하는 경우에 대한 절차를 설명합니다. 2, 3 또는 4 옵션을 선택하려면 88페이지의 "iplsslcfg 스크립트 사용"을 참조하십시오.

```
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. **프롬프트가 나타나면 웹 서버 루트 디렉토리의 경로를 입력한 다음 [Return]을 누릅니다.**

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

4. **프롬프트가 나타나면 y를 입력한 다음 [Return]을 누릅니다.**

```
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. **0을 입력하여 종료합니다.**

▼ 서버 인증서 생성

1. **다음 명령을 입력하여 Sun ONE Web Server 4.1 관리 서버를 다시 시작합니다.**

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

서버에 연결하기 위한 URL이 응답으로 제공됩니다.

2. **웹 브라우저를 열고 다음을 입력하여 관리 GUI를 시작합니다.**

http:// *호스트 이름. 도메인: 관리 포트*

인증 대화 상자에서 setup 실행 중 선택한 Sun ONE Web Server 4.1 관리 서버의 사용자 이름과 암호를 입력합니다.

참고 – Sun ONE Web Server 설치 중 기본 설정을 사용한 경우 사용자 ID 또는 Sun ONE Web Server 4.1 관리 서버 사용자 이름에 admin을 입력합니다.

---

3. **[OK(확인)]를 선택합니다.**

Sun ONE Web Server 4.1 관리 서버 창이 나타납니다.

4. **서버 인증서를 요청하려면 Sun ONE Web Server 4.1 관리 서버 창 상단에 있는 [Security(보안)] 탭을 선택합니다(**그림 5-2**).**

   [Create Trust Database(트러스트 데이터베이스 생성)] 페이지가 표시됩니다.

5. **왼쪽 패널에서 [Request a Certificate(인증서 요청)] 링크를 선택합니다(**그림 5-2**).**

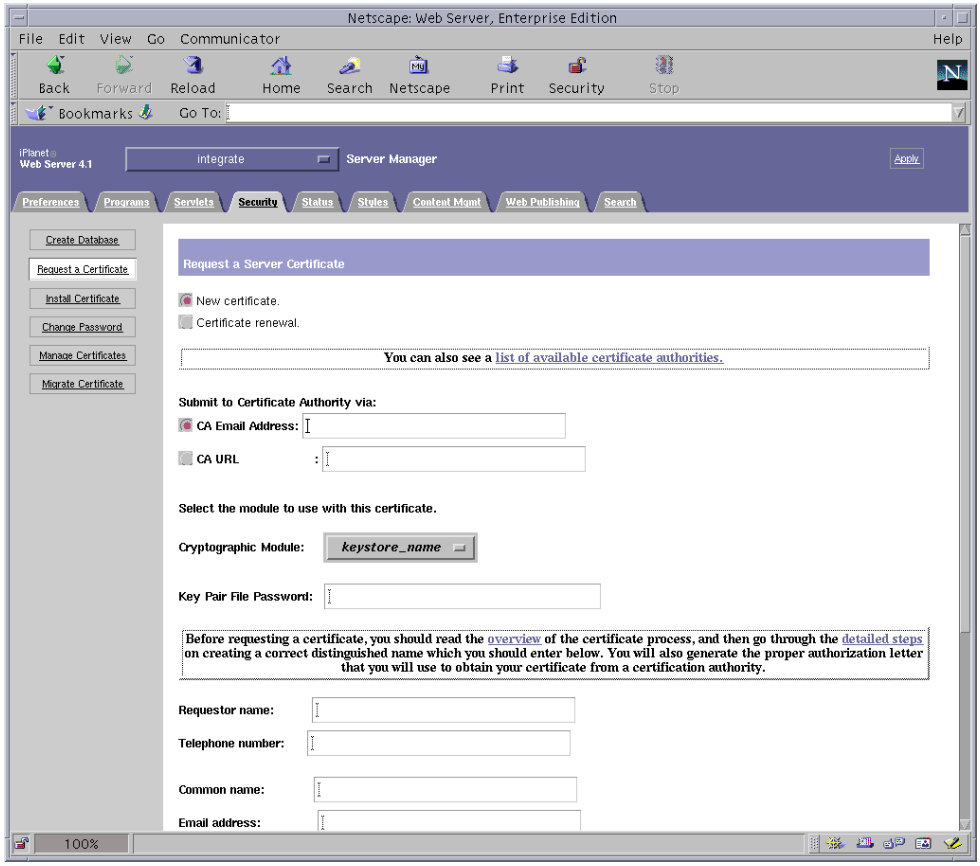

그림 5-2 Sun ONE Web Server 4.1 관리 서버의 서버 인증서 요청 대화 상자

6. **다음 정보를 기입하여 인증서 요청을 작성합니다.**

   a. **[New Certificate(새 인증서)]를 선택합니다.**

      웹 기능이 가능한 인증 기관 또는 등록 기관에 인증서 요청을 직접 보낼 수 있는 경우 [CA URL(CA URL)] 링크를 선택합니다. 그렇지 않은 경우 [CA Email Address(CA 전자 우편 주소]를 선택하고 인증서 요청을 수신할 전자 우편 주소를 입력합니다.

b. 사용할 [Cryptographic Module(암호화 모듈)]을 선택합니다.

풀다운 메뉴에는 각 키스토어의 고유 항목이 있습니다. 올바른 키스토어가 선택되었는지 확인합니다. [SUNW acceleration only(SUNW 가속화만)]는 선택하지 마십시오.

c. [Key Pair File Password(키 쌍 파일 암호)] 대화 상자에서 키를 소유할 사용자의 암호를 입력합니다.

이 암호의 형식은 *사용자 이름:암호*입니다(표 5-1).

d. 표 5-2의 요청자 정보 필드에 적절한 정보를 입력합니다.

표 5-2 요청자 정보 필드

필드	설명
Requestor Name (요청자 이름):	요청자의 연락 정보
Telephone Numbe (전화 번호):	요청자의 연락 정보
Common Name (공용 이름):	방문자 브라우저에 입력된 웹 사이트 도메인
Email Address (전자 우편 주소):	요청자의 연락 정보
Organization (소속 기관):	회사 이름
Organizational Unit (소속 기관 단위):	(선택사항)회사 부서
Locality(지역):	(선택사항)시/도/군/국가
State(주):	(선택사항)주 이름
Country(국가):	두 개의 영문자로 이루어진 ISO 국가 코드(예: 미국의 경우 US)

e. [OK(확인)]를 눌러 해당 정보를 전송합니다.

7. 인증 기관을 이용하여 인증서를 생성합니다.

- 인증서 요청을 CA URL에 보내도록 선택한 경우 인증서 요청이 CA URL에 자동으로 전송됩니다.
- [CA Email Address(CA 전자 우편 주소)]를 선택한 경우 헤더와 함께 전자 우편으로 받은 인증서 요청을 복사하여 인증 기관에 전송됩니다.

8. 인증서가 생성되면 헤더와 함께 클립보드에 복사합니다.

참고 – 인증서는 인증서 요청과는 다르며 일반적으로 텍스트 형식으로 제공됩니다. 다음 절차의 5단계를 위해 이 데이터를 클립보드에 보관합니다.

▼ 서버 인증서 설치

1. **Sun ONE Web Server 4.1 관리 서버 창 왼쪽의 [Install Certificate(인증서 설치)] 링크를 선택합니다.**

   인증 기관의 승인을 받고 인증서가 발급되면 Sun ONE Web Server에 인증서를 설치해야 합니다.

2. **[Security(보안)] 탭을 누릅니다.**

3. **왼쪽 패널에서 [Install Certificate(인증서 설치)] 링크를 선택합니다.**

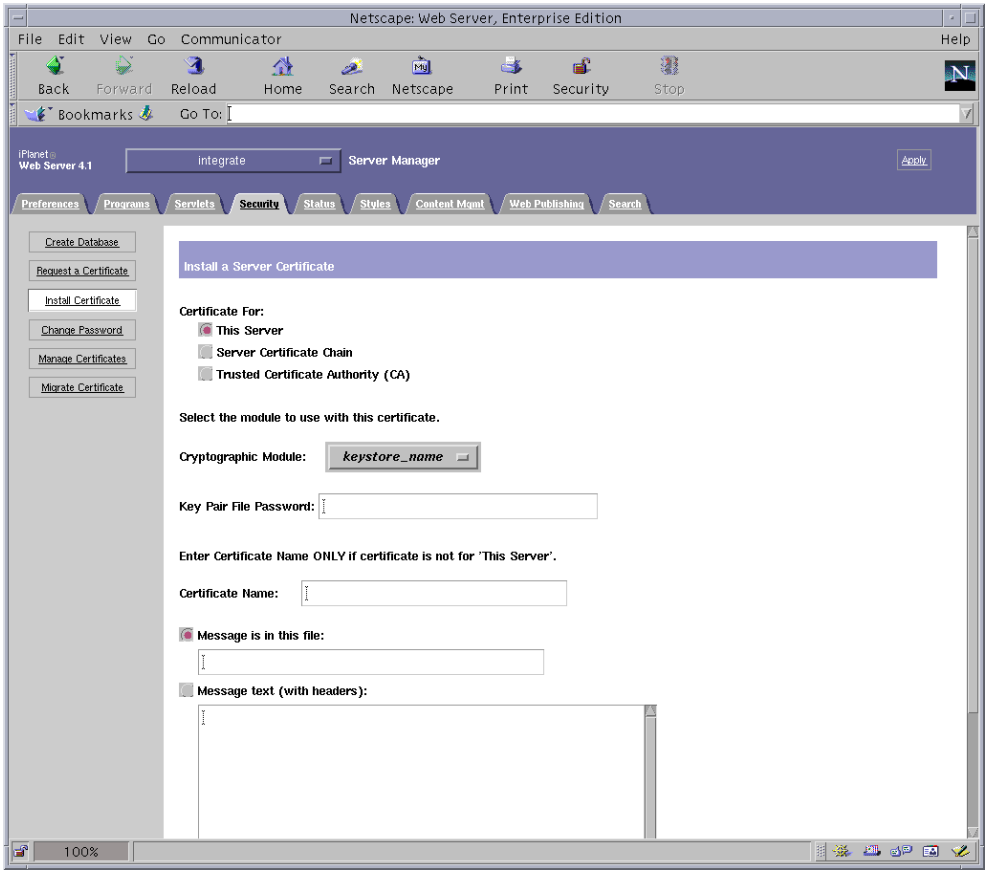

그림 5-3 Sun ONE Web Server 4.1 관리 서버의 서버 인증서 설치 대화 상자

4. **양식을 작성하여 인증서를 설치합니다.**

표 5-3 인증서 설치에 필요한 필드

필드	설명
[Certificate For (인증 대상)]	해당 서버
[Cryptographic Module(암호화 모듈)]	풀다운 메뉴에는 각 키스토어의 고유 항목이 있습니다. 반드시 정확한 키스토어 이름을 선택해야 합니다. 보드를 사용하려면 키스토어에 할당한 이름과 같은 이름을 가진 모듈을 선택해야 합니다.
[Key Pair File Password(키 쌍 파일 암호)]	이 암호의 형식은 *사용자 이름:암호*입니다(표 5-1).
[Certificate Name (인증서 이름)]	대부분의 경우 공백으로 둡니다. 이름을 제공할 경우 SSL 지원으로 실행할 경우 웹 서버가 인증서와 키에 액세스할 때 사용하는 이름을 변경합니다. 이 필드의 기본값은 `Server-Cert`입니다.

5. **인증 기관에서 복사한 인증서(111페이지의 "서버 인증서 생성"의 8단계)를 [Message box(메시지 상자)]에 붙여넣습니다.**

   인증서에 대한 일부 기본 정보가 표시됩니다.

6. **[OK(확인)]를 누릅니다.**

7. **모두 올바르게 입력되었는지 확인한 다음 [Add Server Certificate(서버 인증서 추가)] 단추를 선택합니다.**

   화면에 서버를 다시 시작하라는 메시지가 표시됩니다. 웹 서버 인스턴스는 절차가 진행되는 동안 계속 종료되어 있었기 때문에 이 메시지에 따르지 않아도 됩니다.

   또한 웹 서버가 SSL을 사용하려면 웹 서버를 구성해야 한다는 메시지가 표시됩니다. 다음 절차를 따라하여 웹 서버를 구성합니다.

참고 – 테스트를 위한 인증서 자가 서명 방법에 대한 내용은 mod_SSL 및 OpenSSL 설명서를 참조하십시오.

웹 서버 및 서버 인증서 설치가 완료되면 SSL을 위해 웹 서버를 구성해야 합니다.

▼ SSL을 위한 웹 서버 활성화

1. **Sun ONE Web Server 4.1 관리 서버 기본 페이지에서 작업할 웹 서버 인스턴스를 선택한 후 [Manage(관리)]를 선택합니다.**

2. **페이지 상단의 [Preferences(환경 설정)] 탭이 선택되어 있지 않은 경우 [Preferences (환경 설정)] 탭을 누릅니다.**

3. **페이지 왼쪽에 있는 [Encryption On/Off(암호 설정/해제)] 링크를 선택합니다.**

4. **암호화를 [On(설정)]으로 설정합니다.**

   대화 상자의 [Port(포트)] 필드가 기본 SSL 포트 번호인 443으로 업데이트됩니다. 필요한 경우 포트 번호를 변경합니다.

5. **[OK(확인)] 단추를 누릅니다.**

6. **[Save(저장)] 단추를 눌러 변경 사항을 적용합니다.**

   웹 서버가 보안 모드에서 실행되도록 구성되었습니다.

7. **다음 행을 추가하여** `/usr/netscape/server4/https-`*호스트 이름*`/config/magnus.conf`**(***호스트 이름***은 웹 서버 이름)파일을 편집합니다.**

   ```
   CERTDefaultNickname 키스토어 이름 :Server-Cert
   ```

   생성된 인증서는 기본적으로 `Server-Cert`로 이름이 지정됩니다. 인증서 이름이 다를 경우 `Server-Cert` 대신 선택한 이름을 사용해야 합니다.

8. **관리할 서버를 선택한 다음 페이지의 오른쪽 상단 모서리에 있는 [Apply(적용)] 단추를 누릅니다.**

   그러면 Sun ONE Web Server 4.1 관리 서버를 통해 변경 사항이 적용됩니다.

9. **[Load Configuration Files(구성 파일 로드)] 단추를 눌러** `magnus.conf` **파일에 대한 변경 사항을 적용합니다.**

   웹 서버 인스턴스를 시작할 수 있는 페이지로 다시 돌아갑니다.

   서버가 꺼져 있을 때 [Apply Changes(변경 사항 적용)]를 선택할 경우 인증 대화 상자가 나타나 *사용자 이름:암호* 입력을 요청합니다. 이 창은 크기를 조정할 수 없으며, 변경 사항을 전송하는 데 문제가 생길 수 있습니다.

   이 문제는 다음 두 가지 방법으로 해결할 수 있습니다.

   - [Load Configuration Files(구성 파일 로드)]을 선택합니다.
   - 웹 서버를 먼저 시작한 다음 [Apply Changes(변경 사항 적용)] 단추를 누릅니다.

10. **Sun ONE Web Server 4.1 관리 서버 창에서 창 왼쪽의 [On/Off(설정/해제)] 링크를 선택합니다.**

11. **서버의 암호를 입력한 다음 [OK(확인)] 단추를 선택합니다.**

    하나 이상의 암호를 입력하게 됩니다. [Module Internal(모듈 내부)] 프롬프트에서 웹 서버 트러스트 데이터베이스에 대한 암호를 입력합니다.

    모듈 *keystore-name* 프롬프트에서 해당 키스토어에 대한 *사용자 이름:암호*를 입력합니다.

    요청에 따라 다른 키스토어에 대한 *사용자 이름:암호*를 입력합니다.

12. **다음 웹 사이트에서 SSL이 활성화된 새 웹 서버를 확인합니다.**

    `https://`*호스트 이름.도메인:서버 포트*`/`

참고 – 기본 *서버 포트*는 443입니다.

Sun ONE Web Server 6.0 설치 및 구성

이 항목에서는 Sun ONE Web Server 6.0이 보드를 사용하도록 하기 위해 소프트웨어를 설치 및 구성하는 방법에 대해 설명합니다. 절차는 반드시 순서대로 수행해야 합니다. Sun ONE Web Server 설치 및 사용 방법에 대한 자세한 내용은 Sun ONE Web Server 설명서를 참조하십시오. 이 항목은 다음 절차를 설명합니다.

▼ Sun ONE Web Server 6.0 설치

1. **Sun ONE Web Server 6.0 소프트웨어를 다운로드합니다.**

   웹 서버 소프트웨어는 다음 URL에서 다운받을 수 있습니다.
   `http://www.sun.com/`

2. **설치 디렉토리로 변경하고 웹 서버 소프트웨어를 추출합니다.**

3. **명령행에서 setup 스크립트를 사용해 웹 서버를 설치합니다.**

   이 서버의 기본 경로 이름은 `/usr/iplanet/servers`입니다.

   이 장에서는 이 기본 경로를 사용합니다. 소프트웨어를 다른 위치에 설치하려면 설치한 위치를 기록해 두는 것이 좋습니다.

   ```
   # ./setup
   ```

4. **설치 스크립트의 프롬프트에 응답합니다.**

   다음 프롬프트 이외에는 기본값을 그대로 사용할 수 있습니다.

   a. `yes`**를 입력하여 라이센스 약관에 동의합니다.**

   b. 정식 도메인 이름을 입력합니다.

c. Sun ONE Web Server 6.0 관리 서버 암호를 두 번 입력합니다.

d. 프롬프트가 나타나면 [Return]을 누릅니다.

Sun ONE Web Server 6.0 구성

다음은 웹 서버 인스턴스에 대한 트러스트 데이터베이스를 생성하고 웹 서버로 보드를 등록하며 서버 인증서를 생성 및 설치할 뿐 아니라, SSL을 위해 웹 서버를 구성하는 절차입니다.

Sun ONE Web Server 관리 서버는 구성 프로세스 중에 반드시 실행 중이어야 합니다.

▼ 트러스트 데이터베이스 생성

1. Sun ONE Web Server 6.0 관리 서버를 시작합니다.

`setup` 요청에 따라 `startconsole`을 실행하지 말고 다음 명령을 사용하여 Sun ONE Web Server 6.0 관리 서버를 시작합니다.

```
# /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
```

서버에 연결하기 위한 URL이 응답으로 제공됩니다.

2. 웹 브라우저를 열고 다음을 입력하여 관리 GUI를 시작합니다.

http:// *호스트 이름. 도메인: 관리 포트*

인증 대화 상자에서 `setup` 실행 중 선택한 Sun ONE Web Server 6.0 관리 서버의 사용자 이름과 암호를 입력합니다.

참고 – Sun ONE Web Server 설치 중 기본 설정을 사용한 경우 사용자 ID 또는 Sun ONE Web Server 6.0 관리 서버 사용자 이름에 `admin`을 입력합니다.

---

3. [OK(확인)]를 누릅니다.

Sun ONE Web Server 6.0 관리 서버 창이 나타납니다.

4. 웹 서버 인스턴스에 대한 트러스트 데이터베이스를 생성합니다.

하나 이상의 웹 서버 인스턴스에 대해 보안을 활성화할 수 있습니다. 이 경우에는 각 웹 서버 인스턴스에 대해 1단계 ~ 4단계를 반복합니다.

참고 – Sun ONE Web Server 6.0 관리 서버에서 SSL을 실행하는 경우에도 트러스트 데이터베이스의 설정 절차는 유사합니다. 자세한 내용은 `http://docs.sun.com`에서 *iPlanet Web Server, Enterprise Edition Administrator's Guide*를 참조하십시오.

---

a. Sun ONE Web Server 6.0 관리 서버 대화 상자에서 [Servers(서버)] 탭을 누릅니다.

b. 서버를 선택한 다음 [Manage(관리)] 단추를 누릅니다.

c. 페이지의 상단 부분에 있는 [Security(보안)] 탭을 누르고 [Create Database(데이터베이스 생성)] 링크를 선택합니다.

d. 두 개의 대화 상자에 암호(웹 서버 트러스트 데이터베이스, 표 5-1 **참조)를 입력하고 [OK(확인)]를 선택합니다.**

8개 이상의 문자로 된 암호를 선택합니다. Sun ONE Web Server를 보안 모드로 실행할 경우 이 암호를 사용하여 내부 암호화 모듈을 시작합니다.

▼ Web Server에 보드 등록

1. 다음 스크립트를 실행하여 Web Server에 보드를 등록합니다.

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

이 스크립트는 웹 서버를 선택하고 선택한 Sun ONE 서버를 위한 Sun Crypto Accelerator 4000 암호화 모듈을 설치하라는 메시지를 표시합니다. 그런 다음 스크립트는 구성 파일을 업데이트하여 보드를 활성화합니다.

2. Sun ONE Web Server가 SSL을 사용할 수 있도록 구성하려면 `1`**을 입력한 다음 [Return]을 누릅니다.**

참고 – 여기서는 이 프롬프트에서 `1` 옵션을 선택하는 경우에 대한 절차를 설명합니다. `2`, `3` 또는 `4`옵션을 선택하려면 88페이지의 "`iplsslcfg` 스크립트 사용"을 참조하십시오.

```
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. **프롬프트가 나타나면 웹 서버 루트 디렉토리의 경로를 입력한 다음 [Return]을 누릅니다.**

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

4. **프롬프트가 나타나면 y를 입력하고 [Return]을 누릅니다.**

```
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. **0을 입력하여 종료합니다.**

▼ 서버 인증서 생성

1. **다음 명령을 입력하여 Sun ONE Web Server 6.0 관리 서버를 다시 시작합니다.**

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

서버에 연결하기 위한 URL이 응답으로 제공됩니다.

2. **웹 브라우저를 열고 다음을 입력하여 관리 GUI를 시작합니다.**

http:// *호스트 이름*. *도메인*: *관리 포트*

인증 대화 상자에서 `setup` 실행 중 선택한 Sun ONE Web Server 6.0 관리 서버의 사용자 이름과 암호를 입력합니다.

참고 – Sun ONE Web Server 설치 중 기본 설정을 사용한 경우 사용자 ID 또는 Sun ONE Web Server 6.0 관리 서버 사용자 이름에 **admin**을 입력합니다.

---

3. **[OK(확인)]를 누릅니다.**

Sun ONE Web Server 6.0 관리 서버 창이 나타납니다.

4. **서버 인증서를 요청하려면 Sun ONE Web Server 6.0 관리 서버 창 상단에 있는 [Security(보안)] 탭을 선택합니다.**

[Create Trust Database(트러스트 데이터베이스 생성)] 창이 표시됩니다.

5. **Sun ONE Web Server 6.0 관리 서버 창의 왼쪽 패널에서 [Request a Certificate(인증서 요청)] 링크를 누릅니다.**

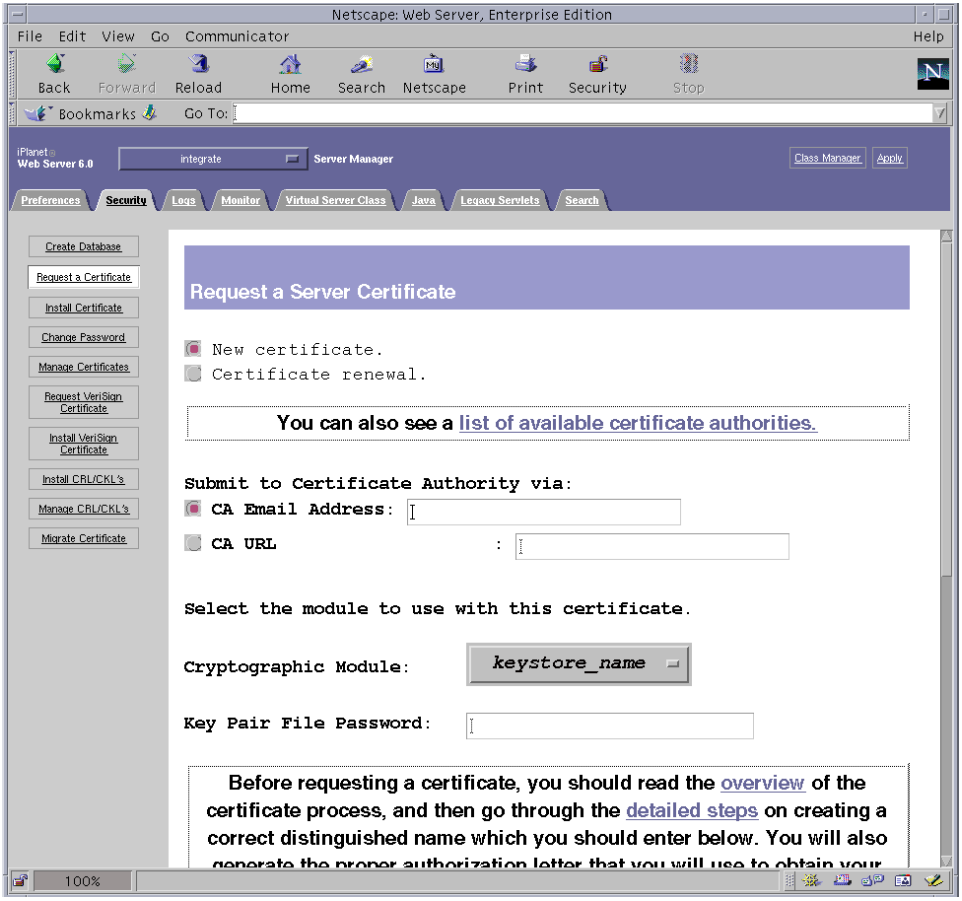

그림 5-4 Sun ONE Web Server 6.0 관리 서버의 서버 인증서 요청 대화 상자

6. **다음 정보를 기입하여 인증서 요청을 작성합니다.**

   a. **[New Certificate(새 인증서)]를 선택합니다.**

      웹 기능이 가능한 인증 기관 또는 등록 기관에 인증서 요청을 직접 보낼 수 있는 경우 [CA URL(CA URL)] 링크를 선택합니다. 그렇지 않은 경우 [CA Email Address(CA 전자 우편 주소]를 선택하고 인증서 요청을 수신할 전자 우편 주소를 입력합니다.

   b. **사용할 [Cryptographic Module(암호화 모듈)]을 선택합니다.**

      풀다운 메뉴에는 각 키스토어의 고유 항목이 있습니다. 올바른 키스토어가 선택되었는지 확인합니다. [SUNW acceleration only(SUNW 가속화만)]는 선택하지 마십시오.

c. [Key Pair File Password(키 쌍 파일 암호)] 대화 상자에서 키를 소유할 사용자의 암호를 입력합니다.

이 암호의 형식은 *사용자 이름:암호*입니다(표 5-1).

d. 표 5-4의 요청자 정보 필드에 적절한 정보를 입력합니다.

표 5-4 요청자 정보 필드

필드	설명
Requestor Name (요청자 이름):	요청자의 연락 정보
Telephone Numbe (전화 번호):	요청자의 연락 정보
Common Name(공용 이름):	방문자 브라우저에 입력된 웹 사이트 도메인
Email Address (전자 우편 주소):	요청자의 연락 정보
Organization (소속 기관):	회사 이름
Organizational Unit (소속 기관 단위):	(선택사항)회사 부서
Locality(지역):	(선택사항)시/도/군/국가
State(주):	(선택사항)주 이름
Country(국가):	두 개의 영문자로 이루어진 ISO 국가 코드(예: 미국의 경우 US)

e. [OK(확인)]를 눌러 해당 정보를 전송합니다.

7. 인증 기관을 이용하여 인증서를 생성합니다.

- 인증서 요청을 CA URL에 보내도록 선택한 경우 인증서 요청이 CA URL에 자동으로 전송됩니다.
- [CA Email Address(CA 전자 우편 주소)]를 선택한 경우 헤더와 함께 전자 우편으로 받은 인증서 요청을 복사하여 인증 기관에 전송합니다.

8. 인증서가 생성되면 헤더와 함께 클립보드에 복사합니다.

참고 – 인증서는 인증서 요청과는 다르며 일반적으로 텍스트 형식으로 제공됩니다. 124페이지의 "서버 인증서 설치"의 5단계를 위해 이 데이터를 클립보드에 보관합니다.

▼ 서버 인증서 설치

1. **Sun ONE Web Server 6.0 관리 서버 창 왼쪽의 [Install Certificate(인증서 설치)] 링크를 선택합니다.**

   인증 기관의 승인을 받고 인증서가 발급되면 Sun ONE Web Server에 인증서를 설치해야 합니다.

2. **[Security(보안)] 탭을 누릅니다.**

3. **왼쪽 패널에서 [Install Certificate(인증서 설치)] 링크를 누릅니다.**

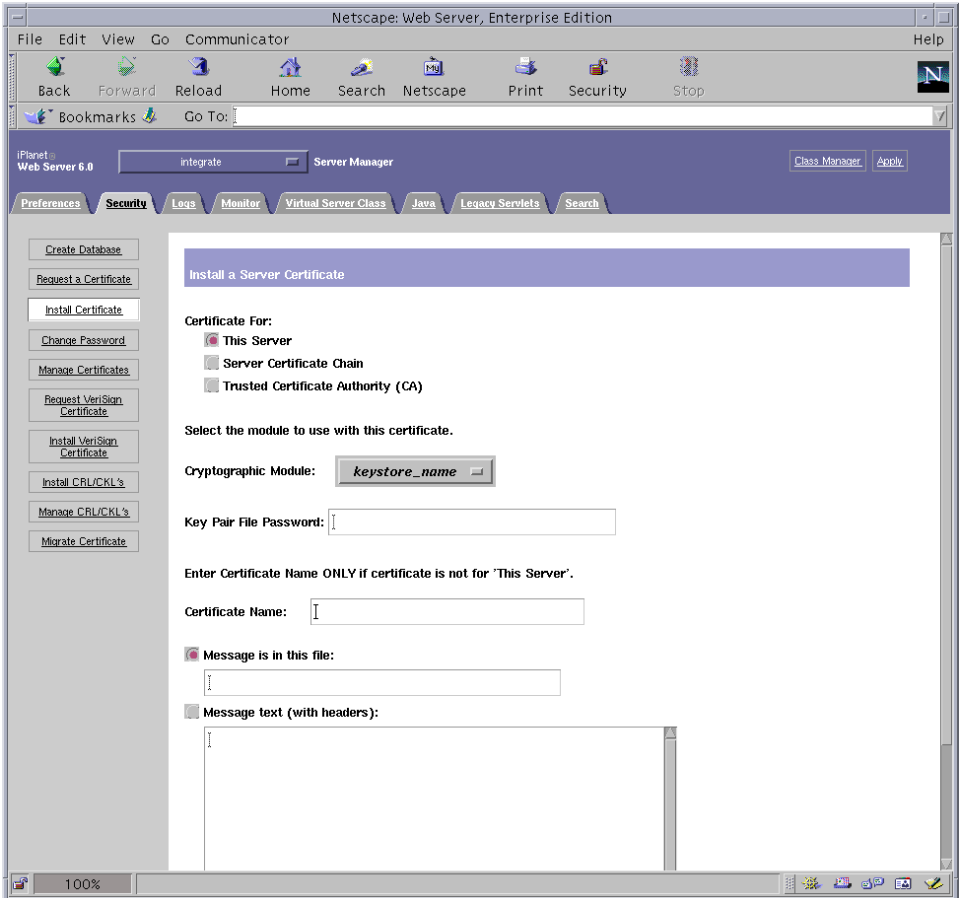

그림 5-5 Sun ONE Web Server 6.0 관리 서버의 서버 인증서 설치 대화 상자

4. **양식을 작성하여 인증서를 설치합니다.**

표 5-5 인증서 설치에 필요한 필드

필드	설명
[Certificate For (인증 대상)]	해당 서버
[Cryptographic Module(암호화 모듈)]	풀다운 메뉴에는 각 키스토어의 고유 항목이 있습니다. 올바른 키스토어 이름이 선택되었는지 확인합니다. 보드를 사용하려면 반드시 *keystore_name* 형식의 모듈을 선택해야 합니다.
[Key Pair File Password(키 쌍 파일 암호)]	이 암호의 형식은 *사용자 이름:암호*입니다(표 5-1).
[Certificate Name (인증서 이름)]	대부분의 경우 공백으로 둡니다. 이름을 제공할 경우 SSL 지원으로 실행할 경우 웹 서버가 인증서와 키에 액세스할 때 사용하는 이름을 변경합니다. 이 필드의 기본값은 `Server-Cert`입니다.

5. **인증 기관에서 복사한 인증서(121페이지의 "서버 인증서 생성"의8단계)를 [Message (메시지)] 텍스트 상자에 붙여넣습니다.**

   인증서에 대한 일부 기본 정보가 표시됩니다.

6. **[OK(확인)]를 누릅니다.**

7. **올바르게 입력되었는지 확인한 다음 [Add Server Certificate(서버 인증서 추가)] 단추를 누릅니다.**

   화면에 서버를 다시 시작하라는 메시지가 표시됩니다. 웹 서버 인스턴스는 절차가 진행되는 동안 계속 종료되어 있었기 때문에 이 메시지에 따르지 않아도 됩니다.

   또한 웹 서버가 SSL을 사용하려면 웹 서버를 구성해야 한다는 메시지가 표시됩니다. 다음 절차를 따라하여 웹 서버를 구성합니다.

참고 – 테스트를 위한 인증서 자가 서명 방법에 대한 내용은 mod_SSL 및 OpenSSL 설명서를 참조하십시오.

웹 서버 및 서버 인증서 설치가 완료되면 SSL을 위해 웹 서버를 구성해야 합니다.

▼ SSL을 위한 웹 서버 활성화

1. **페이지 상단 부분의 [Preferences(환경 설정)] 탭을 선택합니다.**

2. **왼쪽 패널에 있는 [Edit Listen Sockets(수신 대기 소켓 편집)] 링크를 선택합니다.**

   기본 패널에 웹 서버 인스턴스에 대해 설정된 모든 수신 대기 소켓이 나열됩니다.

a. 다음 필드를 수정합니다.

- **Port**(포트): SSL이 활성화된 웹 서버를 실행할 포트로 설정합니다(주로 443 포트).
- **Security**(보안): [On(설정)]으로 설정합니다.

b. [OK(확인)]를 눌러 변경 사항을 적용합니다.

이제 [Edit Listen Sockets(수신 대기 소켓 편집)] 페이지의 보안 필드에 [Attributes(속성)] 링크가 표시됩니다.

3. [Attributes(속성)] 링크를 선택합니다.

4. 시스템의 키스토어에 대한 인증을 받으려면 *사용자 이름:암호***를 입력합니다.**

5. 암호의 기본 설정을 변경하려면 [Ciphers(암호)]에서 해당 암호 모음을 선택합니다.

암호 설정 변경 대화 상자가 나타납니다. [Cipher Default(암호 기본값)] 설정, [SSL2] 또는 [SSL3/TLS]를 선택할 수 있습니다. [Cipher Default(암호 기본값)]를 선택한 경우 기본 설정이 표시되지 않습니다. 다른 두 옵션을 선택하려면 팝업 대화 상자에서 활성화할 알고리즘을 선택해야 합니다. 암호 선택에 대한 내용은 Sun ONE 설명서를 참조하십시오.

6. `Server-Cert`**(또는 이와 다른 경우 선택한 이름) 다음에 나오는 키스토어에 대한 인증서를 선택합니다.**

[Certificate Name(인증서 이름)] 필드에는 해당 키스토어 사용자가 소유하는 키만 나타납니다. 키스토어 사용자는 *사용자 이름:암호*로 인증한 사용자입니다.

7. 인증서를 선택하고 보안 설정을 모두 확인했으면 [OK(확인)]를 누릅니다.

8. 오른쪽 상단 모서리에 있는 [Apply(적용)] 링크를 선택하여 서버를 시작하기 전에 변경 사항을 적용합니다.

9. [Load Configuration Files(구성 파일 로드)] 링크를 선택하여 변경 사항을 적용합니다.

웹 서버 인스턴스를 시작할 수 있는 페이지로 다시 돌아갑니다.

서버가 꺼져 있을 때 [Apply Changes(변경 사항 적용)]를 선택할 경우 인증 대화 상자가 나타나 *사용자 이름:암호* 입력을 요청합니다. 이 창은 크기를 조정할 수 없으며, 변경 사항을 전송하는 데 문제가 생길 수 있습니다.

이 문제는 다음 두 가지 방법으로 해결할 수 있습니다.

- [Load Configuration Files(구성 파일 로드)]을 선택합니다.
- 웹 서버를 먼저 시작한 다음 [Apply Changes(변경 사항 적용)]를 누릅니다.

10. Sun ONE Web Server 6.0 관리 서버 창에서 창 왼쪽의 [On/Off(설정/해제)] 링크를 선택합니다.

11. **서버의 암호를 입력한 다음 [OK(확인)]를 누릅니다.**

    하나 이상의 암호를 입력하게 됩니다. [Module Internal(모듈 내부)] 프롬프트에서 웹 서버 트러스트 데이터베이스에 대한 암호를 입력합니다.

    keystore-name 모듈 프롬프트에서 *사용자 이름:암호*를 입력합니다.

    요청에 따라 다른 키스토어에 대한 *사용자 이름:암호*를 입력합니다.

12. **다음 웹 사이트에서 SSL이 활성화된 새 웹 서버를 확인합니다.**

    `https://`*호스트 이름.도메인:서버 포트*`/`

참고 – 기본 *서버 포트*는 443입니다.

Sun ONE Application Server 7 설치 및 구성

이 항목에서는 Sun ONE Application Server 7이 보드를 사용하도록 하기 위해 소프트웨어를 설치 및 구성하는 방법에 대해 설명합니다. Application Server 소프트웨어 외에도 반드시 Application Server Add-Ons 소프트웨어를 설치해야 합니다. 절차는 반드시 순서대로 수행해야 합니다. Sun ONE Application Server 설치 및 사용 방법에 대한 자세한 내용은 Sun ONE Application Server 설명서를 참조하십시오. 이 항목은 다음 절차를 설명합니다.

- 127페이지의 "Sun ONE Application Server 7 설치"
- 129페이지의 "Sun ONE Application Server 7 구성"
- 130페이지의 "트러스트 데이터베이스 생성"
- 131페이지의 "Application Server에 보드 등록"
- 133페이지의 "서버 인증서 생성"
- 135페이지의 "서버 인증서 설치"
- 137페이지의 "SSL을 위한 응용 프로그램 서버 활성화"

▼ Sun ONE Application Server 7 설치

1. **Sun ONE Application Server 7 소프트웨어를 다운로드합니다.**

    Application Server 소프트웨어는 다음URL에서 다운받을 수 있습니다.
    `http://www.sun.com/`

    Sun ONE Application Server 7의 배포판은 여러 종류가 있으며 각각 고유한 기능을 갖추고 있습니다.

2. **설치 디렉토리로 변경하고 응용 프로그램 서버 소프트웨어를 추출합니다.**

   설치 디렉토리의 기본 경로는 Sun ONE Application Server 7 소프트웨어의 배포판마다 다릅니다.

3. `setup` **프로그램을 실행하여 GUI 기반 설치를 시작합니다.**

참고 – 터미널 창에서 `setup -console` 프로그램을 실행하여 명령행 기반 설치를 시작할 수도 있습니다. 이 예제에서는 GUI 기반 설치를 사용하는 경우의 절차에 대해 설명합니다.

```
# ./setup
```

4. **설치 스크립트의 프롬프트에 응답합니다.**

   다음 프롬프트 이외에는 기본값을 그대로 사용할 수 있습니다.

   a. **yes를 입력하여 라이센스 약관에 동의합니다.**

   b. **JDK(Java™ Development Kit)의 위치를 묻는 프롬프트가 나타나면 [Use Existing Installation if it is supported(지원되는 경우 기존 설치 사용)] 또는 [Install From the Appserver Build(Appserver Build에서 설치)]를 선택합니다.**

   c. **Sun ONE Application Server 관리 서버 사용자 이름을 입력합니다(아무 이름이나 선택할 수 있음).**

   d. **Sun ONE Application Server 관리 서버 암호를 두 번 입력합니다.**

참고 – Solaris 8 OE를 사용하는 경우에만 다음 단계를 수행하십시오.

---

5. **Solaris 8을 사용하는 경우 Solaris 8 Sun ONE Application Server 패치(109326-08)를 설치합니다.**

   Solaris 9에는 이 패치가 필요하지 않습니다. 다음 SunSolve 웹 사이트에서 Solaris 8 Sun ONE Application Server 패치를 다운로드합니다. `http://sunsolve.sun.com`

   다음과 같이 패치를 추가합니다.

```
# cd 패치 위치 /SUNWappserver7/patches
# cd patches/109326-08
# ./patchadd .
```

6. **시스템을 재부팅합니다.**

▼ Sun ONE Application Server Add-Ons 소프트웨어 설치

1. **Sun ONE Application Server 7 Add-Ons 소프트웨어를 다운로드합니다.**
   응용 프로그램 서버 소프트웨어는 다음URL에서 다운받을 수 있습니다.
   `http://www.sun.com/`
2. **Application Aerver Add-Ons 소프트웨어를 추출합니다.**
3. **`./AddOns/SSLUtils` 디렉토리로 변경합니다.**
4. **`iplsslcfg` 스크립트가 `modutil` 보안 도구를 호출하는 디렉토리를 생성합니다.**

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

   이 경로는 `iplsslcfg` 스크립트로 `modutil` 보안 도구를 찾는 데 사용합니다.

5. **`modutil`, `certutil` 및 `pk12util` 바이너리를 `/usr/bin/mps/` 경로에 복사합니다.**

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

6. **`/usr/bin/mps/` 디렉토리에서 바이너리에 대한 실행 권한을 활성화합니다.**

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

Sun ONE Application Server 7 구성

다음은 응용 프로그램 서버 인스턴스에 대한 트러스트 데이터베이스를 생성하고 응용 프로그램 서버로 보드를 등록하며 서버 인증서를 생성 및 설치할 뿐 아니라, SSL 및 TLS을 위해 응용 프로그램 서버를 구성하는 절차입니다.

Sun ONE Application Server 관리 서버는 구성 프로세스 중에 반드시 실행 중이어야 합니다.

▼ 트러스트 데이터베이스 생성

1. Sun ONE Application Server 및 Sun ONE Application Server 관리 서버를 시작합니다.

```
# 설치 디렉토리/bin/asadmin start-appserv
```

참고 – 응용 프로그램 서버가 실행 중임을 알리는 메시지가 나타납니다.

2. 웹 브라우저를 열고 다음 URL을 입력하여 관리 GUI를 시작합니다.

```
http://호스트 이름:4848
```

인증 대화 상자에서 `setup` 프로그램 실행 시 생성한 Sun ONE Application Server 사용자 이름 및 암호를 입력합니다.

참고 – Sun ONE Application Server 설치 중 기본 설정을 사용한 경우 사용자 ID 또는 Sun ONE Application Server 관리 서버 사용자 이름에 `admin`을 입력합니다.

3. [OK(확인)]를 누릅니다.

4. 응용 프로그램 서버 인스턴스에 대한 트러스트 데이터베이스를 생성합니다.

하나 이상의 응용 프로그램 서버 인스턴스에 대해 보안을 활성화할 수 있습니다. 이 경우에는 각 응용 프로그램 서버 인스턴스에 대해 1단계 ~ 4단계를 반복합니다.

참고 – Sun ONE Application Server 6.0 관리 서버에서 SSL을 실행하는 경우에도 트러스트 데이터베이스의 설정 절차는 유사합니다. 자세한 내용은 `http://docs.sun.com/source/816-7158-10/`에서 *Sun ONE Application Server 7 Administrator's Guide*를 참조하십시오.

a. 관리 GUI의 [Manage Database(데이터베이스 관리)] 항목으로 이동합니다.

왼쪽 패널에서 [Security(보안)] 링크를 선택하고 오른쪽 패널에서 [Manage Database(데이터베이스 관리)]를 누릅니다.

b. 두 개의 텍스트 상자에 8개 이상의 문자로 된 암호를 입력하고 [OK(확인)]를 누릅니다.

이 암호는 Sun ONE Application Server의 트러스트 데이터베이스 암호입니다. 응용 프로그램 서버를 보안 모드에서 실행할 경우 이 암호를 사용하여 내부 암호화 모듈을 시작합니다.

▼ Application Server에 보드 등록

1. **iplsslcfg 스크립트를 실행하여 응용 프로그램 서버에 보드를 등록합니다.**

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

이 스크립트는 웹 서버를 선택하고 선택한 Sun ONE 서버를 위한 Sun Crypto Accelerator 4000 암호화 모듈을 설치하라는 메시지를 표시합니다. 그런 다음 스크립트는 구성 파일을 업데이트하여 보드를 활성화합니다.

2. **Sun ONE Application Server의 경우 2를 입력하고 바이너리 및 도메인 경로를 입력합니다.**

참고 – 이 항목에서는 이 프롬프트에서 1 옵션을 선택하는 경우의 절차에 대해 설명합니다. 3 또는 4 옵션을 선택하려면 88페이지의 "iplsslcfg 스크립트 사용"을 참조하십시오.

```
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. **바이너리 및 도메인의 위치를 입력한 다음 도메인 및 서버 이름을 입력합니다.**

```
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>
```

참고 – 기본 설치 디렉토리는 Sun ONE Application Server 7의 배포판마다 다를 수 있습니다.

4. 0**을 입력하여 종료합니다.**

▼ 서버 인증서 생성

1. **관리 GUI의 [Certificate Management(인증서 관리)] 항목으로 이동합니다.**

   왼쪽 패널에서 [Security(보안)] 링크를 선택하고 오른쪽 패널에서 [Certificate Management(인증서 관리)] 탭을 선택합니다. 관리 GUI의 [Certificate Management (인증서 관리)] 항목의 [Request(요청)] 하위 메뉴 창이 나타납니다.

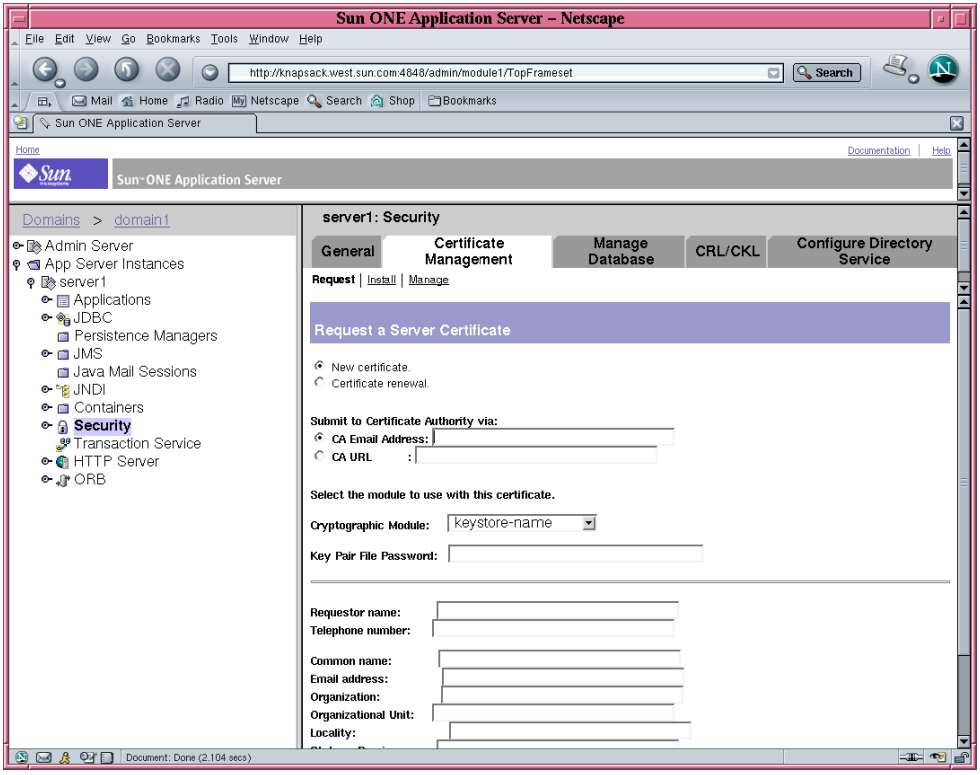

그림 5-6 Sun ONE Application Server 관리 서버의 서버 인증서 요청 대화 상자

2. **다음 정보를 기입하여 인증서 요청을 작성합니다.**

   a. **[New Certificate(새 인증서)]를 선택합니다.**

      웹 기능이 가능한 인증 기관 또는 등록 기관에 인증서 요청을 직접 보낼 수 있는 경우 CA URL 링크를 선택합니다. 그렇지 않은 경우 [CA Email Address(CA 전자 우편 주소]를 선택하고 인증서 요청을 수신할 전자 우편 주소를 입력합니다.

   b. **사용할 [Cryptographic Module(암호화 모듈)]을 선택합니다.**

      풀다운 메뉴에는 각 키스토어의 고유 항목이 있습니다. 올바른 키스토어가 선택되었는지 확인합니다. [SUNW acceleration only(SUNW 가속화만)]는 선택하지 마십시오.

c. [Key Pair File Password(키 쌍 파일 암호)] 대화 상자에서 키를 소유할 사용자의 암호를 입력합니다.

이 암호의 형식은 *사용자 이름:암호*입니다(표 5-1 참조).

d. 표 5-6의 요청자 정보 필드에 적절한 정보를 입력합니다.

표 5-6 요청자 정보 필드

필드	설명
Requestor Name (요청자 이름):	요청자의 연락 정보
Telephone Numbe (전화 번호):	요청자의 연락 정보
Common Name (공용 이름):	방문자 브라우저에 입력된 웹 사이트 도메인
Email Address (전자 우편 주소):	요청자의 연락 정보
Organization (소속 기관):	회사 이름
Organizational Unit (소속 기관 단위):	(선택사항)회사 부서
Locality(지역):	(선택사항)시/도/군/국가
State(주):	(선택사항)주 이름
Country(국가):	두 개의 영문자로 이루어진 ISO 국가 코드(예: 미국의 경우 US)

e. [OK(확인)]를 눌러 해당 정보를 전송합니다.

3. 인증 기관을 이용하여 인증서를 생성합니다.

- 인증서 요청을 CA URL에 보내도록 선택한 경우 인증서 요청이 CA URL에 자동으로 전송됩니다.
- [CA Email Address(CA 전자 우편 주소)]를 선택한 경우 헤더와 함께 전자 우편으로 받은 인증서 요청을 복사하여 인증 기관에 전송합니다.

4. 인증서가 생성되면 헤더와 함께 클립보드에 복사합니다.

참고 – 인증서는 인증서 요청과는 다르며 일반적으로 텍스트 형식으로 제공됩니다. 135페이지의 "서버 인증서 설치"의 4단계를 위해 이 데이터를 클립보드에 보관합니다.

▼ 서버 인증서 설치

1. **관리 GUI의 [Certificate Management(인증서 관리)] 항목의 왼쪽 패널에서 [Install (설치)] 링크를 선택합니다.**

   관리 GUI의 [Certificate Management(인증서 관리)] 항목의 [Install(설치)] 하위 메뉴 창이 나타납니다.

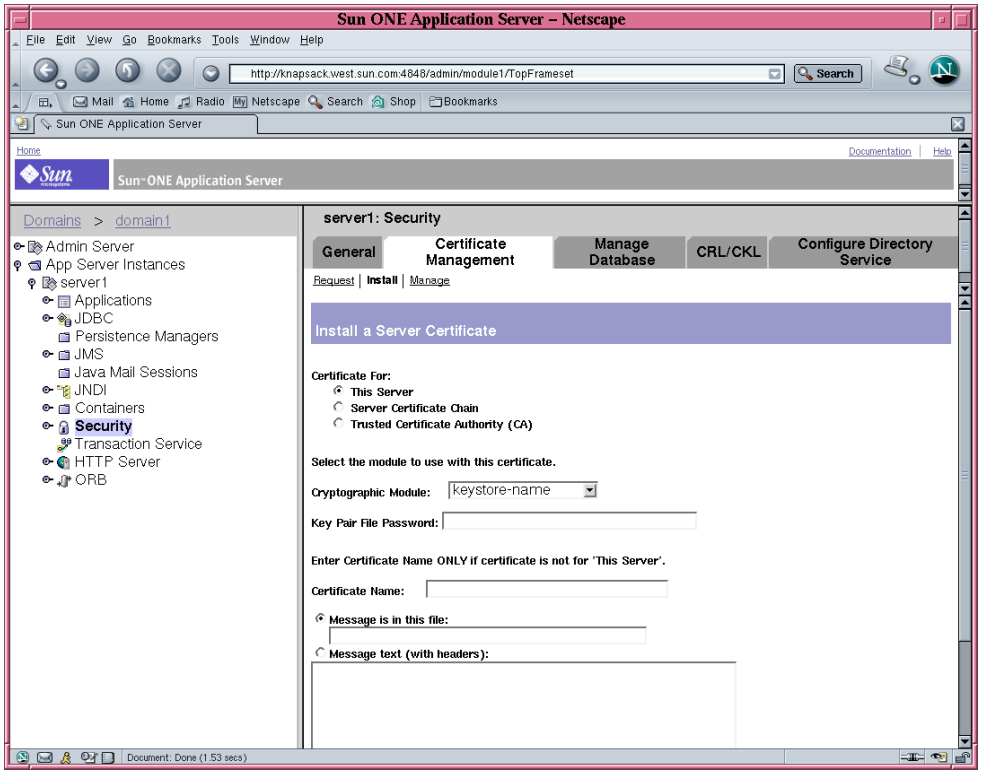

그림 5-7 Sun ONE Application Server 관리 서버의 서버 인증서 설치 대화 상자

2. **양식을 작성하여 인증서를 설치합니다.**

표 5-7 인증서 설치에 필요한 필드

필드	설명
[Certificate For (인증 대상)]	해당 서버
[Cryptographic Module(암호화 모듈)]	풀다운 메뉴에는 각 키스토어의 고유 항목이 있습니다. 올바른 키스토어 이름이 선택되었는지 확인합니다. Sun Crypto Accelerator 4000 보드를 사용하려면 인증서 요청 시 선택한 이름과 같은 이름을 가진 모듈을 선택해야 합니다.
[Key Pair File Password(키 쌍 파일 암호)]	이 암호의 형식은 *사용자 이름:암호*입니다.
[Certificate Name (인증서 이름)]	대부분의 경우 공백으로 둡니다. 이름을 제공할 경우 SSL 지원으로 실행하게 되면 응용 프로그램 서버가 인증서와 키에 액세스할 때 사용하는 이름을 변경합니다. 이 필드의 기본값은 `Server-Cert`입니다.

3. **[Message text(메시지 텍스트)(헤더 포함)] 라디오 단추를 선택합니다.**

4. **[Message text(메시지 텍스트)(헤더 포함)] 라디오 단추를 누른 다음 인증 기관(133페이지의 "서버 인증서 생성"의 4단계)에서 복사한 인증서를 라디오 단추 아래의 텍스트 상자에 붙여 넣습니다.**

5. **[OK(확인)]를 누릅니다.**

   인증서에 대한 일부 기본 정보가 표시됩니다.

6. **올바르게 입력되었는지 확인한 다음 [Add Server Certificate(서버 인증서 추가)]를 누릅니다.**

   응용 프로그램 서버를 다시 시작하라는 메시지가 표시됩니다. 이 때에는 응용 프로그램 서버를 다시 시작하지 마십시오. SSL 구성이 완료되면 응용 프로그램 서버가 자동으로 다시 시작됩니다. 또한 응용 프로그램 서버에서 SSL을 사용하려면 응용 프로그램 서버를 구성해야 한다는 메시지가 표시됩니다.

▼ SSL을 위한 응용 프로그램 서버 활성화

1. **터미널 창에 다음 명령을 입력합니다.**

   또한 이 명령을 실행한 후에는 Sun ONE Application Server 관리 서버 암호를 입력해야 합니다.

   참고 – 명령을 로컬 호스트에서 실행 중이고 Sun ONE Application Server 관리 서버가 기본 포트 4848을 사용하도록 구성되어 있으면 `--host` *호스트 이름* `--port` *관리 서버 포트* 인수는 생략할 수 있습니다.

```
# 설치 디렉토리/bin/asadmin create-ssl --user 응용 프로그램admin --host
호스트 이름 --port 관리 서버 포트 --type http-listener --certname
키스토어 이름:서버 인증서 이름 --instance 서버 이름http 수신기
password>
```

2. **관리 GUI의 왼쪽 패널에서 [HTTP Server(HTTP 서버)] 링크 왼쪽의 확장 아이콘을 선택합니다.**

   [HTTP Server(HTTP 서버)]의 하위 메뉴 항목이 나타납니다.

3. **[HTTP Server(HTTP 서버)] 링크의 [HTTP Liseners(HTTP 수신기)] 하위 메뉴 항목을 선택합니다.**

4. **오른쪽 패널에서 SSL/TLS를 위해 구성할 HTTP 수신기를 선택한 다음 HTTP 수신기의 연결 링크를 선택합니다.**

   HTTP 수신기의 속성을 편집할 수 있는 창이 나타납니다.

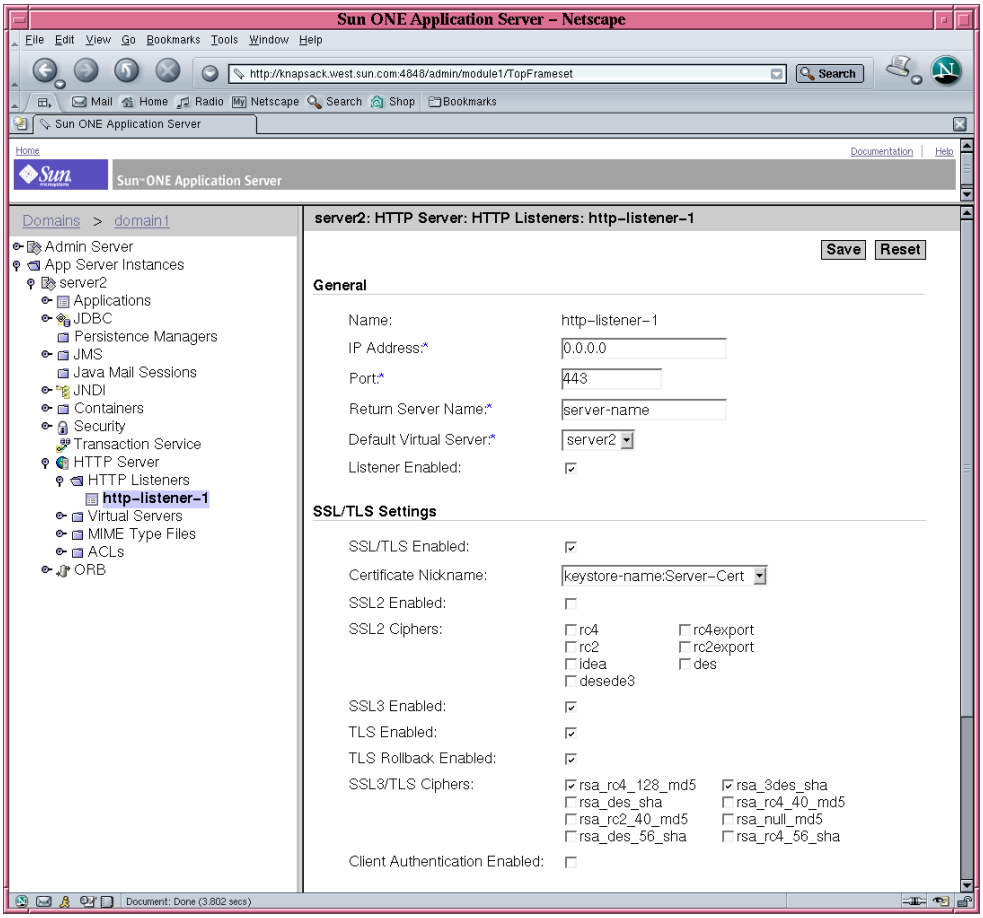

그림 5-8 Sun ONE Application Server 관리 서버의 HTTP 수신기 속성 대화 상자

5. **[Certificate Nickname(인증서 별칭)]이 137페이지의 "SSL을 위한 응용 프로그램 서버 활성화"의 1단계에서 `--certname` 명령 옵션과 함께 선택한 인증서 별칭과 일치하는지 [SSL/TLS Settings(SSL/TLS 설정)]를 확인합니다.**

6. **다음 상자를 반드시 선택합니다.**

   - SSL/TLS Enabled(SSL/TLS 활성화)
   - SSL3 Enabled(SSL3 활성화)
   - TLS Enabled(TLS 활성화)
   - TLS Rollback Enabled(TLS 롤백 활성화)
   - SSL3/TLS Ciphers(SSL3/TLS 암호): `rsa_rc4_128_md5` 및 `rsa_3des_sha`

7. **포트를 설정합니다(일반적으로 443).**

8. **롤백 기능을 사용하려면 서버에 액세스를 시도하는 브라우저에서 TLS를 활성화해야 합니다.**
   - Netscape Navigator 6.0에서는 TLS와 SSL3을 모두 선택해야 합니다.
   - Microsoft Internet Explorer 5.0 및 5.5에서는 TLS 롤백 옵션을 사용합니다.
   - TLS 롤백 기능을 사용하려면 TLS를 선택하고 SSL3과 SSL2를 모두 비활성화합니다.

9. **[Save(저장)]를 누릅니다**

10. **[App Server Instances(응용 프로그램 서버 인스턴스)]를 선택하고 왼쪽 패널에서 자신의 서버 인스턴스를 선택한 다음, 오른쪽 패널에서 [Apply Changes(변경 사항 적용)]를 선택합니다.**

11. **서버를 중지했다 다시 시작하여 변경 사항을 적용합니다.**

    `init.conf` 파일이 자동으로 수정되어 보안 기능이 활성화되며, 모든 가상 서버에 기본 보안 매개 변수가 자동으로 할당됩니다.

    서버에 SSL이 활성화되면 서버의 URL은 `http` 대신 `https`를 사용합니다. SSL이 활성화된 서버의 문서를 지정하는 URL의 형식은 다음과 같습니다.

```
https:// 서버 이름. 도메인.dom: 포트 번호
```

    예제:

```
https://admin.sun.com:443
```

참고 – 기본 보안 HTTP 포트 번호(443)를 사용하면 URL에 포트 번호를 입력할 필요가 없습니다.

다음 웹 사이트에서 *Sun ONE Application Server 7 Administrator's Guide to Security*의 SSL/TLS 활성화 항목을 참조하십시오.
`http://docs.sun.com/source/816-7158-10/sgencryp.html#14403`

Sun ONE Directory Server 5.2 설치 및 구성

이 항목에서는 Sun ONE Directory Server 5.2가 보드를 사용하도록 하기 위해 소프트웨어를 설치 및 구성하는 방법에 대해 설명합니다. 절차는 반드시 순서대로 수행해야 합니다. Sun ONE Directory Server 설치 및 사용 방법에 대한 자세한 내용은 Sun ONE Directory Server 설명서를 참조하십시오. 이 항목은 다음 절차를 설명합니다.

Sun ONE Directory Server 5.2 설치

다음은 명령행으로 디렉토리 서버 소프트웨어를 설치하는 절차입니다.

▼ Sun ONE Directory Server 5.2 설치

1. **Sun ONE Directory Server 5.2 소프트웨어를 다운로드합니다.**
   디렉토리 서버 소프트웨어는 다음 URL에 있습니다. `http://www.sun.com/`
2. **설치 디렉토리로 변경합니다.**
3. `./idsktune` **명령을 실행하여 권장 패치가 설치되어 있는지 확인합니다.**
4. **디렉토리 서버 소프트웨어를 추출합니다.**
5. `setup` **스크립트를 실행하여 소프트웨어를 설치합니다.**

참고 – `setup` 스크립트는 모든 패키지를 설치하므로 패키지를 개별적으로 설치할 필요는 없습니다.

패키지 설치가 끝나면 Sun ONE Directory Server 및 관리 서버가 자동으로 시작됩니다.

수동으로 Directory Server 시작

1. **시작 디렉토리로 변경합니다.**

```
# cd /var/Sun/mps
```

2. `start-admin` **명령을 실행합니다.**

```
# ./start-admin
```

3. `slapd-`*servername* **디렉토리로 변경합니다.**

```
# cd slapd- 서버 이름
```

여기서 *서버 이름*은 인스턴스 이름입니다.

4. `start-slapd` **명령을 입력합니다.**

```
# ./start-slapd
```

Sun ONE Directory Server 5.2 구성

다음은 디렉토리 서버 인스턴스에 대한 트러스트 데이터베이스를 생성하고 디렉토리 서버로 보드를 등록하며 서버 인증서를 생성 및 설치할 뿐 아니라, 루트 CA 인증서를 보고 설치하며 SSL을 위해 디렉토리 서버를 구성하는 절차입니다.

구성 디렉토리 및 Sun ONE Directory Server 관리 서버는 구성 프로세스 중에 반드시 실행 중이어야 합니다.

▼ 트러스트 데이터베이스 생성

다음은 Sun Crypto Accelerator 4000 모듈을 추가하는 절차이며, 32비트 및 64비트 설치에 모두 동일합니다.

1. **디렉토리 서버 콘솔을 시작합니다.**
2. **구성할 디렉토리 서버 인스턴스를 선택하고 기본 콘솔 창에서 [Open(열기)]을 선택합니다.**

3. **새 창이 나타나면 [Console(콘솔)]→[Security(보안)]→[Manage Certificates(인증서 관리)]를 선택합니다.**

   이 단계에서는 디렉토리 서버 인스턴스의 트러스트 데이터베이스를 생성합니다.

   a. **암호를 선택하고 두 상자에 입력한 다음 [OK(확인)]를 누릅니다(**그림 5-9 **참조).**

   b. **[Manage Certificates(인증서 관리)] 대화 상자를 닫습니다.**

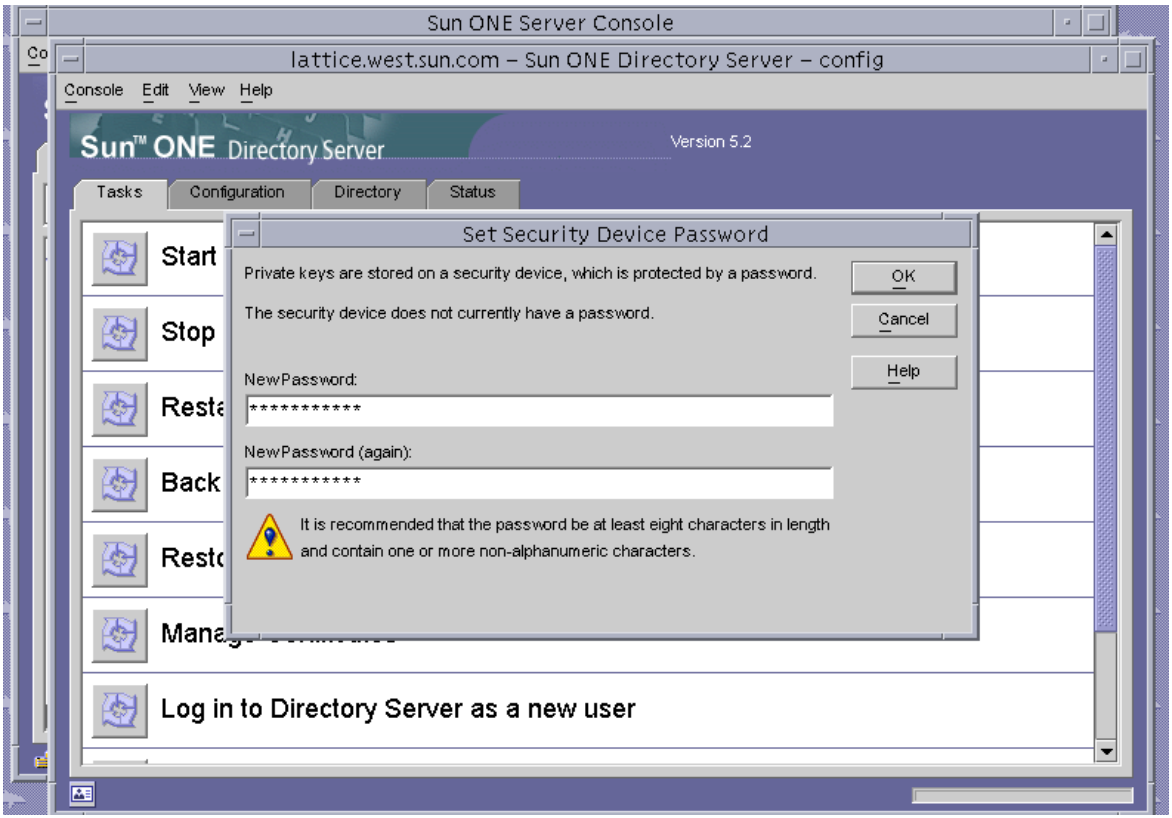

그림 5-9 Sun ONE Directory Server 보안 장치 암호 설정 대화 상자

4. **새 창이 나타나면 [Console(콘솔)]→[Security(보안)]→[Configure Security Modules (보안 모듈 구성)]를 선택합니다.**

   a. **[Install(설치)]을 누릅니다.**

   b. ***Enter the PKCS#11 module driver filename*(PKCS#11 모듈 드라이버 파일 이름 입력) 항목에 다음 경로를 입력합니다.**

```
/opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

5. ***Enter an identifying name for this module*(모듈 식별 이름 입력) 항목에 다음과 같이 이름을 입력합니다.**

```
Sun Crypto Accelerator 4000
```

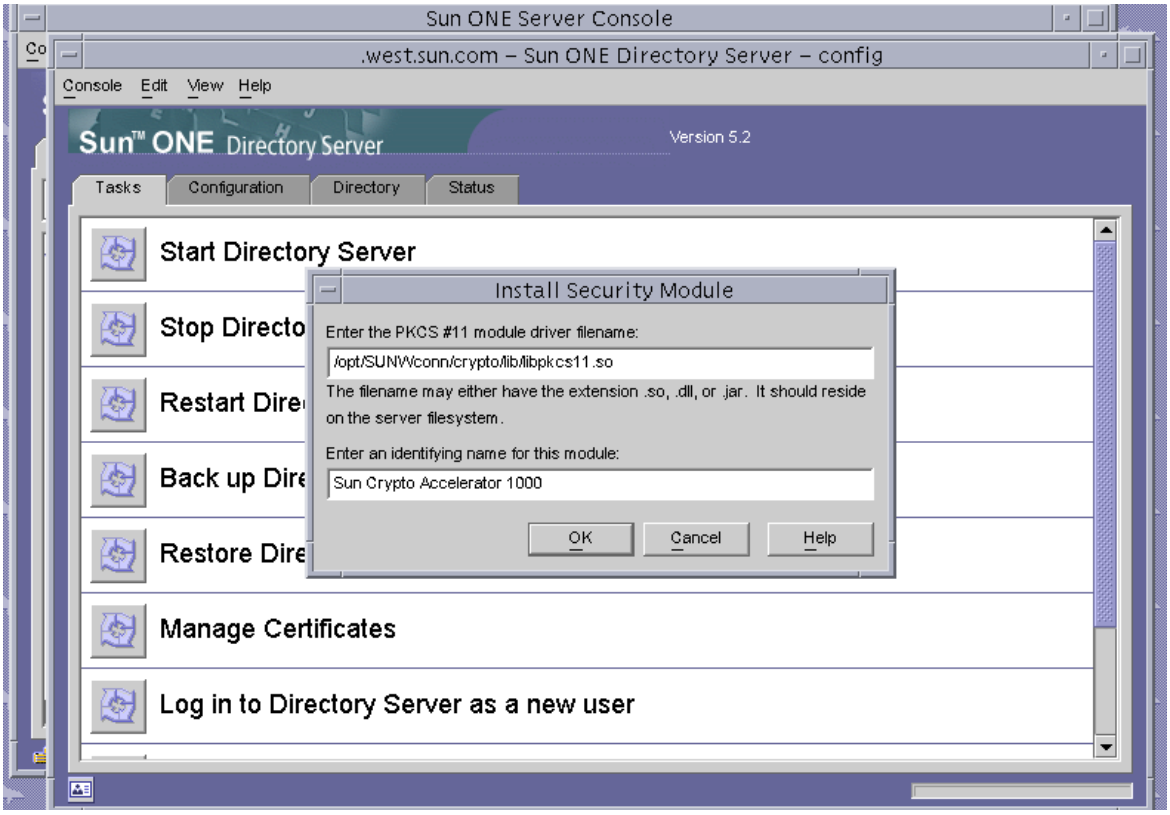

그림 5-10 Sun ONE Directory Server 보안 모듈 설치 대화 상자

6. **[OK(확인)]를 누릅니다.**

▼ Directory Server 서버에 보드 등록(32비트)

다음은 명령행으로 32비트 보드 모듈을 추가하는 절차입니다.

1. **다음 명령을 입력하여 적절한 경로를 설정합니다.**

```
# setenv LD_LIBRARY_PATH 서버 인스턴스/lib:${LD_LIBRARY_PATH}
```

2. secmod.db **데이터베이스에 보드를 추가합니다.**

   a. **다음 디렉토리로 변경합니다.**

```
# cd 서버 인스턴스 /alias
```

   b. modutil **유틸리티를 사용하여 라이브러리를 추가합니다.**

```
# 서버 인스턴스 /shared/bin/modutil -dbdir . -nocertdb -add "Sun Crypto Acclerator
4000" -libfile /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

▼ Directory Server에 보드 등록(64비트)

다음은 명령행으로 64비트 보드 모듈을 추가하는 절차입니다.

1. http://www.mozilla.org**에서 NSS(Netscape Security Services)의 64비트 버전을 다운로드합니다.**

```
ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_3_2_RTM/SunO
S5.8_64_OPT.OBJ/
```

   nss-3.3.2.tar.gz tar 파일을 저장합니다.

2. **다음 명령을 입력하여 적절한 경로를 설정합니다.**

참고 – 이 항목에서 *서버 인스턴스*는 제품의 루트 설치 디렉토리를 의미하며 *nss64 인스턴스*는 NSS 도구의 64비트 버전을 설치한 위치를 의미합니다.

```
# setenv LD_LIBRARY_PATH 서버 인스턴스 /lib/64:${LD_LIBRARY_PATH}
```

3. secmod.db **데이터베이스에 보드를 추가합니다.**

   a. **다음과 같이**alias **디렉토리로 변경합니다.**

```
# cd 서버 인스턴스 /alias
```

b. 라이브러리를 추가합니다.

```
# nss64 인스턴스/bin/modutil -dbdir . -nocertdb -add "Sun Crypto Acclerator 4000"
-libfile /opt/SUNWconn/cryptov2/lib/64/libvpkcs11.so
```

서버 인증서 생성 및 설치

표 5-8에 나와 있는 경로 변수가 다른 점을 제외하면 이 절차는 설치된 PKCS#11 라이브러리의 32비트 및 64비트 버전에 모두 동일합니다.

표 5-8 32비트와 64비트 경로 변수의 차이점

변수 정의	32비트	64비트
LD_LIBRARY_PATH	*서버 인스턴스*/lib	*서버 인스턴스*/lib/64
NSS 도구 위치	*서버 인스턴스* /shared/bin	*nss64 인스턴스*(NSS 도구가 설치된 위치에 상관 없음)

표 5-9 는 이 항목에서 certutil 명령에 사용된 변수에 대해 설명합니다.

표 5-9 certutil 변수 설명

변수	설명
토큰 이름	PKCS#11 토큰의 이름으로서 보드 초기화 시 선택한 키스토어 이름입니다.
서브젝트 이름	디지털 인증서에 표시되는 이름으로서 일반적인 형식은 다음과 같습니다. CN=*정식 도메인 이름*,OU=*소속 기관 단위*,O=*소속 기관* 이름은 소속 기관에 따라 다를 수 있습니다.
출력 파일	인증서 요청의 위치입니다.
인증서 파일	ASCII로 인코딩된 인증서의 위치입니다.
인스턴스 이름	디렉토리 서버 인스턴스 이름입니다.
별칭	사용자가 선택한 서버 인증서의 별칭입니다.

▼ 서버 인증서 생성

1. 다음 디렉토리로 변경합니다.

```
# cd 서버 인스턴스/alias
```

2. 인증서 요청

```
# certutil -R -d . -h 토큰 이름 -s " 서브젝트 이름" -a -o 출력 파일 [-g 키 크기] -P slapd-
인스턴스 이름-
```

3. 출력 파일의 인증서 요청을 선택한 인증 기관으로 전송합니다.

Base64로 인코딩된 인증서를 *인증서 파일*이라는 이름의 텍스트 파일에 넣습니다.

▼ 서버 인증서 설치

1. 서버 인증서를 설치합니다.

```
# certutil -A -d . -h 토큰 이름 -t "Pu,Pu,Pu" -P slapd- 인스턴스 이름- -a -i 인증서
파일 -n 별칭
```

루트 CA 인증서 보기 및 설치

Sun ONE Directory Server에는 현재 신뢰를 받고 있는 여러 공신력 있는 루트 인증 기관의 인증서가 들어 있습니다. 이러한 공신력 있는 루트 CA에서 발급한 서버 인증서를 갖고 있으면 이 절차를 건너뜁니다.

▼ 디렉토리 서버에서 인식하는 루트 CA 인증서 보기

1. 디렉토리 서버 콘솔 창에서 보드의 디렉토리 서버 인스턴스를 엽니다.

2. 콘솔 창 맨 위의 메뉴에서 [Console(콘솔)]→[Security(보안)]→[Manage Certificates (인증서 관리)]를 선택합니다.

3. [Manage Certificates(인증서 관리)] 창 맨 위에서 [CA Certs(CA 인증서)]를 선택합니다.

Sun ONE Directory Server 인스턴스에서 인식하는 CA 인증서 목록이 나타납니다. 항목을 선택하고 [Detail(자세히)] 단추를 누르면 지정한 CA 인증서에 대한 세부 정보를 볼 수 있습니다.

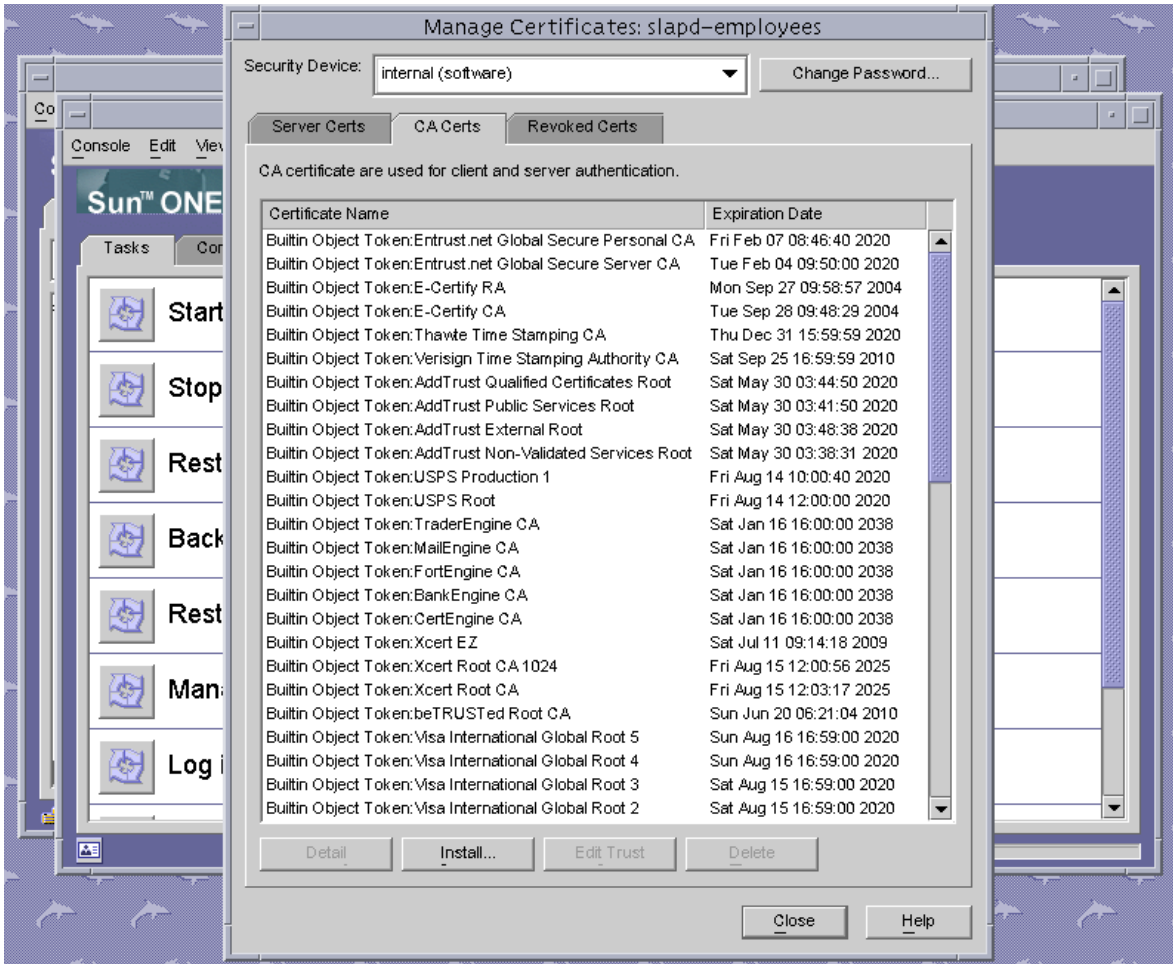

그림 5-11 Sun ONE Directory Server 인증서 관리 대화 상자

▼ 루트 CA 인증서 설치

다음 절차는 독점 소유한 PKI에서 인증서를 검색하는 경우에만 수행합니다. 다시 말해, VeriSign, Thawte 또는 GTE를 사용하는 경우에는 이 절차를 수행하지 않습니다. 이 절차는 주요 공급업체에서 발급한 인증서에 Sun ONE 기본 공신 CA 목록에 설치되지 않은 ICA(Intermediate CA)가 있는 경우를 위한 것입니다.

1. `alias` **디렉토리로 변경합니다.**

```
# cd 서버 인스턴스/alias
```

2. **루트 CA 인증서를 설치합니다.**

참고 – CA 인증서를 하나 이상 설치하는 경우 다른 -n 값을 사용합니다. 같은 -n 값을 사용하면 인증서를 서로 덮어쓰게 됩니다. CA-Cert를 CA 인증서 서브젝트 이름의 CommonName 구성 요소로 대체합니다(SubjectName에서 CN=을 찾음).

```
# certutil -A -d . -P slapd-인스턴스 이름- -n "CA-Cert" -t "CT,CT,CT" -a -i ca 인증서 경로
```

▼ SSL을 위한 디렉토리 서버 활성화

1. **디렉토리 서버 콘솔을 시작합니다.**

```
# ./cd 서버 루트
# ./startconsole
```

2. **기본 콘솔 창의 왼쪽 패널에서 보드의 디렉토리 서버 인스턴스를 두 번 눌러 디렉토리 서버 인스턴스를 엽니다.**
3. **기본 콘솔 창에서 [Directory(디렉토리)] 탭을 누릅니다.**
4. **[Directory(디렉토리)] 탭의 왼쪽 패널에서** cn=config **항목을 열고 다음 매개 변수를 수정합니다(**그림 5-12 **참조).**

   a. nsslapd-security**를 [on(설정)]으로 설정합니다.**

   b. nsslapd-secureport**를 필요한 포트로 설정합니다(기본값 636).**

c. [OK(확인)]를 누릅니다.

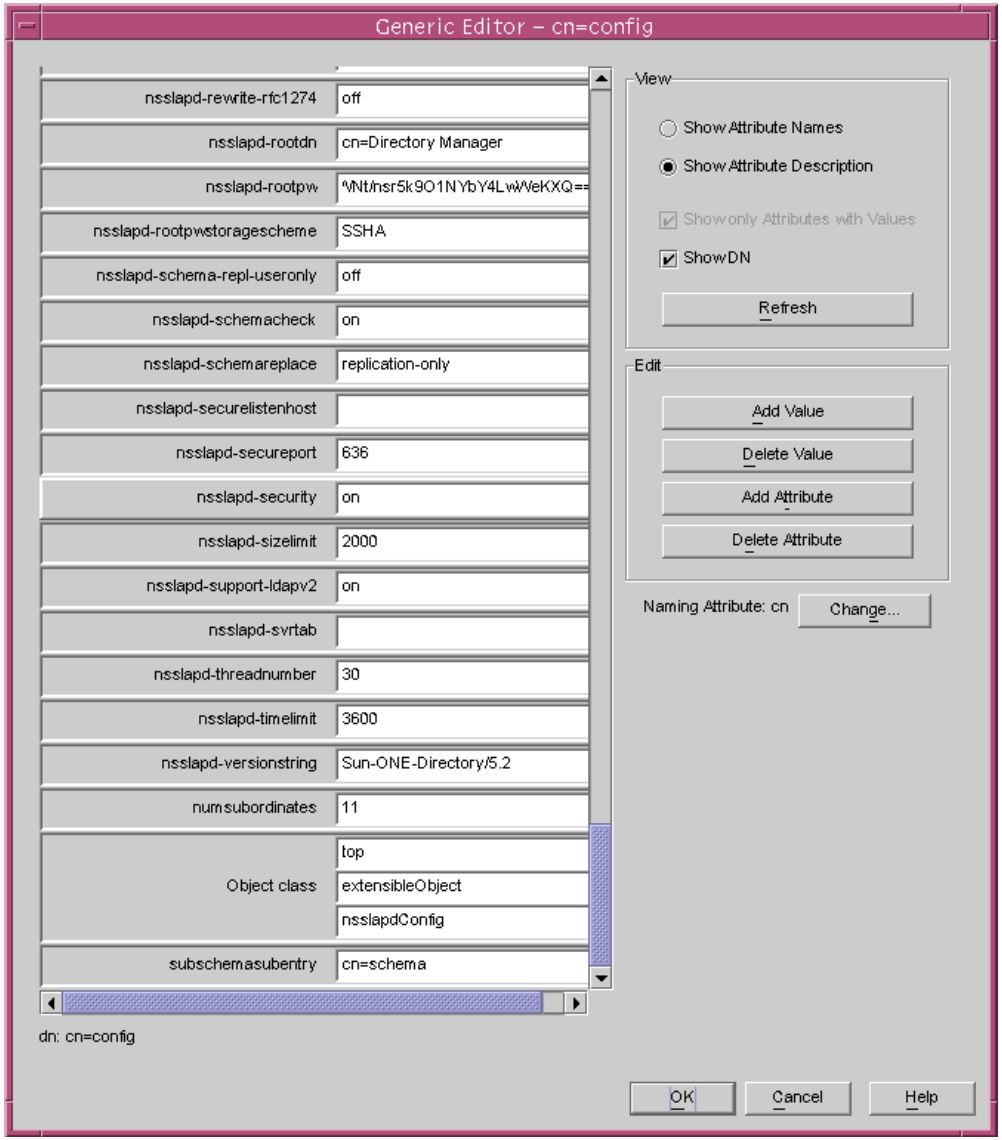

그림 5-12 Sun ONE Directory Server `cn=config` 편집기 대화 상자

5. 기본 콘솔 창의 왼쪽 패널에서 `cn=encryption,cn=config` 항목을 열고 다음 매개변수를 수정합니다(그림 5-13 **참조).**

a. `nsssl3`을 [on(설정)]으로 설정합니다.

b. [Add Attribute(속성 추가)] 단추를 사용해 `alias/slapd-`*인스턴스 이름*`-cert8.db`**의 값으로** `nsCertFile`**을 추가합니다.**

c. [Add Attribute(속성 추가)] 단추를 사용해 값이 `alias/slapd-`*인스턴스*`-key3.db` **의 값으로** `nsKeyFile`**을 추가합니다.**

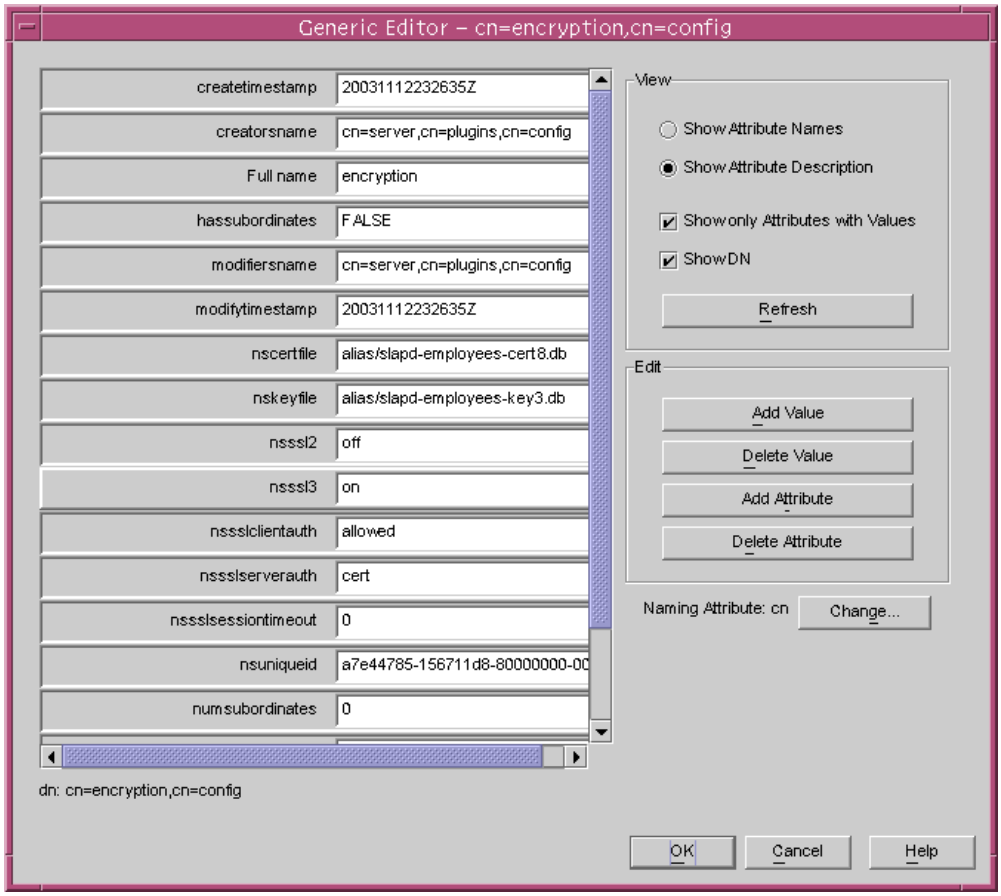

그림 5-13 Sun ONE Directory Server `cn=encryption,cn=config` 대화 상자

d. [OK(확인)]를 누릅니다.

6. `cn=encryption,cn=config`**에서 데이터베이스에 새 항목을 생성합니다**

a. 기본 창의 암호화 아이콘에서 마우스 오른쪽 단추를 눌러 [New(새로 만들기)]→ [Other(기타)]을 선택합니다.

b. `nsEncryptionModule`**을 선택합니다.**

c. [New(새로 만들기)]에서 [Full Name(전체 이름)] 속성 값을 [RSA(원격 보안 액세스)]로 변경합니다(그림 5-14 **참조).**

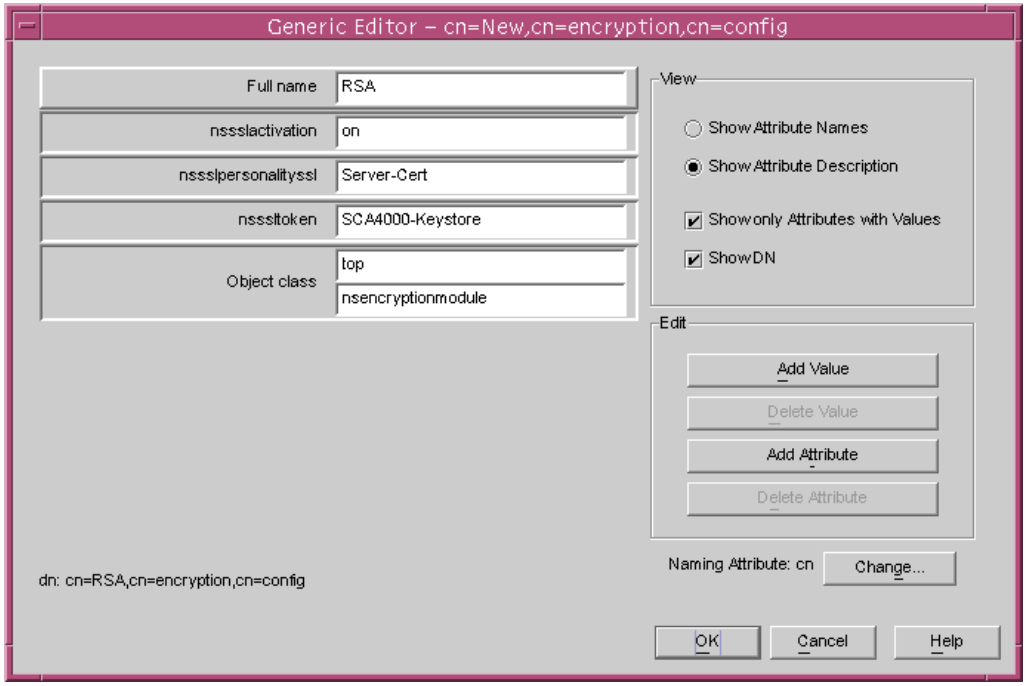

그림 5-14 Sun ONE Directory Server `nsEncryption` 모듈 대화 상자

d. [Add Attribute(속성 추가)] 단추를 사용해 다음 속성 및 값을 추가합니다.

`nsssltoken`	*토큰 이름*
`nsslpersonalityssl`	*별칭*
`nssslactivation`	`on`

e. [OK(확인)]를 누릅니다.

Sun ONE Messaging Server 5.2 설치 및 구성

이 항목에서는 Sun ONE Messaging Server 5.2가 보드를 사용하도록 하기 위해 소프트웨어를 설치 및 구성하는 방법에 대해 설명합니다. 절차는 반드시 순서대로 수행해야 합니다. Sun ONE Messaging Server 설치 및 사용 방법에 대한 자세한 내용은 Sun ONE Messaging Server 설명서를 참조하십시오. 이 항목에서는 다음을 설명합니다.

Sun ONE Messaging Server 5.2 설치

다음은 명령행으로 Sun ONE Messaging Server 5.2를 설치하는 절차입니다.

▼ Sun ONE Messaging Server 5.2 설치

1. **Sun ONE Messaging Server 5.2 소프트웨어를 다운로드합니다.**

   메시징 서버 소프트웨어는 다음 URL에서 다운받을 수 있습니다.
   `http://www.sun.com/`

2. **설치 디렉토리로 변경하고 메시징 서버 소프트웨어를 추출합니다.**

3. `setup` **스크립트를 사용하여 메시징 서버 소프트웨어를 설치합니다.**

   a. **프롬프트가 나타나면 설치 경로를 입력합니다.**

   b. **프롬프트가 나타나면 설치할 구성 요소를 입력합니다.**

   c. `./setup` **명령을 실행하여 구성 요소를 설치합니다.**

Sun ONE Messaging Server 5.2 구성

다음은 메시징 서버 인스턴스에 대한 트러스트 데이터베이스를 생성하고 메시징 서버로 보드를 등록하며 서버 인증서를 생성 및 설치할 뿐 아니라, SSL을 위해 메시징 서버를 구성하는 절차입니다.

구성 디렉토리 및 Sun ONE Messaging Server 관리 서버는 구성 프로세스 중에 반드시 실행 중이어야 합니다.

▼ 트러스트 데이터베이스 생성

1. **메시징 서버 콘솔을 시작합니다.**
2. **Sun ONE Messaging server 인스턴스를 엽니다.**

   그림 5-15의 메뉴가 나타납니다.

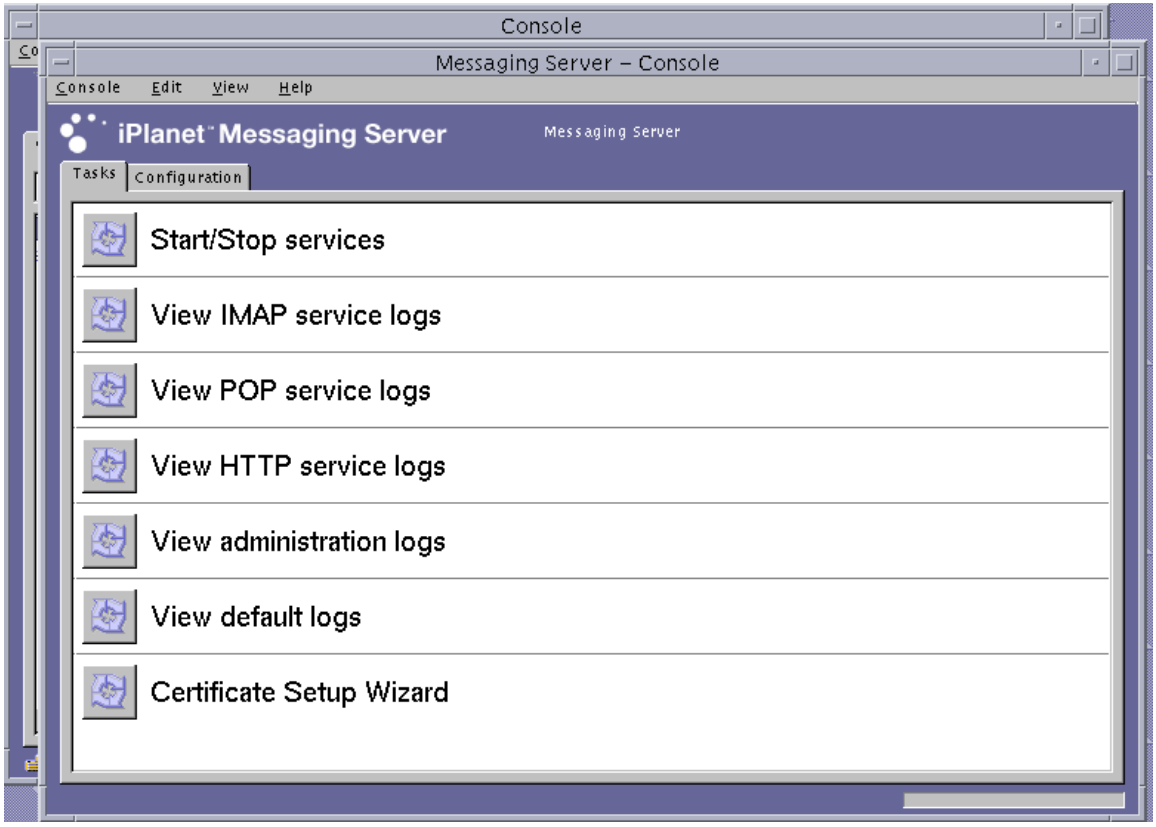

그림 5-15 Sun ONE Messaging Server 기본 콘솔 창

3. **[Console(콘솔)]→[Certificate Setup Wizard(인증서 설치 마법사)]를 선택합니다.**
   인증서 설치 마법사가 나타납니다.

   a. **[Next(다음)]를 누릅니다.**

   b. **[Internal(software)(내부(소프트웨어))] 토큰을 선택합니다.**

   c. **[Do not install a certificate(인증서를 설치하지 않음)]를 선택하고 [Next(다음)]를 누릅니다.**

   d. **[Next(다음)]를 누릅니다.**

   e. **내부 데이터베이스의 암호를 설정하고 [Next(다음)]를 누릅니다.**

   f. **[Done(완료)]을 누릅니다.**

▼ Messaging Server에 보드 등록

1. **다음 디렉토리로 변경합니다.**

```
# cd 서버 루트/shared/bin
```

2. LD_LIBRARY_PATH **변수가 제대로 설정되어 있는지 확인합니다.**

```
# setenv LD_LIBRARY_PATH 서버 루트/lib:${LD_LIBRARY_PATH}
```

3. secmod.db **데이터베이스에 보드 모듈을 추가합니다.**

```
# ./modutil -dbdir ../../admin-serv/config \
-nocertdb \
-add "Sun Crypto Accelerator 4000" \
-libfile "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
```

▼ 서버 인증서 생성

1. **인증서 설치 마법사를 열어([Console(콘솔)] -> [Certificate Setup Wizard(인증서 설치 마법사)] 선택) 메시징 서버 콘솔에서 인증서를 요청합니다.**

   a. **[Next(다음)]를 누릅니다.**

   b. 그림 5-16**과 같이 키를 저장할 Sun Crypto Accelerator 4000 토큰과 일치하는 토큰을 선택합니다.**

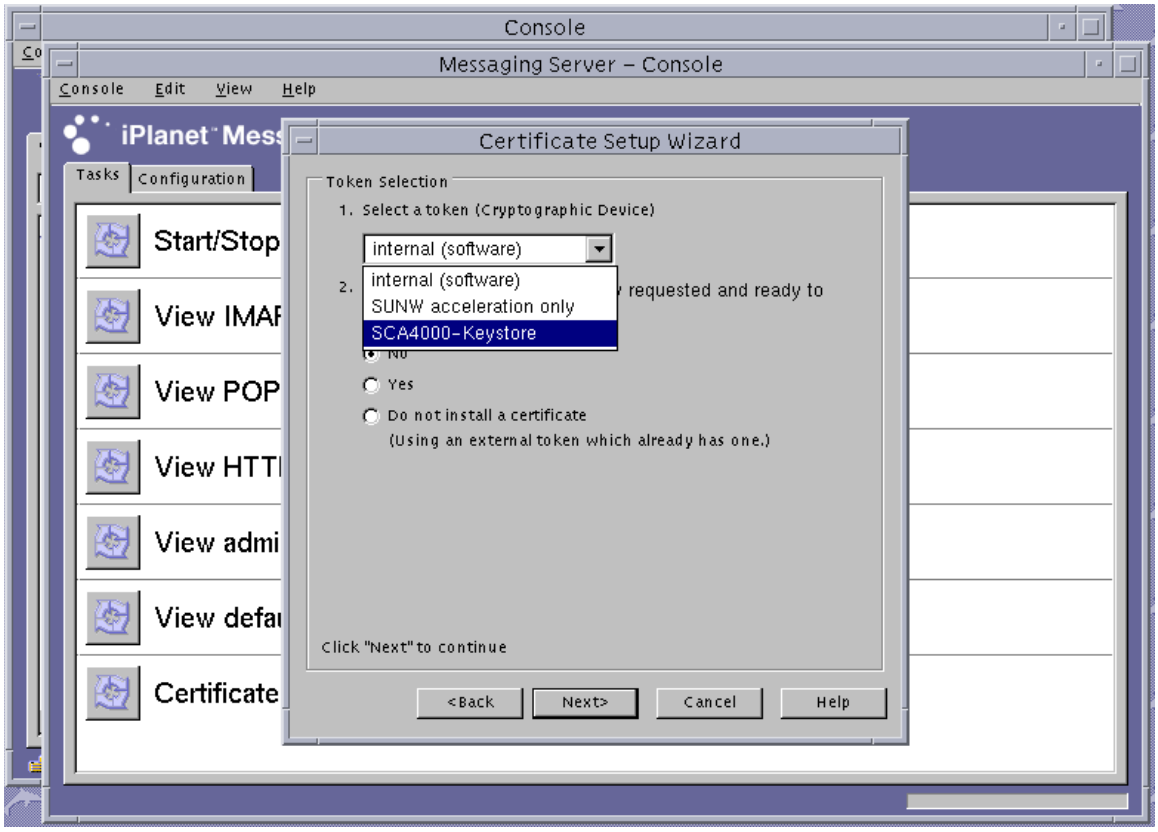

그림 5-16 Sun ONE Messaging Server 인증서 설치 마법사의 토큰 선택 대화 상자

c. [Is the certificate already requested and ready to install?(요청한 인증서를 설치할 준비가 되었습니까?)]에 [No(아니오)]로 응답하고 [Next(다음)]를 누릅니다.

d. [Next(다음)]를 누릅니다.

e. [New Certificate(새 인증서)]를 선택하고 인증서 요청을 인증 기관(그림 5-17)으로 전송할 방식(전자 우편 또는 HTTPS)을 선택한 다음 [Next(다음)]를 누릅니다.

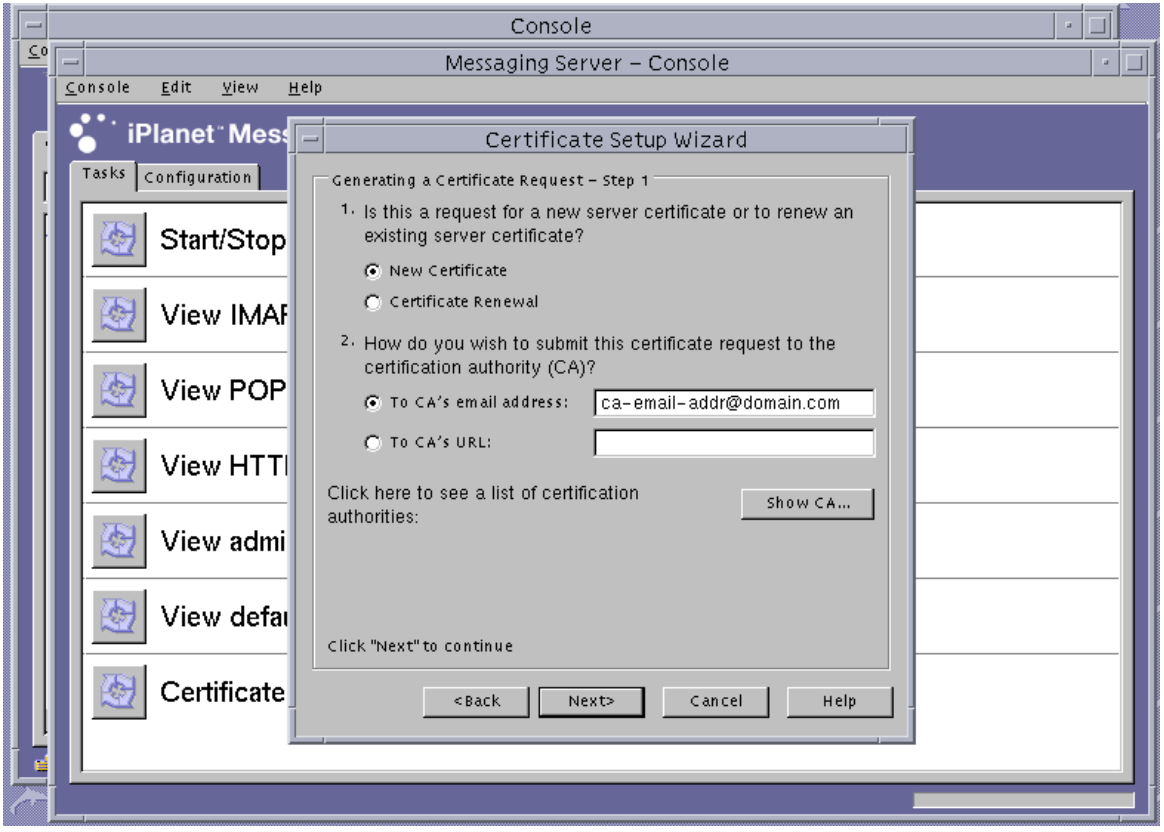

그림 5-17 Sun ONE Messaging Server 인증서 설치 마법사의 인증서 요청 대화 상자

f. 표 5-10의 요청자 정보 필드에 적절한 정보를 입력하고 [Next(다음)]를 누릅니다.

표 5-10 요청자 정보 필드

필드	설명
Requestor Name (요청자 이름):	요청자의 연락 정보
Telephone Numbe (전화 번호):	요청자의 연락 정보
Common Name (공용 이름):	방문자 브라우저에 입력된 웹 사이트 도메인

표 5-10 요청자 정보 필드*(계속)*

필드	설명
Email Address (전자 우편 주소):	요청자의 연락 정보
Organization (소속 기관):	회사 이름
Organizational Unit (소속 기관 단위):	(선택사항)회사 부서
Locality(지역):	(선택사항)시/도/군/국가
State(주):	(선택사항)주 이름
Country(국가):	두 개의 영문자로 이루어진 ISO 국가 코드(예: 미국의 경우 US)

g. 화면에 트러스트 데이터베이스 생성 시 사용한 암호를 입력하라는 요청이 표시됩니다. 대신 키스토어 사용자 암호(*사용자 이름:암호*)를 입력하고 [Next(다음)]를 누릅니다.

*사용자 이름:암호*에 대한 자세한 내용은 표 5-1을 참조하십시오.

h. e단계에서 HTTP 방식을 선택했다면 요청은 이미 CA로 전송되었습니다. e단계에서 전자 우편 방식을 선택했다면 [Copy to Clipboard(클립보드로 복사)]를 누르고 [Next(다음)]를 누릅니다(그림 5-18**).**

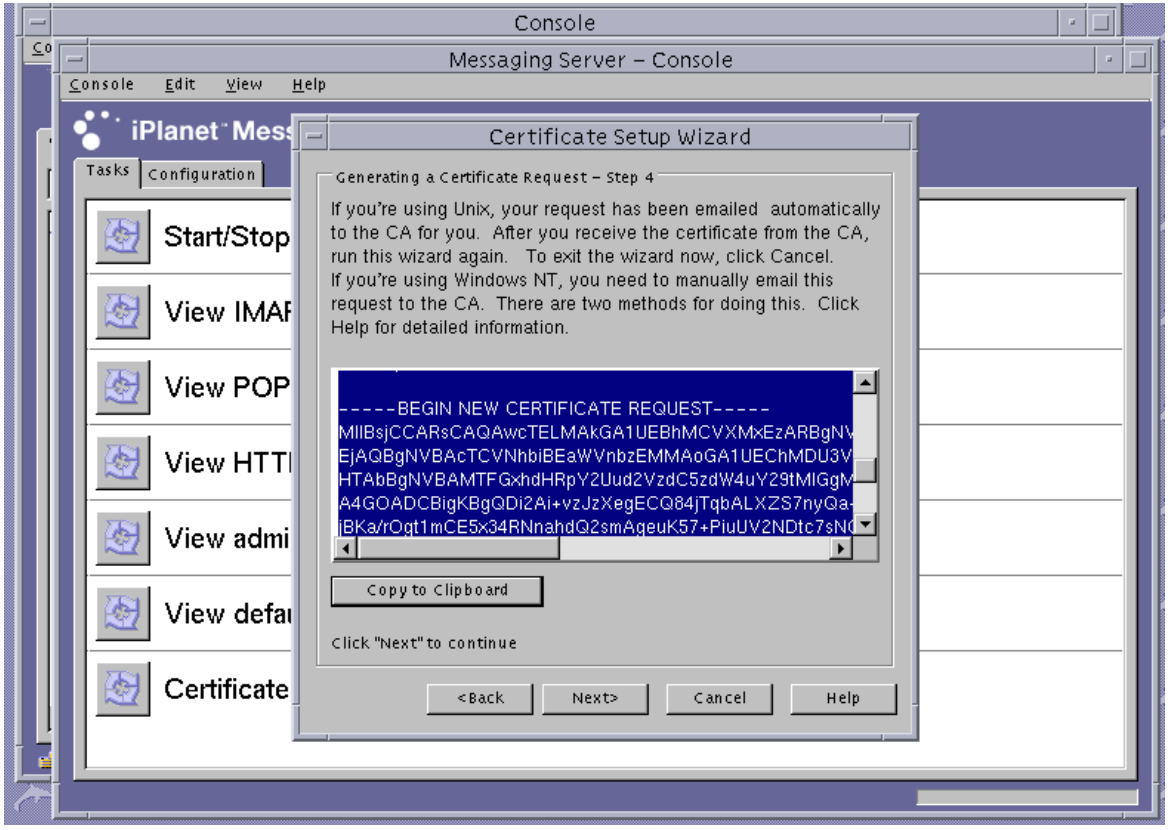

그림 5-18 Sun ONE Messaging Server 인증서 설치 마법사의 인증서 전달 대화 상자

i. [Next(다음)]를 누릅니다.

참고 – 인증서 요청이 끝난 후에도 인증서 설치 마법사를 계속 진행하여 발급된 인증서를 Sun Crypto Accelerator 4000 키스토어에 설치할 수 있습니다. 인증서를 생성한 후 이를 설치하기 전에 인증서 설치 마법사를 종료한 경우에는 인증서 설치 마법사를 중단된 부분부터 다시 시작할 수 있습니다.

▼ 서버 인증서 설치

1. **서버 인증서 생성 절차 도중 인증서 설치 마법사를 종료한 경우 [Console(콘솔)] -> [Certificate Setup Wizard(인증서 설치 마법사)]를 선택하여 마법사를 다시 시작하고 첫 번째 화면에서 [Next(다음)]를 누릅니다.**

2. **인증서를 설치할 Sun Crypto Accelerator 4000 토큰과 일치하는 토큰을 선택합니다.**
   이 토큰은 요청을 생성한 토큰과 반드시 같아야 합니다.

3. **서버 인증서의 설치 준비 여부를 묻는 질문에 [Yes(예)]로 대답하고 [Next(다음)]를 누릅니다.**

4. **[Next(다음)]를 누릅니다.**

5. **[This Server(해당 서버)]에 대한 인증서를 설치하고 마법사에서 제공하지 않은 경우 키스토어 암호(*사용자 이름:암호*)를 입력한 다음 [Next(다음)]를 누릅니다(**그림 5-19 **참조).**

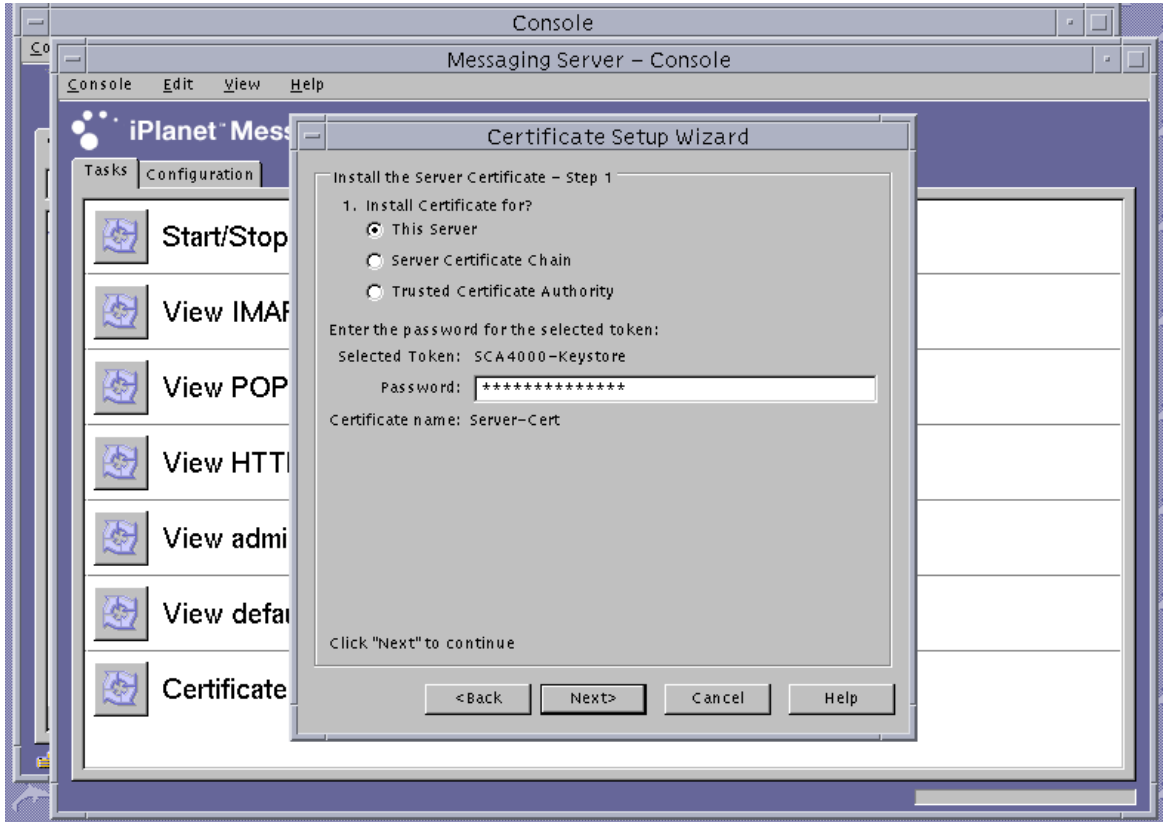

그림 5-19 Sun ONE Messaging Server 인증서 설치 마법사의 암호 대화 상자

참고 – 기본 인증서 이름은 `Server-Cert`입니다.

6. **Base 64로 인코딩된 인증서를 클립보드로 복사하고 [The certificate is located in the following text field(인증서는 다음 텍스트 필드에 있습니다)]라고 표시된 텍스트 상자에 붙여 넣은 다음 [Next(다음)]를 누릅니다(**그림 5-20 **참조).**

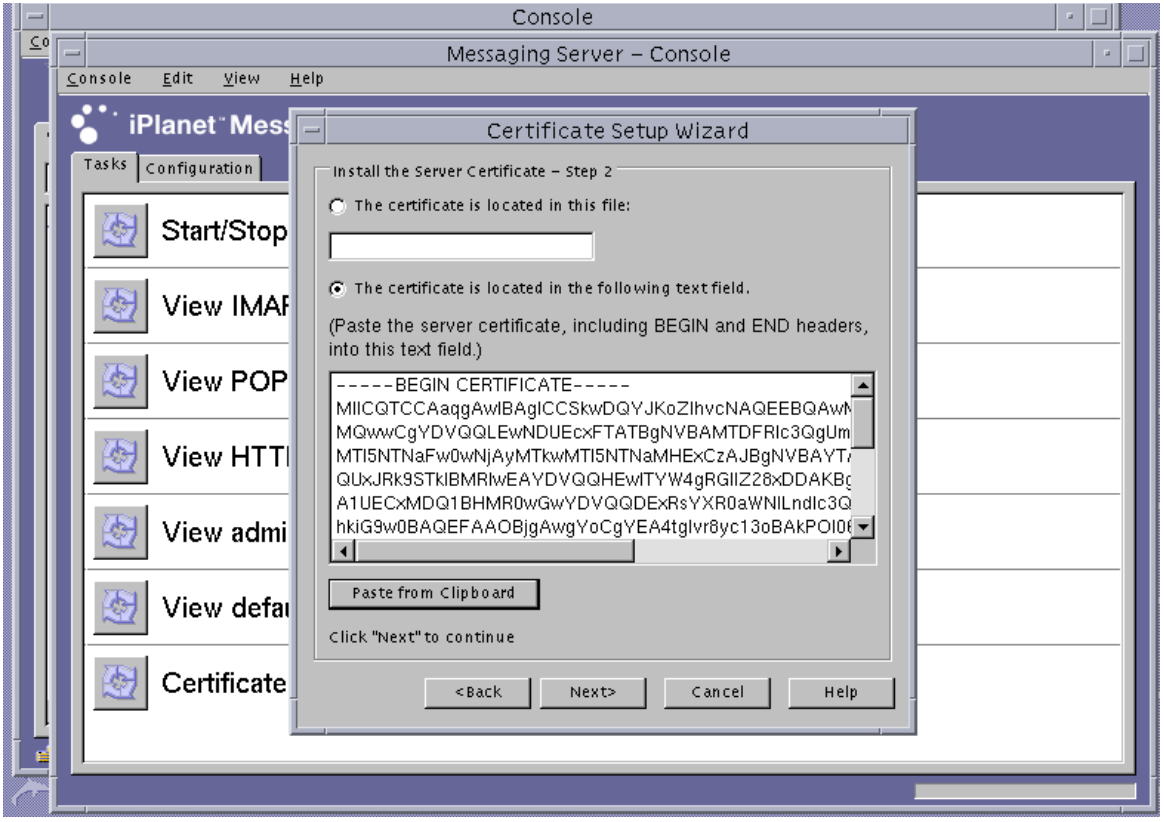

그림 5-20 Sun ONE Messaging Server 인증서 설치 마법사의 인증서 입력 대화 상자

   a. **[Add(추가)]를 눌러 인증서를 추가합니다.**

   b. **[Done(완료)]을 누릅니다.**

7. **루트 CA 인증서를 추가합니다(메시징 서버에서 신뢰하는 루트 인증 기관에서 발급되지 않은 경우).**

   이 단계는 인증서 설치 마법사를 사용하여 수행합니다.

   a. **메시징 서버 콘솔에서 [Console(콘솔)]→[Certificate Setup Wizard(인증서 설치 마법사)]를 선택합니다.**

b. **[Next(다음)]를 누릅니다.**

c. **[Internal(software)(내부(소프트웨어))]를 토큰으로 선택하고 [Is the certificate already requested and ready to install(요청한 인증서를 설치할 준비가 되었습니까?)]에 대해 [Yes(예)]를 누른 다음 [Next(다음)]를 누릅니다.**

d. **[Next(다음)]를 누릅니다.**

e. **[Trusted Certificate Authority(신뢰하는 인증 기관)]를 선택하고 [Next(다음)]를 누릅니다.**

f. **Base 64로 인코딩된 인증서를 클립보드로 복사하고 [The certificate is located in the following text field(인증서는 다음 텍스트 필드에 있습니다)]로 표시된 텍스트 상자에 붙여 넣은 다음 [Next(다음)]를 누릅니다.**

g. **[Add(추가)]를 눌러 인증서를 추가합니다(**그림 5-21**).**

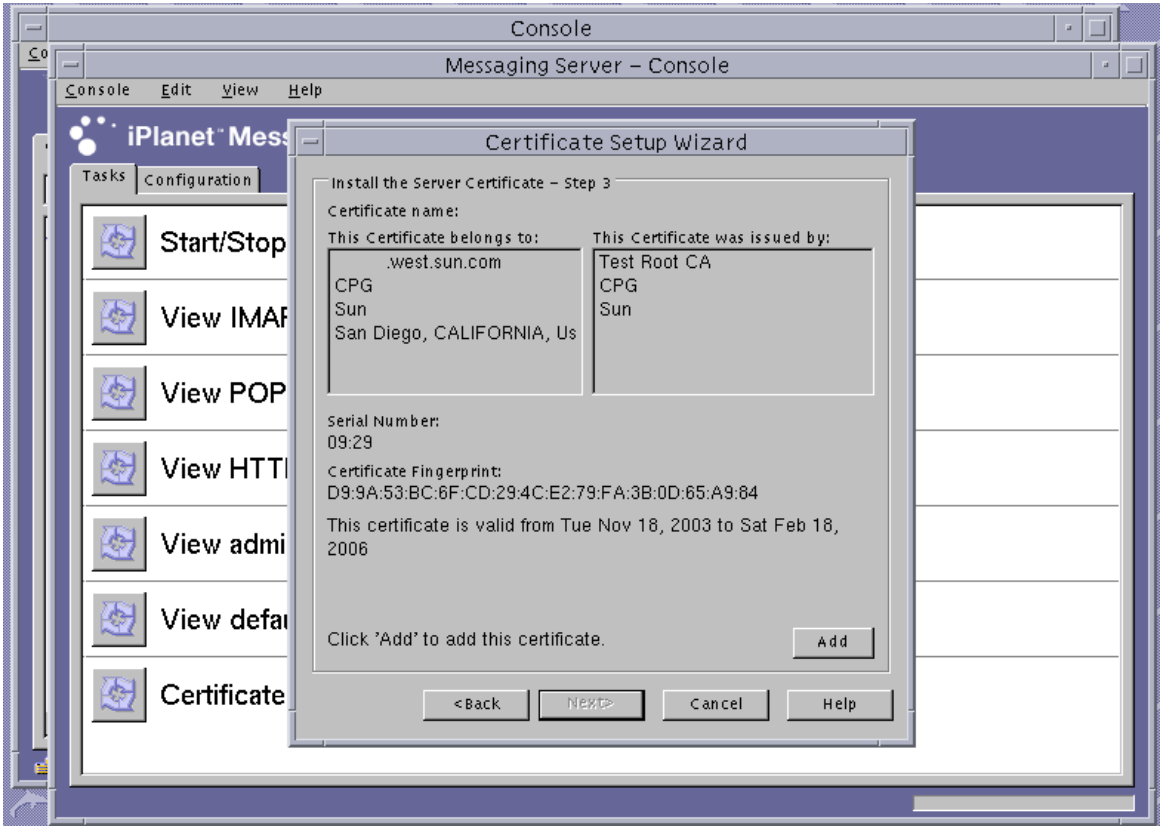

그림 5-21 Sun ONE Messaging Server 인증서 설치 마법사의 암호 대화 상자

h. **[Done(완료)]을 누릅니다.**

▼ SSL을 위한 메시징 서버 활성화

1. `su` 명령을 사용하여 메시징 서버를 실행하기 위해 선택한 사용자로 전환합니다.

이 사용자 이름이 기억나지 않는 경우
서버 루트/msg-*인스턴스 이름*/config/msg.conf 파일에서 `local.serveruid` 속성을 검색하여 사용자 이름을 찾습니다.

```
# cd 서버 루트 /msg- 인스턴스 이름
# su 사용자 이름
```

2. `configutil` 도구를 사용하여 메시징 서버에 대한 SSL 매개 변수를 설정합니다.

표 5-11은 `configutil` 도구에서 사용되는 변수의 정의를 설명합니다.

표 5-11 `configutil` 변수 정의

변수	정의
키스토어 이름	1단계에 사용된 키스토어 이름입니다.
인증서 이름	사용할 인증서에 대한 별칭입니다. 기본값은 `Server-Cert`입니다.
포트 번호	SSL에서 POP3를 실행할 포트 번호로, 일반적으로 995입니다.

```
# ./configutil -o nsserversecurity -v on
# ./configutil -o encryption.rsa.nsssslactivation -v on
# ./configutil -o encryption.rsa.nssstoken -v 키스토어 이름
# ./configutil -o encryption.rsa.nssslpersonalityssl -v 인증서 이름
# ./configutil -l -o service.pop.enablesslport -v yes
# ./configutil -l -o service.pop.sslport -v 포트 번호
```

3. 메시징 서버 콘솔에서 Sun ONE Messaging Server 인스턴스 관리에 사용하는 콘솔 창의 [Configuration(구성)] 탭을 누릅니다. [Messaging Server(메시징 서버)]의 [System(시스템)] 탭 -> [Services(서비스)] -> IMAP를 차례로 누릅니다.

4. 위 창에서 [Use separate port for IMAP over SSL(SSL 상의 IMAP에 개별 포트 사용)]에 대해 포트 번호를 설정합니다. 이 포트의 기본값은 993입니다.

5. **메시징 서버 인스턴스에 대해** `sslpassword.conf` **파일을 구성합니다.**

```
# cd 서버 루트 /msg- 인스턴스 이름 /config
# vi sslpassword.conf
```

`Internal (Software) token:netscape!` 행을 *토큰 이름:사용자 이름:암호*로 대체합니다. 여기서 *토큰 이름*은 키스토어 이름입니다. 이 토큰 이름은 1단계에서 키를 생성하기 위해 선택한 토큰의 이름입니다. *사용자 이름:암호*는 이 토큰에 대한 인증을 받기 위해 사용합니다. *사용자 이름:암호*에 대한 자세한 내용은 표 5-1을 참조하십시오.

6. `sslpassword.conf` **파일의 소유권 및 권한을 변경합니다.**

`sslpassword.conf` 파일에는 키 요소에 대한 인증을 받기 위해 사용하는 암호 정보가 들어 있으므로 이 파일은 데몬을 실행하는 사용자가 소유해야 하며 해당 사용자만 읽을 수 있어야 합니다.

```
# cd 서버 루트 /msg- 인스턴스 이름 /config
# chown msg 사용자 sslpassword.conf
# chmod 0400 sslpassword.conf
```

7. **명령행에서 서버를 다시 시작합니다.**

```
# cd 서버 루트
# msg- 인스턴스 이름 /start-msg
```

Sun ONE Portal Server 6.2 설치 및 구성

이 항목에서는 Sun ONE Portal Server 6.2가 보드를 사용하도록 하기 위해 소프트웨어를 설치 및 구성하는 방법에 대해 설명합니다. 절차는 반드시 순서대로 수행해야 합니다. Sun ONE Portal Server 설치 및 사용 방법에 대한 자세한 내용은 Sun ONE Portal Server 설명서를 참조하십시오. 이 항목은 다음 절차를 설명합니다.

이 항목에서는 Sun ONE Portal Server 6.2가 보드를 사용하도록 하기 위해 소프트웨어를 설치 및 구성하는 방법에 대해 설명합니다. 절차는 반드시 순서대로 수행해야 합니다. Sun ONE Portal Server 설치 및 사용 방법에 대한 자세한 내용은 Sun ONE Portal Server 설명서를 참조하십시오.

Sun ONE Portal Server 6.2에는 Sun ONE Web Server 6.0이 포함되어 있습니다. Sun ONE Web Server 소프트웨어는 포털 서버를 설치 및 구성하기 전에 설치하고 구성해야 합니다(117페이지의 "Sun ONE Web Server 6.0 설치 및 구성" 참조).

참고 – Sun ONE Web Server를 포털 서버와 함께 사용하기 위해 구성 및 설치하는 경우에는 설치 경로로 `/opt/SUNWam/servers`를 사용합니다.

Sun ONE Portal Server 6.2 설치

이 항목에서는 명령행으로 Sun ONE Portal Server 6.1을 설치하는 방법에 대해 설명합니다.

▼ Sun ONE Portal Server 6.2 설치

1. **Sun ONE Portal Server 6.1 소프트웨어를 다운로드합니다.**

   포털 서버 소프트웨어는 다음 URL에서 다운받을 수 있습니다.
   `http://www.sun.com/`

2. **설치 디렉토리로 변경하고 포털 서버 소프트웨어를 추출합니다.**

3. `setup` **스크립트를 사용하여 포털 서버 소프트웨어를 설치합니다.**

   a. **프롬프트가 나타나면 설치 경로를 입력합니다.**

   b. **프롬프트가 나타나면 설치할 구성 요소를 입력합니다.**

   c. `./setup` **명령을 실행하여 구성 요소를 설치합니다.**

참고 – 트러스트 데이터베이스는 설치 도중 자동으로 생성됩니다.

Sun ONE Portal Server 6.2 구성

다음은 포털 서버 SRA(secure remote access) 게이트웨이를 구성하고 포털 서버로 보드를 등록하며 서버 인증서를 생성 및 설치할 뿐 아니라, SSL을 위해 포털 서버를 구성하는 절차입니다.

시작하기 전에 SRA와 게이트웨이 서버 인증서(자체 서명되었거나 CA에서 발급한)가 설치되었는지 확인합니다. Sun ONE Portal Server 관리 서버는 구성 프로세스 중에 반드시 실행 중이어야 합니다.

▼ Portal Server에 보드 등록

1. vcaadm **유틸리티를 사용하여 보드의 새 사용자 계정을 생성합니다(55페이지의 "vcaadm 유틸리티 사용" 참조).**

```
vcaadm{vca0@localhost, sec-officer}> create user
New user name: 사용자 이름
Enter new user password:
Confirm password:
User crypta created successfully.
```

2. **Sun Crypto Accelerator 4000 모듈을 로드합니다.**

   LD_LIBRARY_PATH 변수는 반드시 다음을 지정하고 있어야 합니다.

```
/usr/lib/mps/secv2/
```

   a. 모듈을 로드합니다.

```
# /usr/bin/mps/modutil -dbdir /etc/opt/SUNWps/cert/default -add "Sun Crypto
Accelerator 4000" -libfile /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

   b. 이 모듈이 로드되었는지 확인합니다.

```
# /usr/bin/mps/modutil -list -dbdir /etc/opt/SUNWps/cert/default -nocertdb
```

서버 인증서 생성 및 설치

절차 수행 시 LD_LIBRARY_PATH 환경 변수는 반드시 다음을 지정하고 있어야 합니다.

```
/usr/lib/mps/secv1/
```

표 5-12는 이 항목에서 certutil 명령에 사용된 변수에 대해 설명합니다.

표 5-12 certutil 변수 설명

변수	설명
토큰 이름	PKCS#11 토큰의 이름으로서 보드 초기화 시 선택한 키스토어 이름입니다.
서브젝트 이름	디지털 인증서에 표시되는 이름으로서 일반적인 형식은 다음과 같습니다. CN=*정식 도메인 이름*, OU=*소속 기관 단위*, O=*소속 기관* 이름은 소속 기관에 따라 다를 수 있습니다.
출력 파일	인증서 요청의 위치입니다.
인증서 파일	ASCII로 인코딩된 인증서의 위치입니다.
인스턴스 이름	Portal server 인스턴스의 이름입니다.
별칭	사용자가 선택한 서버 인증서의 별칭입니다.

▼ 서버 인증서 생성

1. 다음 디렉토리로 변경합니다.

```
# cd /etc/opt/SUNWps/cert/default
```

2. 인증서를 요청합니다.

```
# /usr/bin/mps/bin/certutil -R -d . -h 토큰 이름 -s " 서브젝트 이름 " -a -o 출력 파일
[-g 키 크기 ]
```

3. *출력 파일*의 인증서 요청을 선택한 인증 기관으로 전송합니다.

Base64로 인코딩된 인증서를 *인증서 파일*이라는 이름의 텍스트 파일에 넣습니다.

▼ 서버 인증서 설치

1. 서버 인증서를 설치합니다.

```
# /usr/bin/mps/certutil -A -d . -h 토큰 이름 -t "Pu,Pu,Pu" -a -i 인증서 파일 -n 별칭
```

루트 CA 인증서 보기 및 설치

Sun ONE Portal Server에는 현재 신뢰를 받고 있는 여러 공신력 있는 루트 인증 기관의 인증서가 들어 있습니다. 이러한 공신력 있는 루트 CA에서 발급한 서버 인증서를 갖고 있으면 이 절차를 건너뜁니다.

▼ 포털 서버에서 인식하는 루트 CA 인증서 보기

- **다음 명령을 입력합니다.**

```
# /usr/bin/mps/certutil -L -d /etc/opt/SUNWps/cert/default
```

▼ 루트 CA 인증서 설치

다음 절차는 독점 소유한 PKI에서 인증서를 검색하는 경우에만 수행합니다. 다시 말해, VeriSign, Thawte 또는 GTE를 사용하는 경우에는 이 절차를 수행하지 않습니다. 이 절차는 주요 공급업체에서 발급한 인증서에 Sun ONE 기본 공신 CA 목록에 설치되지 않은 ICA(Intermediate CA)가 있는 경우를 위한 것입니다.

1. 인증서 데이터베이스 디렉토리로 변경합니다.

```
# cd /etc/opt/SUNWps/cert/default
```

2. 루트 CA 인증서를 설치합니다.

참고 – CA 인증서를 하나 이상 설치하는 경우 다른 -n 값을 사용합니다. 같은 -n 값을 사용하면 인증서를 서로 덮어쓰게 됩니다. CA-Cert를 CA 인증서 서브젝트 이름의 CommonName 구성 요소로 대체합니다(SubjectName에서 CN=을 찾음).

```
# /usr/bin/mps/certutil -A -d . -n "CA-Cert" -t "CT,CT,CT" -a -i ca 인증서 경로
```

▼ SSL을 위한 포털 서버 활성화

1. `/etc/opt/SUNWps/cert/default/.nickname` **파일을 생성합니다.**

```
# vi /etc/opt/SUNWps/cert/default/.nickname
```

파일에는 공백 없이 다음 행만 들어 있어야 합니다.

```
키스토어 이름: 서버 인증서
```

2. 가속화 암호를 선택합니다.

참고 – Sun Crypto Accelerator 4000 하드웨어에서 DES 및 3DES 알고리즘을 가속화하려면 `/etc/opt/SUNWconn/cryptov2/sslreg` 파일을 제공해야 합니다. 103페이지의 "대량 암호화 활성화 및 비활성화"를 참조하십시오.

보드는 RSA 기능을 가속화하지만 DES 및 3DES 암호에 대해서만 가속화를 지원합니다. 이 암호 중 하나를 활성화하려면 다음과 같이 합니다.

```
Gateway >> Security >> Enable SSL Cipher Selection: >> SSL3
Ciphers: >>
SSL3_RSA_WITH_3DES_EDE_CBC_SHA or
SSL3_RSA_WITH_DES_CBC_SHA
```

3. `/etc/opt/SUNWps/platform.conf.`*게이트웨이 프로파일 이름***을 수정하여 보드를 활성화합니다.**

```
gateway.enable.accelerator=true
```

4. 터미널 창에서 게이트웨이를 다시 시작합니다.

```
# InstallDir/SUNWps/bin/gateway -n gateway-profile-name start
```

게이트웨이에서 키스토어 암호를 입력하라는 메시지를 표시합니다. *sra 키스토어:사용자 이름:암호*의 암호 또는 핀을 입력합니다.

6 장

Apache Web Server 소프트웨어 설치 및 구성

이 장은 Apache Web Server이 보드를 사용하도록 하기 위해 소프트웨어를 설치 및 구성하는 방법에 대해 설명하며 다음 항목으로 구성되어 있습니다.

- 170페이지의 "Apache Web Server 1.3x 구성"
- 176페이지의 "Apache Web Server 2.x 구축 및 구성"
- 180페이지의 "재부팅 시 무인 시작되도록 Apache Web Server 구성"
- 181페이지의 "Sun Crypto Accelerator 4000 소프트웨어 설치 후 Apache와 함께 사용하기 위해 Sun Crypto Accelerator 1000 구성"

다음은 보드를 사용하기 위해 Apache Web Server를 구성하는 데 필요한 소프트웨어 요구 사항입니다.

- Apache Web Server 1.3.26 이상 — 1.3.26 버전은 Sun Crypto Accelerator 4000 소프트웨어에 들어 있음
- Solaris 8용 109234-09 패치(`http://sunsolve.sun.com`)
- Solaris 9용 113146-02 패치9(`http://sunsolve.sun.com`)
- Sun Crypto Accelerator 4000 소프트웨어에 들어 있는 `SUNWkcl2a` 패키지

`SUNWkcl2a` 패키지가 추가되면 시스템은 Apache Web Server 및 mod_ssl 1.3.26으로 구성됩니다.

참고 – Apache Web Server는 5장 100페이지의 "개념 및 용어"에 설명된 키스토어나 사용자 계정 기능은 사용하지 않습니다.

주의 – Apache Web Server로 Sun Crypto Accelerator 1000 보드와 Sun Crypto Accelerator 4000 보드를 동시에 사용하도록 구성하지 마십시오. 이렇게 구성하면 Apache가 올바르게 작동되지 않습니다.

참고 – Apache Web Server 소프트웨어의 대량 암호화 기능은 기본적으로 활성화되어 있으며 비활성화할 수 없습니다.

Apache Web Server 1.3x 구성

이 항목에서는 apsslcfg 스크립트를 사용해 웹 서버에서 보드를 사용하도록 구성하는 방법에 대해 설명합니다. 또한 서버 인증서의 생성 및 설치 방법도 함께 설명합니다.

▼ Apache Web Server 구성

1. **httpd 구성 파일이 없으면 하나를 생성합니다.**

   Solaris 시스템인 경우 httpd.conf-example 파일은 일반적으로 /etc/apache 디렉토리 안에 있습니다. 이 파일을 템플릿으로 사용하여 다음 방법으로 복사할 수 있습니다.

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

2. **ServerName을 http.conf 파일의 서버 이름으로 교체합니다.**

3. **apsslcfg를 시작합니다.**

```
# /opt/SUNWconn/cryptov2/bin/apsslcfg
```

4. **1을 선택하여 SSL을 사용할 Apache Web Server를 구성합니다.**

참고 – 여기서는 이 프롬프트에서 1 옵션을 선택하는 경우에 대한 절차를 설명합니다. 2 옵션을 선택하려면 93페이지의 "apsslcfg 스크립트 사용"을 참조하십시오.

```
Sun Crypto Accelerator Apache 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. **Apache 바이너리의 경로를 입력합니다.**
   Solaris 시스템인 경우, 이 경로는 일반적으로 /usr/apache입니다.

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

6. **Apache 구성 파일의 경로를 입력합니다.**
   Solaris 시스템인 경우, 이 경로는 일반적으로 /etc/apache입니다.

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

7. **시스템의 RSA(원격 보안 액세스) 키 쌍을 생성합니다.**
   키 쌍 생성을 선택하지 않을 경우 이후에는 apsslcfg를 사용해 키를 생성해야 합니다.

```
Do you wish to create a new RSA keypair and certificate request? [Y/N]: Y
```

   [No]로 응답한 경우 173페이지의 "서버 인증서 생성"으로 건너뜁니다.

8. **키를 저장할 디렉토리를 제공합니다.**
   이 디렉토리가 존재하지 않을 경우에는 새로 생성됩니다.

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

9. 키 요소의 기본 이름을 선택합니다.

이 이름에는 키 파일, 인증서 요청 파일 및 인증서 파일과 서로 구별되도록 하기 위해 다른 접미사가 추가됩니다.

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

10. 키의 길이는 512비트에서 2,048비트 사이로 제공합니다.

대부분의 웹 서버 응용 프로그램에는 1,024비트 정도면 충분하지만 필요한 경우 더 강력한 키를 사용할 수 있습니다.

```
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. PEM 패스 문구를 생성합니다.

패스 문구는 키 요소를 보호합니다. 안전하면서도 쉽게 기억할 수 있는 패스 문구를 선택해야 합니다. 패스 문구를 잊을 경우 해당 키에 액세스할 수 없습니다.

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

주의 – 입력한 패스 문구는 반드시 기억해야 합니다. 패스 문구가 없으면 해당 키에 액세스할 수 없습니다. 잊은 패스 문구를 찾을 수 있는 방법은 없습니다.

▼ 서버 인증서 생성

1. 170페이지의 "Apache Web Server 구성"의 7단계에서 생성한 키를 사용하여 인증서 요청을 작성합니다.

a. 암호를 입력하여 키에 액세스합니다. 그런 다음, 요청자 정보 필드에 적절한 정보를 입력합니다.

표 6-1 에는 요청자 정보 필드에 대한 설명이 나와 있습니다.

```
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) []: 회사
Organizational Unit Name (eg, section) []: 부서
SSL Server Name (eg, www.company.com) []:www.company.com
Email Address []:admin@company.com
```

표 6-1 요청자 정보 필드

필드	설명
Country Name (국가 이름):	두 개의 영문자로 이루어진 ISO 국가 코드(예: 미국의 경우 US)
State or Province Nam(주/도 이름):	(선택사항)주/도의 전체 이름(또는 마침표(.)를 입력할 수 있음)
Locality(지역):	시/도/군/국가
Organization Name (소속 기관 이름)	회사 이름
Organizational Unit Name(소속 기관 단위 이름):	회사 부서
SSL Server Name (SSL 서버 이름):	방문자 브라우저에 입력되는 웹 사이트 도메인
Email Address (전자 우편 주소):	요청자의 연락 정보

2. **/etc/apache/httpd.conf 파일을 지침에 따라 수정합니다.**

   키와 인증서 파일 관련 정보 및 /etc/apache/httpd.conf 파일 수정 방법에 대한 지침이 나타납니다.

```
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
```

참고 – 해당 구성에 대한 정확한 *버전 번호*가 표시됩니다.

3. VirtualHost **설정을 선택하지 않은 경우,** httpd.conf **파일의** SSLEngine, SSLCertificateFile **및** SSLCertificateKeyFile **지시어를** SSLPassPhraseDialog **지시어 바로 위에 넣습니다.**

```
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>
```

178페이지의 "Apache Web Server 2.x 구성"의 7단계 질문에 아니오라고 대답한 경우, 키 요소 작성 방법에 대한 추가 정보가 제공됩니다.

```
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. apsslcfg **작업이 완료되면** 0**을 선택하여 이를 종료합니다.**

▼ 서버 인증서 설치

1. **/etc/apache/keys/*기본 이름*-certreq.pem 파일(*기본 이름*이 170페이지의 "Apache Web Server 구성"의 9단계에서 설정됨)에서 헤더와 함께 인증서 요청을 복사한 다음 해당 인증 기관으로 전송합니다.**

2. **인증서가 생성되면 인증서 파일 /etc/apache/keys/*기본 이름*-cert.pem을 작성한 후 이를 해당 파일에 붙여 넣습니다.**

3. **Apache Web Server를 시작합니다.**

   다음은 Apache 바이너리 디렉토리를 /usr/apache/bin으로 가정한 것입니다. 사용자의 바이너리 디렉토리가 아닌 경우 올바른 경로를 입력합니다.

```
# /usr/apache/bin/apachectl sslstart
```

4. **프롬프트가 나타나면 PEM 패스 문구를 입력합니다.**

5. **브라우저에서 다음 URL을 입력하여 SSL이 활성화된 새 웹 서버를 확인합니다:**
   https://*서버 이름:서버 포트*/

   기본 *서버 포트*는 443입니다.

참고 – 테스트를 위한 인증서 자가 서명 방법에 대한 내용은 mod_SSL 및 OpenSSL 설명서를 참조하십시오.

Apache Web Server 2.x 구축 및 구성

Sun Crypto Accelerator 4000 소프트웨어에는 Apache 2.x Web Server용 mod_ssl 라이브러리가 들어 있지 않습니다. 이 항목에서는 웹 서버 구축 시 포함시켜야 하는 옵션과 보드를 사용하기 위해 Apache 2.x를 구성하는 방법을 설명합니다.

Apache 2.x Web Server 구축

이 절차를 시작하려면 OpenSSL 구현을 위해 필요한 모든 필수 패치를 설치해야 합니다. 이 항목에서는 보드에 해당되는 옵션에 대해서만 설명하며 전체 Apache 2.x를 구축하기 위한 지침을 세부적으로 다루지는 않습니다. 전체 지침은 http://www.apache.org에서 설명서를 참조하십시오.

▼ Apache 2.x 구축

1. **SH_LIBS 환경 변수를 configure 스크립트에 따라 미리 설정합니다.**

```
sh:
# SH_LIBS="-lssl -lcrypto"
# export SH_LIBS
csh/tcsh:
# setenv SH_LIBS "-lssl -lcrypto"
```

2. **설치 디렉토리로 변경하고 configure 스크립트를 실행합니다.**

   이 스크립트에는 많은 명령행 옵션이 있으며 다음은 웹 서버에서 보드를 사용하도록 구성하기 위해 필요한 옵션입니다.

```
# ./configure --enable-ssl --enable-mods-shared=ssl
--with-ssl=/opt/SUNWconn/cryptov2
```

3. **스크립트가 완료되면 다음 중 하나를 수행합니다.**

   a. **Apache 2.x를 처음으로 구축하고 설치하는 경우 다음을 입력합니다.**

```
# make
# make install
```

   b. **기존 Apache 2.x Web Server용 mod_ssl 공유 라이브러리를 구성하는 경우, 다음을 입력합니다.**

```
# make shared-build
# cp modules/ssl/.libs/mod_ssl.so Apache 디렉토리 /modules
```

Apache Web Server 2.x 구성

이 항목에서는 서버 인증서를 생성 및 설치하고 SSL을 위해 웹 서버를 구성함으로써 웹 서버에서 보드를 사용하도록 구성하는 방법에 대해 설명합니다.

▼ 서버 인증서 생성

1. 키 및 인증서 요청을 작성합니다.

```
# /opt/SUNWconn/cryptov2/bin/openssl req \
-new -newkey rsa: 키 크기 -keyout 키 출력 파일 \
-out 인증서 요청 출력 파일 \
-config /opt/SUNWconn/cryptov2/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....................................................................
..........++++++
.......++++++
writing new private key to '/tmp/key1.pem'
```

2. 키 파일을 보호하기 위해 사용할 암호를 입력합니다.

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

3. 고유 이름(DN) 값을 입력합니다(표 6-2 **참조).**

```
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) []: 회사 부서
SSL Server Name (eg, www.company.com) []:www.company.com
Email Address []: admin@domain.com
```

표 6-2 고유 이름 필드

필드	설명
Country Name (국가 이름):	두 개의 영문자로 이루어진 ISO 국가 코드(예: 미국의 경우 US)
State or Province Nam(주/도 이름):	(선택사항)주/도의 전체 이름(또는 마침표(.)를 입력할 수 있음)
Locality Name(지역 이름):	(선택사항)시/도/군/국가
Organization Name (소속 기관 이름)	회사 이름
Organizational Unit Name(소속 기관 단위 이름):	(선택사항)회사 부서
SSL Server Name (SSL 서버 이름):	방문자 브라우저에 입력되는 웹 사이트 도메인
Email Address (전자 우편 주소):	요청자의 연락 정보

▼ 서버 인증서 설치

- **헤더와 함께 인증서 요청을 178페이지의 "서버 인증서 생성"의 1단계에서 키 파일을 생성한 디렉토리와 동일한 디렉토리에 복사합니다.**

▼ SSL 활성화

1. **Apache 2.x Web Server 설치 디렉토리의** `conf` **하위 디렉토리에 있는** `ssl.conf` **파일을 편집합니다.**

   `ssl.conf` 파일에는 여러 지시어가 있으며 웹 서버에서 보드를 사용하게 하려면 반드시 다음 지시어를 구성해야 합니다.

```
Listen 포트 번호
ServerName 정식 도메인 이름
SSLEngine on
SSLCertificateFile 인증서 파일 경로
SSLCertificateKeyFile 키 파일 경로
```

2. **Apache Web Server를 시작합니다.**

   다음은 Apache 바이너리 디렉토리를 `/usr/apache/bin`으로 가정한 것입니다. 사용자의 바이너리 디렉토리가 아닌 경우 올바른 디렉토리를 입력합니다.

```
# /usr/apache/bin/apachectl sslstart
```

3. **프롬프트가 나타나면 PEM 패스 문구를 입력합니다.**

4. **다음 웹 사이트에서 새로운 SSL 작동 웹 서버를 확인합니다:**

   `https://`*서버 이름*`:`*서버 포트*`/`

   기본 *서버 포트*는 443입니다.

참고 – 테스트를 위한 인증서 자가 서명 방법에 대한 자세한 내용은 mod_SSL 및 OpenSSL 설명서를 참조하십시오.

재부팅 시 무인 시작되도록 Apache Web Server 구성

암호화된 키를 통해 Apache Web Server가 재부팅 될 때 사용자의 개입 없이 자동으로 시작되도록 구성할 수 있습니다.

▼ 재부팅 시 Apache Web Server의 자동 시작을 위한 암호화 키 생성

1. `httpd.conf` **파일에 다음 항목이 있는지 확인합니다.**

```
SSLPassPhraseDialog exec:/opt/SUNWconn/cryptov2/bin/apgetpass
```

   이 지시어는 `/etc/apache` 디렉토리의 암호로 보호된 파일에서 암호를 검색합니다.

2. **다음 파일 이름 규칙에 따라** `/etc/apache` **디렉토리에서 암호만 포함된 암호 파일을 생성합니다.**

```
서버 이름: 포트 .KEYTYPE.pass
```

   - *서버 이름* – `httpd.conf` 파일에서 "ServerName" 지시어에 입력한 값
   - *포트* – 해당 SSL 서버가 실행되는 포트(예: 443)
   - *KEYTYPE* – `RSA` 또는 `DSA`

예제: 이름이 webserv101이고 RSA 키를 가지고 있으며 443 포트에서 SSL을 실행하는 서버인 경우 /etc/apache에 다음 파일을 생성합니다.

```
webserv101:443.RSA.pass
```

암호 파일에 대한 권한 및 소유권을 다음과 같이 변경합니다.

```
# chmod 400 서버 이름: 포트. KEYTYPE.pass
# chown root 서버 이름: 포트. KEYTYPE.pass
```

자세한 내용은 mod_SSL 및 OpenSSL 설명서를 참조하십시오.

Sun Crypto Accelerator 4000 소프트웨어 설치 후 Apache와 함께 사용하기 위해 Sun Crypto Accelerator 1000 구성

SUNWkcl2a 소프트웨어 패키지가 설치되면 시스템은 Apache Web Server mod_ssl 1.3.26으로 구성됩니다.

Apache에서 Sun Crypto Accelerator 1000 보드를 구성하려면 다음 패치를 설치해야 합니다.

SUNWkcl2a 패키지가 설치된 Solaris 8 시스템에서 Apache 1.3.26과 함께 사용할 수 있도록 하기 위해 Sun Crypto Accelerator 1000을 구성하려면 다음 패치가 필요합니다.

- Apache 1.3.26 – 패치 ID 109234-09 이상
- Sun Crypto Accelerator 1000 버전 1.0 소프트웨어 – 패치 ID 112869-02
- Sun Crypto Accelerator 1000 버전 1.1 소프트웨어 – 패치 ID 113355-01

SUNWkcl2a 패키지가 설치된 Solaris 9 시스템에서 Apache 1.3.26과 함께 사용할 수 있돌록 하기 위해 Sun Crypto Accelerator 1000을 구성하려면 다음 패치가 필요합니다.

- Apache 1.3.26 – 패치 ID 113146-01 이상
- Sun Crypto Accelerator 1000 버전 1.1 소프트웨어 – 패치 ID 113355-01

7 장

진단 및 문제 해결

이 장에서는 Sun Crypto Accelerator 4000 소프트웨어에 대한 진단 테스트 및 문제 해결에 대해 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

SunVTS 진단 소프트웨어

핵심 SunVTS 래퍼는 테스트 제어 및 일련의 테스트에 대한 사용자 인터페이스를 제공합니다. 일부 테스트는 Solaris 8/9 Software Supplement CD안에 번들로 구성된 `SUNWvts` 및 `SUNWvtsx` 패키지로 제공됩니다. 번들에 포함되지 않고 SunVTS 핵심을 사용하는 기타 테스트는 테스트되는 드라이버 소프트웨어 패키지와 함께 제공됩니다.

Sun Crypto Accelerator 4000 보드는 세 종류의 SunVTS 테스트로 테스트할 수 있습니다. 이 테스트 중 `nettest` 및 `netlbtest` 두 가지는 SunVTS 5.1 Patch Set(PS) 2 릴리스부터 핵심 SunVTS 소프트웨어와 번들로 제공됩니다. 이 테스트는 보드의 이더넷 회로에서 실행됩니다.

세 번째 SunVTS 테스트인 `vcatest`는 Sun Crypto Accelerator 4000 CD의 `SUNWvcav` 패키지에 제공되어 핵심 SunVTS 래퍼와 함께 작동하여 보드의 암호화 회로를 진단합니다.

SunVTS netlbtest 및 nettest 설치vca 드라이버 지원

표 7-1은 설치된 SunVTS 소프트웨어를 업데이트하여 vca 드라이버에 대한 SunVTS netlbtest 및 nettest 지원을 제공하는 방법을 설명합니다.

표 7-1 vca 드라이버를 위한 SunVTS netlbtest 및 nettest 필수 소프트웨어

기본 Solaris 소프트웨어	기본 SunVTS 소프트웨어	필수 교체 패키지	필수 오버레이 패치
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 소프트웨어는 각 Solaris 릴리스와 함께 배포되는 Solaris Software Supplement CD에 담겨 전달됩니다. 표 7-1의 기본 SunVTS 소프트웨어 열에 나열된 SunVTS 소프트웨어 버전은 같은 행에 명시된 Solaris 릴리스와 함께 제공되는 Solaris Software Supplement CD를 통해 배포됩니다.

표 7-1에서 "SunVTS"로 시작되는 항목은 SunVTS 패키지 세트의 버전을 식별합니다. 각 SunVTS 패키지 세트에 포함된 SUNWvts 및 SUNWvtsx 패키지는 반드시 설치해야 합니다.

표 7-1의 필수 교체 패키지 열은 이전에 설치한 SunVTS 패키지 세트를 대체해야 하는 SunVTS 패키지 세트를 나열합니다. SunVTS 교체 패키지를 설치하기 전에 이전에 설치한 SunVTS 패키지를 제거해야 합니다. 이전에 설치한 SunVTS 패키지는 설치 시와 같은 방법으로 제거해야 합니다. 예를 들어, 패키지를 설치할 때 pkgadd 명령을 사용한 경우 이를 제거할 때는 pkgrm 명령을 사용해야 합니다.

표 7-1의 필수 오버레이 패치 열에 항목이 있는 경우 patchadd 명령을 사용하여 기본 SunVTS 소프트웨어 열에 표시된 SunVTS 패키지 위에 패치를 설치합니다. 필수 패치를 추가하기 전에 이전에 설치한 SunVTS 패키지를 제거하지 마십시오.

patchadd 명령으로 패치 113614-11를 설치하는 것은 이전에 설치한 SunVTS 패키지를 SunVTS5.1ps2 패키지로 대체하는 것과 같습니다.

교체 패키지를 다음 사이트에서 얻을 수 있습니다.
http://www.sun.com/oem/products/vts/

오버레이 패치는 다음 사이트에서 다운받을 수 있습니다.
http://sunsolve.sun.com/

참고 – SUNWvcav 패키지를 설치하기 전에 필수 SunVTS 패키지 및 기타 필수 패치를 설치해야 합니다. SUNWvcav 패키지에는 SunVTS 테스트 vcatest가 포함되어 있습니다.

SunVTS 소프트웨어를 통한 vcatest, nettest 및 netlbtest 실행

이러한 진단 테스트의 수행 및 감시 지침은 SunVTS 테스트 참조 설명서, 사용 설명서 및 빠른 참조 안내서를 참조하십시오. 해당 설명서를 http://docs.sun.com에서 Sun Hardware Documentation Set의 Solaris 항목에서 얻을 수 있습니다. 또한 시스템의 Solaris와 함께 배포되는 Solaris Software Supplement CD에도 제공됩니다.

참고 – 필수SunVTS 패키지와 기타 필수 SunVTS 패치를 설치한 경우에만 SunVTS를 사용할 수 있습니다.

▼ vcatest 실행

1. **수퍼유저로 로그인하고 SunVTS를 시작합니다.**

```
# /opt/SUNWvts/bin/sunvts
```

SunVTS 시작에 대한 자세한 지침은 SunVTS 설명서를 참조하십시오.

다음은 CDE 사용자 인터페이스를 통해 SunVTS를 시작한 가정 하의 지침입니다.

2. **[SunVTS Diagnostic(SunVTS 진단)] 기본 창에서 [System Map(시스템 맵)]을 [Logical(논리적)] 모드로 설정합니다.**

참고 – 물리적 모드 또한 지원되지만 여기서는 논리적 모드를 사용하는 경우에 대한 절차를 설명합니다.

---

3. **해당 확인 상자를 해제하여 모든 테스트를 비활성화합니다.**

4. **[Cryptography(암호화)]의 확인 상자를 선택하고 Cryptography의 플러스 상자를 선택하여 Cryptography 그룹의 모든 테스트를 표시합니다.**

5. **[Cryptography(암호화)] 그룹에서 `vcatest` 이름이 지정되지 않은 확인 상자를 해제합니다.**

   - `vcatest`가 표시된 경우 6단계로 이동합니다.
   - `vcatest`가 표시되지 않은 경우 [Commands(명령)] 드롭다운 메뉴에서 [Reprobe system(시스템 검색)]을 선택하고 시스템을 검색하여 vcatest를 찾습니다.

   정확한 절차는 SunVTS 사용 설명서를 참조하십시오. 검색이 완료되고 `vcatest`가 표시되면 6단계로 이동합니다.

6. **`vcatest`의 인스턴스 중 하나를 선택한 다음 마우스 오른쪽 단추로 드래그하여 [Test Parameter Options(테스트 매개 변수 옵션)] 대화 상자를 표시합니다.**

   이 옵션은 `vcatest`에만 해당되며, 187페이지의 "`vcatest`에 대한 테스트 매개 변수 옵션"에서 설명됩니다.

7. **선택이 모두 완료되면 [Within Instance(인스턴스 내에서)] 드롭다운 메뉴에서 [Apply(적용)]를 눌러 선택한 `vcatest`의 인스턴스를 변경하거나 [Across All Instances(인스턴스 전체)] 드롭다운 메뉴에서 [Apply(적용)]를 선택하여 선택한 모든 `vcatest`의 인스턴스를 변경합니다.**

   그러면 대화 상자가 제거되고 [Sun Diagnostic(Sun 진단)] 기본 창으로 돌아갑니다.

8. **`vcatest`의 인스턴스 중 하나를 선택한 다음 마우스 오른쪽 단추로 드래그하여 [Test Execution Options(테스트 실행 옵션)]을 표시합니다.**

   [Options(옵션)] 드롭다운 기본 메뉴를 선택한 다음 [Test Executions(테스트 실행)]를 선택하는 방법으로 [Test Execution Options(테스트 실행 옵션)] 대화 상자를 표시할 수도 있습니다. 이 옵션은 모든 테스트에 영향을 주는 일반적인 SunVTS 컨트롤입니다. 자세한 내용은 SunVTS 사용 설명서를 참조하십시오.

9. **선택이 모두 완료되면 [Apply(적용)]를 선택하여 대화 상자를 제거하고 [Sun Diagnostic(Sun 진단)] 기본 창으로 돌아갑니다.**

10. **[Start(시작)]를 눌러 선택한 테스트를 수행합니다.**

11. **[Stop(중지)]을 눌러 모든 테스트를 중지합니다.**

vcatest에 대한 테스트 매개 변수 옵션

표 7-2는 vcatest 하위 테스트를 설명합니다.

표 7-2 vcatest 하위 테스트

테스트 이름	설명
CDMF	[CDMF bulk encryption(CDMF 대량 암호화)]을 테스트합니다.
DES	[DES bulk encryption(DES 대량 암호화)]을 테스트합니다.
3DES	[3DES Bulk Encryption(3DES 대량 암호화)]을 테스트합니다.
RSA	[RSA Public and Private Keys(RSA 공개 및 개인 키)]를 테스트합니다.
DSA	[DSA Signature Verification(DSA 서명 확인)]을 테스트합니다.
MD5	[MD5 Message Digest/Digital Signature(메시지 요약/디지털 서명)]를 테스트합니다.
SHA1	[SHA1 Digest Key Creation(SHA1 요약 키 생성)]을 테스트합니다.
RNG	난수 생성을 테스트합니다.

vcatest 명령행 구문

CDE 인터페이스 대신 명령행에서vcatest를 실행하려면 명령행 문자열에 모든 인수를 지정합니다.

32비트 모드인 경우 vcatest 경로는 /opt/SUNWvts/bin/입니다. 64비트 모드인 경우 vcatest 경로는 /opt/SUNWvts/bin/sparcv9/입니다.

vcatest에 대한 명령행 인터페이스에서 모든 SunVTS 표준 옵션이 지원됩니다. 테스트와 관련된 옵션은 -o 인수로 지정됩니다.

표준 명령행 인수에 대한 정의는 SunVTS 테스트 참조 설명서를 참조하십시오. vcatest는 [Functional Mode(기능 모드)] 테스트이므로 -f가 포함되어야 합니다. 용도 메시지를 표시하려면 -u를, 자세한 메시지를 표시하려면 -v를 포함합니다. 대괄호 안에 있는 항목은 옵션 항목을 나타냅니다.

다음은 32비트 모드에서 vcatest를 독립형 프로그램으로 호출하는 예제입니다. 다음 명령은 vca0에서 모든 하위 테스트를 수행합니다.

```
# /opt/SUNWvts/bin/vcatest -f -o dev=vca0,tl=all
```

다음은 SunVTS 인프라에서 64비트 모드로 vcatest를 호출하는 예제입니다. 다음 명령은 vca2에서 RSA, DSA 및 MD5를 테스트합니다.

```
# /opt/SUNWvts/bin/sparcv9/vcatest -f -o dev=vca2,tl=RSA+DSA+MD5
```

명령행에서 vcatest를 실행할 때 옵션을 생략하게 되면 표 7-3에 설명된 대로 해당 옵션의 기본 작동이 수행됩니다.

표 7-3 vcatest 명령행 구문

옵션	설명
dev=vca*N*	vca0 또는 vca2와 같이 테스트할 장치의 인스턴스를 지정합니다. 지정되지 않은 경우 기본값인 vca0로 지정됩니다. *N*은 테스트할 장치의 인스턴스 번호 배치를 나타냅니다.
tl=*testlist*	실행할 하위 테스트 목록을 지정합니다. tl의 하위 테스트는 +(플러스) 문자로 구분됩니다. 지원되는 하위 테스트는 CDMF, DES, 3DES, DSA, RSA, MD5, SHA1 및 RNG이기 때문에 tl=CDMF+DES+3DES+DSA+RSA+MD5+SHA1+RNG 명령은 모든 하위 테스트를 활성화합니다. 또는 모든 테스트를 실행하는 tl=all을 입력해도 됩니다. 하위 테스트가 지정되지 않은 경우 기본값인 all이 지정됩니다.

▼ netlbtest 실행

1. 수퍼유저로 로그인하고 SunVTS를 시작합니다.

```
# /opt/SUNWvts/bin/sunvts
```

자세한 시작 지침은 SunVTS 사용 설명서를 참조하십시오.

다음은 CDE 사용자 인터페이스를 통해 SunVTS를 시작한 가정 하의 지침입니다.

2. **[SunVTS Diagnostic(SunVTS 진단)] 기본 창에서 [System Map(시스템 맵)]을 [Logical(논리적)] 모드로 설정합니다.**

참고 – 물리적 모드 또한 지원되지만 여기서는 논리적 모드를 사용하는 경우에 대한 절차를 설명합니다.

---

3. **해당 확인 상자를 해제하여 모든 테스트를 비활성화합니다.**
4. **[Network(네트워크)]의 확인 상자를 선택하고 Network의 플러스 상자를 선택하여 Network 그룹의 모든 테스트를 표시합니다.**
5. **[Network(네트워크)] 그룹에서** `vca`*N*`(netlbtest)` **이름이 지정되지 않은 확인 상자를 해제합니다.**

   *N*은 테스트 중인 장치의 인스턴스 번호를 나타냅니다.

   - `vca`*N*`(netlbtest)`이 표시된 경우 6단계로 이동합니다.
   - `vca`*N*`(netlbtest)`가 표시되지 않은 경우, [Commands(명령)] 드롭다운 메뉴에서 [Reprobe system(시스템 검색)]을 선택하고 시스템을 검사하여 vcatest를 찾습니다.

   정확한 절차는 SunVTS 사용 설명서를 참조하십시오. 검색이 완료되고 `vca`*N*`(netlbtest)`가 표시되면 6단계로 이동합니다.

6. **[Intervention Mode(중재 모드)] 단추를 선택합니다.** `vca`*N*`(netlbtest)` **인스턴스 중 하나를 선택한 다음 마우스 오른쪽 단추로 드래그하여 [Test Parameter Options(테스트 매개 변수 옵션)] 대화 상자를 표시합니다.**

   이 옵션은 `netlbtest`에만 해당되며, SunVTS 테스트 참조 설명서에서 설명됩니다.

7. **선택이 모두 완료되면 [Within Instance(인스턴스 내에서)] 드롭다운 메뉴에서 [Apply(적용)]를 눌러 선택한** `vca`*N*`(netlbtest)`**의 인스턴스를 변경하거나 [Across All Instances(인스턴스 전체)] 드롭다운 메뉴에서 [Apply(적용)]를 선택하여 선택한 모든** `vca`*N*`(netlbtest)`**의 인스턴스를 변경합니다.**

   그러면 대화 상자가 제거되고 [Sun Diagnostic(Sun 진단)] 기본 창으로 돌아갑니다.

8. `vca`*N*`(netlbtest)` **인스턴스 중 하나를 선택한 다음 마우스 오른쪽 단추로 드래그하여 [Test Execution Options(테스트 실행 옵션)] 대화 상자를 표시합니다.**

   [Options(옵션)] 드롭다운 기본 메뉴를 선택한 다음 [Test Executions(테스트 실행)]를 선택하는 방법으로 [Test Execution Options(테스트 실행 옵션)] 대화 상자를 표시할 수도 있습니다. 이 옵션은 모든 테스트에 영향을 주는 일반적인 SunVTS 컨트롤입니다. 자세한 내용은 SunVTS 사용 설명서를 참조하십시오.

9. **선택이 모두 완료되면 [Apply(적용)]를 선택하여 대화 상자를 제거하고 [Sun Diagnostic(Sun 진단)] 기본 창으로 돌아갑니다.**
10. **[Start(시작)]를 눌러 선택한 테스트를 수행합니다.**
11. **[Stop(중지)]을 눌러 모든 테스트를 중지합니다.**

▼ nettest 수행

1. **수퍼유저로 로그인하고 SunVTS를 시작합니다.**

```
# /opt/SUNWvts/bin/sunvts
```

자세한 시작 지침은 SunVTS 사용 설명서를 참조하십시오.

참고 – 다음은 CDE 사용자 인터페이스를 통해 SunVTS를 시작한 가정 하의 지침입니다.

---

2. **[SunVTS Diagnostic(SunVTS 진단)] 기본 창에서 [System Map(시스템 맵)]을 [Logical(논리적)] 모드로 설정합니다.**

참고 – 물리적 모드 또한 지원되지만 여기서는 논리적 모드를 사용하는 경우에 대한 절차를 설명합니다.

---

3. **해당 확인 상자를 해제하여 모든 테스트를 비활성화합니다.**
4. **[Network(네트워크)]의 확인 상자를 선택하고 Network의 플러스 상자를 선택하여 Network 그룹의 모든 테스트를 표시합니다.**
5. **[Network(네트워크)] 그룹에서 vca*N*(nettest) 이름이 지정되지 않은 확인 상자를 해제합니다.**

   *N*은 테스트 중인 장치의 인스턴스 번호 배치를 나타냅니다.

   - vca*N*(nettest)이 표시된 경우 6단계로 이동합니다.
   - vca*N*(nettest)이 표시되지 않은 경우 vca*N* 보드를 가진 다른 서버에서 창을 열고 ifconfig -a를 입력합니다. 다음과 같은 항목이 나열되어 있어야 합니다.

```
vcaN up inet ip-주소 plumb
```

앞의 ifconfig 항목이 나열되어 있지 않은 경우 nettest 검색은 장치를 테스트 부적합으로 간주합니다. 인터페이스를 온라인 상태로 전환하려면 ifconfig 온라인 매뉴얼 페이지의 지침을 따라야 합니다.

ifconfig -a가 위 항목을 생성하면 [SunVTS Diagnostic(SunVTS 진단)] 기본 창으로 돌아간 후 [Commands(명령)] 드롭다운 메뉴에서 [Reprobe system(시스템 검색)]을 선택하여 vca를 찾습니다.

정확한 절차는 SunVTS 사용 설명서를 참조하십시오. 검색이 완료되고 vca0(nettest)가 표시되면 6단계로 이동합니다.

6. **vca*N*(nettest) 인스턴스 중 하나를 선택한 다음 마우스 오른쪽 단추로 드래그하여 [Test Parameter Options(테스트 매개 변수 옵션)] 대화 상자를 표시합니다.**

   이 옵션은 nettest에만 해당되며, SunVTS 테스트 참조 설명서에서 설명됩니다.

7. **선택이 모두 완료되면 [Within Instance(인스턴스 내에서)] 드롭다운 메뉴에서 [Apply(적용)]를 눌러 선택한 vca*N*(nettest)의 인스턴스를 변경하거나 [Across All Instances(인스턴스 전체)] 드롭다운 메뉴에서 [Apply(적용)]를 선택하여 선택한 모든 vca*N*(nettest)의 인스턴스를 변경합니다.**

   그러면 대화 상자가 제거되고 [Sun Diagnostic(Sun 진단)] 기본 창으로 돌아갑니다.

8. **vca*N*(nettest) 인스턴스 중 하나를 선택한 다음 마우스 오른쪽 단추로 드래그하여 [Test Execution Options(테스트 실행 옵션)] 대화 상자를 표시합니다.**

   [Options(옵션)] 드롭다운 기본 메뉴를 선택한 다음 [Test Executions(테스트 실행)]를 선택하는 방법으로 [Test Execution Options(테스트 실행 옵션)] 대화 상자를 표시할 수도 있습니다. 이 옵션은 모든 테스트에 영향을 주는 일반적인 SunVTS 컨트롤입니다. 자세한 내용은 SunVTS 사용 설명서를 참조하십시오.

9. **선택이 모두 완료되면 [Apply(적용)]를 선택하여 대화 상자를 제거한 후 [Sun Diagnostic(Sun 진단)] 기본 창으로 돌아갑니다.**

10. **[Start(시작)]를 눌러 선택한 테스트를 수행합니다.**

11. **[Stop(중지)]을 눌러 모든 테스트를 중지합니다.**

참고 – nettest와 netlbtest를 동시에 수행하도록 선택하지 마십시오.

---

kstat를 통한 암호화 작업 결정

Sun Crypto Accelerator 4000 보드에는 보드에서 수행되는 암호화 작업을 나타내는 신호나 기타 표시등이 없습니다. 암호화 작업 요청이 보드에서 실제로 수행되고 있는지를 확인하려면 kstat(1M) 명령을 사용하여 장치 사용 내역을 표시합니다.

```
# 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
```

참고 – 위 예제에서 0은 vca 장치의 인스턴스 번호입니다. 이 번호는 kstat 명령을 수행하는 보드의 인스턴스 번호를 반영해야 합니다.

kstat 정보 표시는 암호화 요청 또는 "작업"이 Sun Crypto Accelerator 4000 보드로 전송되고 있는지의 여부를 나타냅니다. 시간 경과에 따라 "*작업*" 값이 변하면, 보드가 Sun Crypto Accelerator 4000 보드에 전송된 암호화 작업 요청을 가속화하고 있는 것입니다. 암호화 작업 요청이 보드로 전송되지 않을 경우, 웹 서버의 각 특정 구성별로 웹 서버 구성을 확인하십시오.

kstat(1M)가 반환하는 커널/드라이버 통계 값을 해석하려고 시도하지 마십시오. 이 값은 드라이버 내에 유지되어 필드 지원을 도와 줍니다. 의미와 실제 이름은 시간에 따라 변경됩니다.

참고 – nostats 속성이 /kernel/drv/vca.conf 파일에 정의된 경우 통계의 캡처와 표시는 비활성화됩니다. 이 속성은 트래픽 분석을 방지하는 데 사용될 수 있습니다.

OpenBoot PROM FCode 자가 테스트 사용

시스템이 부팅되지 않은 경우 다음 테스트를 통해 어댑터의 문제를 식별할 수 있습니다.

OpenBoot PROM `ok` 프롬프트에서 `test` 또는 `test-all` 명령을 사용하여 FCode 자가 테스트 진단을 호출할 수 있습니다. 진단 수행 중 오류가 발생한 경우 이에 대한 적절한 메시지가 나타납니다. `test` 및 `test-all` 명령에 대한 자세한 내용은 *OpenBoot Command Reference Manual*을 참조하십시오.

FCode 자가 테스트는 대부분의 기능을 하위 항목별로 실행하여 다음을 확인합니다.

- 어댑터 보드 설치 중 연결성
- 시스템 부팅에 필요한 모든 구성 요소의 기능 여부 확인

▼ 이더넷 FCode 자가 테스트 진단 수행

이더넷 진단을 수행하려면 우선 재설정을 실행한 후 OpenBoot PROM `ok` 프롬프트에서 시스템을 멈추어야 합니다. 시스템을 재설정하지 않은 경우 진단 테스트로 인해 시스템이 중지될 수도 있습니다.

이 항목에서 설명하는 OpenBoot 명령에 대한 자세한 내용은 *OpenBoot Command Reference Manual*을 참조하십시오.

1. **시스템을 종료합니다.**

   *Sun 주변 장치에 대한 Solaris 안내서*에 설명된 표준 종료 절차를 따릅니다.

2. **OpenBoot PROM** `ok` **프롬프트에서** `auto-boot?` **구성 변수를** `false`**로 설정합니다.**

```
ok setenv auto-boot? false
```

3. **시스템을 재설정합니다.**

```
ok reset-all
```

4. **show-nets를 입력하여 장치 목록을 표시하고 선택을 입력합니다.**

   어댑터 고유의 장치 목록이 아래 예제와 유사한 형식으로 표시됩니다.

```
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
```

참고 – test 명령으로 다음의 자가 테스트를 수행하려면 이더넷 포트가 네트워크에 연결되어 있어야 합니다.

5. **test 명령으로 자가 테스트를 수행합니다.**

   test 명령이 실행되면 다음 테스트가 수행됩니다.

   - vca 레지스터 테스트(diag-switch?가 true인 경우에만 수행됨)
   - 내부 루프백 테스트
   - 링크 활성화/비활성화 테스트

참고 – 외부 루프백 케이블을 사용하는 1,000Mbps 연결에 대한 Sun Crypto Accelerator 4000 UTP 어댑터 자가 테스트는 지원되지 않으며, 이것은 링크 클럭을 재조정할 수 없기 때문입니다. 이 테스트를 수행하려면 로컬 및 원격 포트를 클럭 마스터와 클럭 슬레이브로 재조정해야 합니다. 외부 루프백 케이블이 사용된 경우 로컬 및 원격 포트 모두가 동일합니다. 따라서, 단일 포트가 클럭 마스터와 클럭 슬레이브 모두가 될 수 없어 PHY 연결이 항상 실패하게 됩니다. 1,000Mbps 연결에 대한 Sun Crypto Accelerator 4000 UTP 어댑터 자가 테스트를 수행하려면 원격 1000BASE-T 포트를 연결해야 합니다.

다음을 입력합니다.

```
ok test 장치-경로
```

test를 통과하면 다음 메시지가 표시됩니다.

```
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
```

보드가 네트워크에 연결되어 있지 않은 경우, 다음 메시지가 표시됩니다.

```
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. **어댑터 테스트 후, 다음을 입력하여 OpenBoot PROM** ok **프롬프트 인터페이스를 표준 운영 모드로 되돌립니다.**

```
ok setenv diag-switch? false
```

7. auto-boot? **구성 매개 변수를** true**로 설정합니다.**

```
ok setenv auto-boot? true
```

8. **시스템을 재설정하고 재부팅합니다.**

Sun Crypto Accelerator 4000 보드 문제 해결

이 항목에서는 보드의 문제를 해결하기 위해 OpenBoot PROM 수준에서 실행할 수 있는 명령을 설명합니다. 다음 하위 항목에서 설명하는 명령에 대한 자세한 내용은 *OpenBoot Command Reference Manual*을 참조하십시오.

show-devs

Sun Crypto Accelerator 4000 장치가 시스템에 나열되어 있는지 확인하려면 OpenBoot PROM ok 프롬프트에서 show-devs를 입력하여 장치 목록을 표시하십시오. 장치 목록에는 보드와 관련된 행이 아래 예제와 유사하게 표시됩니다.

```
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
.
.
```

위 예제에서 /pci@8,600000/network@1 항목은 보드에 대한 장치 경로를 나타냅니다. 시스템의 각 보드마다 이런 행이 하나씩 있습니다.

.properties

Sun Crypto Accelerator 4000 장치 속성이 정확하게 나열되는지 확인하려면 ok 프롬프트에서 .properties를 입력하여 속성 목록을 표시합니다.

```
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 04-03-03
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

네트워크 연결을 감시하려면 ok 프롬프트에서 apply watch-net 명령과 장치 경로를 함께 입력합니다.

```
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.....
```

시스템은 오류 없는 패킷을 전송받으면 "."를, 네트워크 하드웨어 인터페이스가 감지할 수 있는 오류를 가진 패킷을 받을 때는 "X"를 표시하여 네트워크 트래픽을 감시합니다.

8 장

PKCS#11 인터페이스

이 장에서는 Sun Crypto Accelerator 4000 소프트웨어가 기본 위치에 설치된 가정 하에서 보드의 PKCS#11 인터페이스를 구현하는 것에 대해 설명합니다. 이 장은 또한 PKCS#11 인터페이스에 익숙한 사용자를 대상으로 작성되었습니다. PKCS#11 표준 관련 정보와 헤더 파일 `pkcs11.h`, `pkcs11f.h` 및 `pkcs11t.h`의 원본은 다음 웹 사이트에 있습니다. `http://www.rsasecurity.com/rsalabs/PKCS`

이 장은 다음 항목으로 구성되어 있습니다.

일반 정보

Sun Crypto Accelerator 4000 보드 및 관련 소프트웨어는 PKCS#11 인터페이스를 제공합니다. Sun Crypto Accelerator 4000 소프트웨어에는 대부분의 응용 프로그램에 필요한 PKCS#11 기능이 모두 들어 있습니다.

PKCS#11은 단일 사용자 시스템용으로 설계되었습니다. Solaris 운영 체제는 다중 사용자 시스템이므로 상호 간에 신뢰성이 없는 여러 명의 사용자를 동시에 처리해야 합니다. 이를 위해 이 보드에는 PKCS#11을 확장하지 않고도 여러 사용자를 식별 및 인증할 수 있는 메커니즘이 추가되었습니다. 비밀 PIN을 허용하는 모든 PKCS#11 기능에는 *사용자 이름:암호* 형식의 문자열을 제공해야 합니다(표 5-1 참조). 이러한 PIN 구조는 일반적으로 응용 프로그램을 통해 전달되지만 일부 보드 전용 응용 프로그램에서는 사용자 이름과 비밀 부분을 개별적으로 요청할 수도 있습니다.

PKCS#11에는 토큰을 초기화하는 `C_InitToken`과 사용자 PIN을 설정하는 `C_InitPin`의 두 가지로 관리 기능이 제한되어 있습니다. 보드에서는 이 기능 대신 `vcaadm` 유틸리티를 사용합니다.

vcaadm 보안 관리자(SO)는 UNIX 수퍼유저와 관련되어 있지 않습니다. 또한 보안 관리자가 vcaadm 유틸리티를 사용하여 생성하는 보드 사용자의 userid도 UNIX 사용자 이름 또는 ID와 관련이 없습니다.

PKCS#11에는 슬롯과 토큰이라는 별개의 개념이 사용됩니다. 토큰은 스마트 카드와 유사하며 *슬롯*에 연결됩니다. Sun Crypto Accelerator 4000 시스템에서는 슬롯과 토큰을 구분하지 않습니다. 이 설명서에서는 일반적으로 *토큰*이라는 용어를 사용하지만 응용 프로그램 및 기타 설명서에서는 *슬롯*을 사용할 수도 있습니다.

보드별로 *키스토어*를 하나 이상씩 지원합니다. 보안 관리자는 vcaadm을 사용해 키스토어별로 이름을 부여합니다. 보드는 각각의 키스토어를 PKCS#11 토큰으로 표시하며 토큰 레이블은 공백 없이 최대 32문자로 관련 키스토어의 이름을 나타냅니다. 고가용성을 위해 여러 보드에서 하나의 키스토어를 지원할 수도 있습니다.

또한 SUNW acceleration only라는 레이블의 특수한 토큰도 하나 존재합니다. 이 토큰은 영구 키를 저장할 수 없으므로 응용 프로그램은 이 토큰에 로그인할 수 없습니다. 이 토큰에 전송된 요청은 사용 가능한 모든 보드에 분산됩니다.

토큰 목록은 대부분의 응용 프로그램에 표시되며 일반적으로 PKCS#11 토큰 레이블로 식별합니다(토큰 레이블은 공백 없이 입력된 관련 키스토어 이름이며 보안 관리자가 지정합니다).

PKCS#11을 사용하기 위한 보드 관리

Sun Crypto Accelerator 4000 시스템은 vcaadm 유틸리티를 사용하여 관리합니다(4장 참조). SO는 키스토어의 이름을 지정하고 사용자 계정을 생성하며 계정별로 초기 암호를 제공합니다. SO는 또한 FIPS 모드에서의 보드 운용 여부를 제어합니다(202페이지의 "PKCS#11와 FIPS 모드" 참조).

보드는 여러 가지 PKCS#11 메커니즘을 지원합니다. 이러한 메커니즘들은 대부분 무제한으로 사용할 수 있습니다. 하지만 관리자는 다음 메커니즘의 표시를 일부 제어할 수 있습니다.

- 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

위의 메커니즘은 항상 가속화 전용 토큰을 통해 표시되며, /etc/opt/SUNWconn/cryptov2/sslreg가 표시된 경우에만 키스토어와 함께 토큰으로 표시됩니다. 이 파일을 생성하려면 수퍼유저 권한으로 다음 명령을 입력합니다.

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

변경 사항을 적용하려면 응용 프로그램을 다시 시작해야 합니다.

네트워크 보안 서비스(NSS)는 이러한 메커니즘의 사용 가능 시기를 인식합니다. 메커니즘이 제공되면 NSS는 소용량의 버퍼를 사용해 C_DigestUpdate를 여러 번 호출하는데, 이는 성능을 저하시키는 원인이 됩니다. 이러한 이유 때문에 위의 메커니즘은 기본값으로 제공되지 않습니다.

암호화 서비스 사용 응용 프로그램 설치 및 관리

PKCS#11 라이브러리의 기본 위치는 /opt/SUNWconn/cryptov2/lib/libvpkcs11.so입니다.

대부분의 응용 프로그램에는 PKCS#11 라이브러리의 위치가 포함된 구성 파일이나 데이터베이스가 있으며 때때로 GUI를 통해 액세스합니다. 편집기나 GUI를 사용하여 기본 위치에 위의 값을 입력합니다.

키에 CKA_SENSITIVE 속성이 있으면 해당 키와 관련된 작업은 하드웨어로 국한됩니다. 하지만 하드웨어서 모든 작업과 모든 유형의 키를 지원하지는 않습니다. 응용 프로그램이 하드웨어서 수행할 수 없는 작업을 요청하고 키의 CKA_SENSITIVE 속성이 true이면 작업은 실패하게 됩니다. 202페이지의 "하드웨어 가속화 및 Sensitive 키"에는 사용 가능한 조합 키, 작업 및 메커니즘에 관한 정확한 규칙이 자세히 설명되어 있습니다. 이런 규칙으로 인해 응용 프로그램이 실행되지 않으면 키를 sensative로 표시하지 않도록 응용 프로그램을 구성할 수 있습니다.

SSL... 및 TLS... 메커니즘의 표시 여부는 관리자가 제어합니다. 응용 프로그램에 이런 메커니즘이 필요하거나 이러한 메커니즘을 사용하는 성능 효과를 실험해야 하는 경우 200페이지의 "PKCS#11을 사용하기 위한 보드 관리"를 참조하십시오.

보드가 FIPS 모드이면 FIPS 승인 메커니즘만 제공됩니다(202페이지의 "PKCS#11와 FIPS 모드" 참조).

PKCS#11와 FIPS 모드

SO에 의해 FIPS 모드로 들어가면(vcaadm을 사용해) Sun Crypto Accelerator 4000 보드는 FIPS(Federal Information Processing Standard) 140-2 레벨 3을 준수합니다. FIPS 140-2에 대한 자세한 내용은 http://www.nist.gov를 참조하십시오.

FIPS 모드에서 보드를 운용하면 보드 작업이 다음과 같이 변경됩니다.

- 보드에서는 FIPS 승인 메커니즘만 사용할 수 있습니다.
- 모든 키와 필수 보안 매개 변수가 암호화된 형식으로 PCI 버스를 교차합니다.
- 시작 시와 키 및 난수 생성 시 특정 무결성 검사가 추가로 수행됩니다.
- 해시 및 산술 연산을 사용해 열 잡음 기반 생성기에서 저장된 상태 및 임의의 true 데이터(엔트로피)를 결합하는 FIPS 승인 알고리즘에 의해 난수가 생성됩니다.출력 데이터 160비트마다 열 잡음 기반 생성기에서 512비트가 사용됩니다(비FIPS 모드에서는 160비트에 대해 열 잡음 기반 생성기의 512비트가 SHA-1으로 해시됩니다).

FIPS 모드는 Sun Crypto Accelerator 4000 보드에만 적용됩니다. 앞서 언급한 것처럼 보드가 FIPS 모드이면 FIPS 승인 메커니즘만 제공됩니다. 특히 MD5, RC2 및 RC4는 FIPS 승인 메커니즘이 아닙니다. 하지만 FIPS 규칙은 하드웨어에만 적용되므로 소프트웨어는 정상적으로 제공하는 모든 메커니즘을 계속 사용할 수 있습니다.

FIPS 모드 동작 시 발생하는 주된 차이점은 비FIPS 승인 작업이 소프트웨어에서만 수행된다는 것이며, 이는 다음과 같은 두 가지 결과로 이어집니다.

- 비FIPS 승인 메커니즘을 사용한 암호화 작업은 가속화되지 않습니다.
- 비FIPS 승인 메커니즘을 사용한 암호화 작업이 CKA_SENSITIVE 속성이 ture로 설정된 키와 연관되어 있는 경우 true로 설정된 CKA_SENSITIVE 속성 키는 하드웨어에서만 사용할 수 있으므로 작업은 실패하게 됩니다.

하드웨어 가속화 및 Sensitive 키

보드는 하드웨어의 성능, 보안 요구 사항 및 성능을 기반으로 실행 위치를 선택합니다.

PKCS#11은 많은 키 유형과 메커니즘을 지정하지만 이들이 모두 하드웨어에서 완전히 지원되는 것은 아닙니다. 응용 프로그램이 하드웨어에서 완전히 지원되지 않는 작업, 키 및 메커니즘의 조합을 요청하면 일부는 하드웨어에서 그리고 일부는 소프트웨어에서 실행되거나 소프트웨어에서만 실행될 수 있습니다.

키의 CKA_SENSITIVE 속성이 true이면 이 키를 사용하는 작업은 안전하게 실행되어야 하며 하드웨어에 키 요소를 남기지 않아야 합니다. 하드웨어에서 안전하게 작업을 수행할 수 없으면 작업은 실패하게 됩니다. 또한 키의 CKA_SENSITIVE 속성이 false면 보드는 성능을 토대로 하드웨어와 소프트웨어 사이에서 선택합니다. 이 항목은 하드웨어, 소프트웨어 및 작업 실패를 선택하기 위해 사용하는 규칙에 대해 설명합니다.

편의상 키 및 메커니즘 집합을 다음과 같이 정의합니다.

- hardware_key_set =
  - 키 크기가 2048비트를 넘지 않는 RSA
  - 키 크기가 1024비트를 넘지 않는 DSA
  - DES
  - 3DES
  - CDMF
- hardware_mechanism_set =
  - CKM_CDMF_...(CKM_CDMF_ECB 제외)
  - CKM_DES_...(CKM_DES_ECB 제외)
  - CKM_DES3_...(CKM_DES3_ECB 제외)
  - CKM_DSA
  - CKM_MD5(FIPS 모드인 경우 제외)
  - 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(FIPS 모드인 경우 제외)

하드웨어에서 작업을 안전하게 실행하려면 키는 hardware_key_set에, 그리고 메커니즘은 hardware_mechanism_set에 있어야 합니다. 키는 hardware_key_set에 있지만 메커니즘이 hardware_mechanism_set에 있지 않은 경우 하드웨어는 작업을 가속화하지만 소프트웨어에서는 지원되지 않을 수 있습니다.

C_DeriveKey는 하드웨어에서 가속화할 수 있지만 소프트웨어 지원이 필요하므로 하드웨어 레벨 보안이 아닙니다.

다음 표는 키 관련 작업을 수행하는 경우 및 위치를 설명합니다.

표 8-1 키 관련 암호화 작업 처리

설정	CKA_SENSITIVE=**False**	CKA_SENSITIVE=**True**
하드웨어 레벨 보안	RSA, DSA 및 대용량 버퍼의 경우 하드웨어(그 외는 소프트웨어)	하드웨어
소프트웨어 지원을 통해 가능한 하드웨어 가속화	RSA, DSA 및 대용량 버퍼의 경우 하드웨어 및 소프트웨어(그 외는 소프트웨어)	실패
소프트웨어만	소프트웨어	실패

C_WrapKey 및 C_UnwrapKey는 두 키의 두 가지 작업과 관련되어 있습니다. C_Wrap 키의 경우 래핑된 키를 인코딩하는 인코딩 작업 다음, 래핑 키를 사용해 인코딩된 값을 암호화하는 암호화 작업이 이뤄집니다. C_UnwrapKey는 역순으로 수행되지만 암호 해독 및 디코딩이 이뤄집니다.

래핑된 키가 RSA 또는 DSA 키이고 래핑 메커니즘이 hardware_wrap_mechanism_set이면 인코딩 및 암호화 단계는 모두 하드웨어에서 수행됩니다. 두 키의 작업에는 모두 하드웨어 레벨 보안이 적용됩니다.

위의 조건이 하나라도 충족되지 않으면 인코딩 단계는 소프트웨어에서 수행됩니다. 래핑된 키의 작업에는 하드웨어 레벨 보안이 적용되지 않습니다. 암호화 단계는 래핑된 키와 메커니즘을 사용하는 C_Encrypt 작업과 동일한 것으로 간주됩니다. 표 8-1을 참조하십시오.

다음 표에는 다양한 설정이 요약되어 있습니다.

표 8-2 C_WrapKey 및 C_UnwrapKey의 실패 조건

조건	래핑된 키가 sensative인 경우 실패	래핑 키가 sensative인 경우 실패
래핑된 키가 RSA 또는 DSA이고 메커니즘이 hardware_wrap_mechanism_set에 있는 경우	–	–
래핑 키가 hardware_key_set에 있고 메커니즘이 hardware_mechanism_set에 있는 경우	실패	–
기타 설정	실패	실패

C_Digest는 호스트 메모리에 전체 버퍼를 수집합니다. C_DigestFinal은 버퍼가 대용량이지만 65532바이트를 넘지 않는 경우 전체 버퍼를 하드웨어로 보냅니다. 그렇지 않을 경우 전체 버퍼는 소프트웨어에서 처리됩니다.

C_DigestKey는 호스트 메모리로 키 요소를 옮긴 다음 일반 데이터처럼 취급하는데, 이후 C_DigestUpdate로 처리됩니다. 키의 CKA_SENSITIVE 속성이 true이면 작업에 실패하게 됩니다.

PKCS#11 사용을 위한 응용 프로그램 개발

필요한 헤더 파일은 /opt/SUNWconn/cryptov2/include에 있으며 이 디렉토리를 include 경로 및 include cryptoki.h에 추가합니다. Sun Crypto Accelerator 4000 소프트웨어에는 pkcs11.h, pkcs11f.h 및 pkcs11t.h 같은 하위 레벨 include 파일이 들어있습니다. 이 파일들은 PKCS#11 웹 사이트 (http://www.rsasecurity.com/rsalabs/PKCS)에 있는 파일과 동일합니다. pkcs11_preamble.h 파일은 include 디렉토리에 있으며 반드시 하위 레벨 파일보다 먼저 포함시켜야 합니다.

pkcs11 라이브러리의 위치는 /opt/SUNWconn/cryptov2/lib/libvpkcs11.so입니다.

Sun Crypto Accelerator 4000 라이브러리는 일반 라이브러리로 연결하거나 dlopen을 사용해 동적으로 열 수 있습니다(3DL).

일반 라이브러리로 연결하려면 다음 명령을 사용합니다.

```
cc [ 플래그 ] 파일 ... -L /opt/SUNWconn/cryptov2/lib \
-R /opt/SUNWconn/cryptov2/lib -l vpkcs11 [ 라이브러리 ...]
```

코드는 다음 예제에서처럼 기능을 직접 호출합니다.

```
rv = C_Initialize(NULL);
```

이 때, 동적 연결은 다음을 사용합니다(오류 처리는 생략되어 있음).

```
cc [ 플래그 ] files... -ldl [ 라이브러리… ]

#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) ...
```

코드는 다음과 같이 기능을 간접적으로 호출합니다.

```
rv = pk11funclist -> C_Initialize(NULL);
```

Sun Crypto Accelerator 4000 소프트웨어는 임의의 제한이 극히 적습니다. 대부분의 리소스는 호스트 메모리에서만 제한됩니다. 가속화 전용 토큰을 포함한 최대 토큰의 수는 1024입니다.

커널 메모리를 과도하게 소모하는 결함이 있거나 악의적인 프로그램에 의한 서비스 거부 공격을 막기 위해 소프트웨어는 Solaris 사용자 당(프로세스가 아닌) 16Mbyte 이상 소모할 수 없도록 커널 메모리의 양을 제한하고 있습니다. 이 제한은 구성할 수 없습니다.

다음 권장 사항에 유의하면 커널 메모리 소모 문제를 피할 수 있습니다.

- 다중 단계 작업을 중단하지 않습니다. 작업을 모두 완료한 다음 적절한 종료 기능(예: `C_EncryptFinal`)을 호출하거나 세션을 종료합니다.
- 필요 없는 객체를 버리지 않습니다. 작업을 모두 완료한 다음 생성 세션을 닫거나(휘발성 객체만 해당) `C_DestroyObject`를 호출합니다.
- 한 번에 너무 큰(몇 메가바이트) 데이터 청크를 전송하지 않습니다(대용량 요약 작업은 항상 소프트웨어에서 수행되므로 요약 작업에는 해당되지 않습니다).

PKCS#11 관리 기능 C_InitToken 및 C_InitPin은 구현되지 않습니다. 또한 CKU_SO(보안 관리자) 플래그의 C_Login 기능은 거부됩니다.

PKCS#11에서 *공개 토큰* 객체는 인증 과정 없이 보고 감지할 수 있는 불변 객체입니다. Sun Crypto Accelerator 4000에서 인식하는 사용자는 Solaris 사용자와 관련되어 있지 않고 소프트웨어는 C_Login이 성공할 때까지 사용자 ID를 확인하지 않으므로 이러한 객체는 모든 사용자들이 전체적으로 보고 감지할 수 있어야 합니다. 이런 동작은 허용되지 않으므로 공개 토큰 객체는 사용할 수 없습니다. 또한 공개 토큰 객체를 생성하려는 시도는 실패하게 됩니다.

휘발성(세션) 객체의 수는 가상 메모리에 의해서만 제한됩니다. 불변 객체는 모두 보드의 RAM에 맞아야 하지만 이로 인해 실제 사용에 제한을 받지는 않습니다. 이러한 개념에 따라 최대 메모리 크기를 나타내는 CK_TOKEN_INFO 구조의 필드(C_GetTokenInfo 기능으로 반환되는)는 모두 CK_EFFECTIVELY_INFINITE으로 설정됩니다. C_GetObjectSize 기능은 구현되지 않습니다.

옵션인 *이중 작업* 기능(C_DigestEncryptUpdate, C_DecryptDigestUpdate, C_SignEncryptUpdate 및 C_DecryptVerifyUpdate)은 구현되지 않으며, C_GetTokenInfo로 반환되는 플래그 필드의 CKF_DUAL_OPERATIONS_FLAG는 false입니다.

C_GetOperationState 및 이에 수반되는 기능 C_SetOperationState은 제한적으로 구현됩니다. C_GetOperationState는 작업이 C_Digest이고 축적된 입력 데이터의 크기가 65532바이트를 넘지 않을 때에만 수행됩니다.

Sun Crypto Accelerator 4000 시스템에서 제공하는 토큰은 삭제할 수 없습니다. 따라서 CK_GetSlotInfo에서 반환하는 CKF_REMOVABLE_DEVICE 플래그는 false입니다.

C_WaitForSlotEvent 기능은 구현되지 않으며 Sun Crypto Accelerator 4000 시스템은 Notify 매개 변수로 C_OpenSession으로 전달한 콜백 기능을 호출하지 않습니다. 소프트웨어는 C_OpenSession의 pApplication 매개 변수를 가진 호출 응용 프로그램으로 다시 제어 권한을 넘겨주지 않습니다.

Sun Crypto Accelerator 4000 보드에는 뛰어난 true 난수 생성기가 포함되어 있습니다. 또한 시드할 필요가 없으며 실제로 C_SeedRandom은 CKR_RANDOM_SEED_NOT_SUPPORTED로 거부됩니다.

호스트 메모리의 임계 필드에 따라 구현이 달라지는 기능이 true로 설정된 CKA_SENSITIVE 속성으로 생성된 키와 연관되어 있는 경우 작업은 실패하게 됩니다. 정확한 규칙은 다음과 같습니다.

- 키의 CKA_SENSITIVE가 true로 설정되어 있으면 C_DigestKey는 실패합니다.
- 기본 키 또는 파생 될 키의 CKA_SENSITIVE가 true로 설정되어 있으면 C_DeriveKey는 모든 메커니즘에 대해 실패합니다.
- 래핑 또는 래핑 해제될 키의 CKA_SENSITIVE가 true이고 다음 상태가 true이면 C_WrapKey 및 C_UnwrapKey는 실패합니다.
  - 키가 RSA 또는 DSA 키가 아닙니다.
  - 메커니즘이 CKM_DES_CBC_PAD, CKM_DES3_CBC_PAD, CKM_RC2_CBC_PAD 또는 CKM_AES_CBC_PAD가 아닙니다.

- 키의 CKA_SENSITIVE가 true로 설정되어 있으면 다음 메커니즘과 관련된 작업은 실패합니다.
  - 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...
- CKA_SENSITIVE가 true로 설정되어 있으면 2048비트보다 큰 RSA 키 또는 2048비트보다 큰 DSA와 연관된 작업은 실패합니다.

CKA_EXTRACTABLE 속성은 기본적으로 true입니다. CKA_SENSITIVE의 기본값은 CKA_EXTRACTABLE과 반대입니다. CKR_TEMPLATE_INCONSISTENT로는 CKA_SENSITIVE 및 CKA_EXTRACTABLE을 false로 설정할 수 없습니다.

불일치 속성은 일반적으로 감지되지 않습니다. 예를 들어, 템플릿에 동일한 속성이 한 번 이상 포함되면 구현은 마지막 값만 사용합니다. 키 유형과 연결되지 않은 속성은 무시됩니다. 잘못된 속성이 모두 감지되지는 않습니다.

CKA_LOCAL, CKA_ALWAYS_SENSITIVE 및 CKA_NEVER_EXTRACTABLE 속성은 구현되지 않습니다.

소프트웨어에서 반환하는 오류 코드의 내용을 항상 예상할 수 있는 것은 아닙니다. 특히, 다른 값이 보다 적절한 경우의 오류에 대해서는 대부분 CKR_MECHANISM_INVALID이 반환됩니다. 반환 코드 CKR_HOST_MEMORY는 대개 malloc(3c)의 내부 호출 명령에 실패했음을 나타냅니다. 이 오류가 반환되면 중요한 상태가 올바르게 저장되지 않았으며 C_Finalize를 호출하는 경우를 제외하면 계속할 수 없습니다.

소프트웨어의 C_EncryptInit 및 유사한 기능 구현은 오버헤드를 줄이기 위해 실제 암호화할 데이터가 있을 때까지 보드에 키의 전송을 연기합니다. 이러한 전송 연기로 인해 C_EncryptInit(및 유사한 기능)로 보고되어야 하는 PKCS#11 선언은 실제로 첫 번째 이후의 C_EncryptUpdate(및 유사한 기능) 호출 시 보고됩니다.

Sun Crypto Accelerator 4000 소프트웨어에는 다음과 같이 PKCS#11 지정자에서 인식하는 메커니즘이 들어 있습니다. 아래 목록에 나와 있는 CKM_SSL3... 및 CKM_TLS... 메커니즘은 파일 /etc/opt/SUNWconn/cryptov2/sslreg이 나타난 경우에만 키스토어가 있는 토큰에서 사용할 수 있습니다(200페이지의 "PKCS#11을 사용하기 위한 보드 관리" 참조).

- 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 및 Diffie-Hellman 키의 최대 키 크기는 다음과 같습니다.

표 8-3 최대 키 크기

키	Nonsensitive 최대 키 크기	Sensitive 최대 키 크기
RSA	4096	2048
DSA	4096	1024
DH	2048	사용할 수 없음

객체 핸들 또는 세션 핸들이 작은 정수이거나 순차적으로 할당되는 것으로 가정하지 않습니다. 이런 핸들은 오랫 동안 서명되지 않을 수도 있습니다.

C_Initialize로 전달할 수 있는 mutex 콜백 기능 포인터는 무시됩니다.

대부분의 경우 데이터의 양이 작은 작업은 보드가 아닌 호스트 프로세서에서 처리되는데, 이는 작업을 보드로 보내는 비용이 호스트에서 처리하는 비용보다 높기 때문입니다. 하지만 true로 설정된 CKA_SENSITIVE 속성을 가진 객체는 보드에서 처리됩니다.

축적된 모든 C_DigestUpdate 버퍼의 크기가 65532바이트를 넘으면 요약은 호스트 내의 소프트웨어에서 처리됩니다. 또한 C_Digest에도 동일한 특성이 적용됩니다. 따라서 용량이 작은 데이터와 매우 큰 데이터는 소프트웨어에서 처리됩니다.

사용자가 C_Login 기능을 수행하여 캐시 상태가 되면 프로세스에서 불변 객체에 관한 정보를 가져옵니다. 다른 프로세스에서 이후에 수행되는 불변 객체의 생성, 삭제 또는 변경은 관찰할 수 없습니다. 보드에서 발생하는 작업은 키의 현재 상태를 사용하게 됩니다(보드를 사용할 수 있고 키가 sensitive이거나, 보드를 사용할 수 있고 버퍼가 이를 조절할 만큼 충분히 크면 작업은 보드에서 수행됩니다). C_FindObjects 기능을 포함한 그 밖의 다른 경우는 키가 캐시된 상태로 소프트웨어에서 처리됩니다.

주의 – 이후 릴리즈에서는 변경하지 않는 위의 키 캐싱 동작에 의존하지 않습니다.

PKCS#11 표준에 따라 사용자가 C_Logout 기능을 호출하거나 마지막 PKCS#11 세션을 닫으면 모든 불변 객체 핸들을 사용할 수 없습니다. 소프트웨어는 소프트웨어의 캐시에서 토큰 객체를 제거합니다. 이후에 C_Login 기능을 수행하면 현재의 모든 토큰 객체가 나타납니다. 이 로그인을 다른 사용자로 수행하면 다른 토큰 객체 집합이 나타날 수 있습니다. 하지만 같은 사용자로 로그인을 하더라도 토큰 객체는 전과 동일한 핸들을 가져오지 못할 수 있습니다.

부록 **A**

사양

본 부록에서는 Sun Crypto Accelerator 4000 MMF 및 UTP 어댑터의 사양을 설명합니다. 다음 항목으로 구성되어 있습니다.

Sun Crypto Accelerator 4000 MMF 어댑터

이 항목은 Sun Crypto Accelerator 4000 MMF 어댑터의 사양을 설명합니다.

커넥터

그림 A-1은 Sun Crypto Accelerator 4000 MMF 어댑터의 커넥터를 설명합니다.

그림 A-1 Sun Crypto Accelerator 4000 MMF 어댑터 커넥터

표 A-1은 SC 커넥터의 특성을 설명합니다(850nm).

표 A-1 SC 커넥터 링크 특성(IEEE P802.3z)

특성	62.5마이크론 MMF	50마이크론 MMF
동작 범위	최대 260m	최대 550m

물리적 크기

표 A-2 물리적 크기

크기	치수	미터 치수
길이	12.283인치	312.00mm
너비	4.200인치	106.68mm

성능 사양

표 A-3 성능 사양

기능	사양
PCI 클럭	최대 33/66MHz
PCI 데이터 버스트 전송률	최대 64바이트 버스트
PCI 데이터/주소 폭	32/64비트
PCI 모드	마스터/슬레이브
1Gbps, 850nm	1000Mbps(전이중)

전력 요구 사항

표 A-4 전력 요구 사항

사양	치수
최대 전력 소모량	6.25 W @ 5V 12.75 W @ 3.3V
전압 안정도	5V +/- 5% 3.3V +/- 5%

인터페이스 사양

표 A-5 인터페이스 사양

기능	사양
PCI 클럭	33MHz 또는 66MHz
호스트 인터페이스	33MHz 또는 66MHz의 클럭 속도 및 3.3V 또는 5V 전력을 지원하는 PCI 2.1
PCI 버스 너비	32비트 또는 64비트

환경 사양

표 A-6 환경 사양

조건	동작 사양	보관 사양
온도	0° ~+55°C(+32° ~+131°F)	-40° ~+75°C(-40° ~+167°F)
상대 습도	5~85%, 비응축	0~95%, 비응축

Sun Crypto Accelerator 4000 UTP 어댑터

이 항목은 Sun Crypto Accelerator 4000 UTP 어댑터의 사양을 설명합니다.

커넥터

그림 A-1은 Sun Crypto Accelerator 4000 UTP 어댑터에 대한 커넥터를 설명합니다.

그림 A-2 Sun Crypto Accelerator 4000 UTP 어댑터 커넥터

표 A-7은 Sun Crypto Accelerator 4000 UTP 어댑터가 사용하는 Cat-5 커넥터의 특성을 설명합니다.

표 A-7 Cat-5 커넥터 링크 특성

특성	설명
동작 범위	최대 100m

물리적 크기

표 A-8 물리적 크기

크기	치수	미터 치수
길이	12.283인치	312.00mm
너비	4.200인치	106.68mm

성능 사양

표 A-9 성능 사양

기능	사양
PCI 클럭	최대 33/66MHz
PCI 데이터 버스트 전송률	최대 64바이트 버스트
PCI 데이터/주소 폭	32/64비트
PCI 모드	마스터/슬레이브
1Gbps	1000Mbps(전이중)
100Mbps	100Mbps(전이중 및 반이중)
10Mbps	10Mbps(전이중 및 반이중)

전력 요구 사항

표 A-10 전력 요구 사항

사양	치수
최대 전력 소모량	6.25 W @ 5V 12.75 W @ 3.3V
전압 안정도	5V +/- 5% 3.3V +/- 5%

인터페이스 사양

표 A-11 인터페이스 사양

기능	사양
PCI 클럭	33MHz 또는 66MHz
호스트 인터페이스	33MHz 또는 66MHz의 클럭 속도 및 3.3V 또는 5V 전력을 지원하는 PCI 2.1
PCI 버스 너비	32비트 또는 64비트

환경 사양

표 A-12 환경 사양

조건	동작 사양	보관 사양
온도	0° ~+55°C(+32° ~+131°F)	-40° ~+75°C(-40° ~+167°F)
상대 습도	5~85%, 비응축	0~95%, 비응축

부록 **B**

설치 스크립트 없이 소프트웨어 설치

본 부록은 제품 CD에 제공된 설치 스크립트(`/cdrom/cdrom0/install`)를 사용하지 않고 Sun Crypto Accelerator 4000 소프트웨어를 수동으로 설치하는 방법을 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

소프트웨어 수동 설치

Sun Crypto Accelerator 4000 소프트웨어는 CD에 포함되어 있습니다. SunSolve 웹 사이트(`http://sunsolve.sun.com`)에서 패치를 다운로드해야 할 경우도 있습니다. 자세한 내용은 10페이지의 "필수 패치"를 참조하십시오.

▼ 소프트웨어 수동 설치

1. **시스템에 연결된 CD-ROM 드라이브에 Sun Crypto Accelerator 4000 CD를 넣습니다.**
   - 시스템이 Sun Enterprise Volume Manager를 실행 중인 경우 CD-ROM이 `/cdrom/cdrom0` 디렉토리에 자동으로 마운트됩니다.
   - 시스템에 Sun Enterprise Volume Manager가 실행 중이 아닌 경우 다음을 입력하여 CD-ROM을 마운트합니다.

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

/cdrom/cdrom0 디렉토리에 다음 파일과 디렉토리가 표시됩니다.

표 B-1 /cdrom/cdrom0 디렉토리의 파일

파일 또는 디렉토리	내용	
Copyright	미국저작권 파일	
FR_Copyright	프랑스 저작권 파일	
install	Sun Crypto Accelerator 4000 소프트웨어의 설치 스크립트	
remove	Sun Crypto Accelerator 4000 소프트웨어의 제거 스크립트	
Docs	*Sun Crypto Accelerator 4000 보드 버전 1.1 설치 및 사용 설명서* *Sun Crypto Accelerator 4000 보드 릴리스 노트*	
Packages	Sun Crypto Accelerator 4000소프트웨어 패키지:	
	SUNWkcl2r	암호화 커널 구성 요소
	SUNWkcl2u	암호화 관리 유틸리티 및 라이브러리
	SUNWkcl2a	Apache용 SSL 지원*(옵션)*
	SUNWkcl2m	암호화 관리 매뉴얼 페이지*(옵션)*
	SUNWvcar	VCA Crypto Accelerator(루트)
	SUNWvcau	VCA Crypto Accelerator(Usr)
	SUNWvcaa	VCA 관리
	SUNWvcafw	VCA 펌웨어
	SUNWvcamn	VCA Crypto Accelerator 매뉴얼 페이지*(옵션)*
	SUNWvcav	VCA Crypto Accelerator의 SunVTS 테스트*(옵션)*
	SUNWkcl2o	SSL 개발 도구 및 라이브러리*(옵션)*
	SUNWkcl2i.u	KCLv2 Crypto를 통한 IPsec 가속화*(옵션)*

필수 패키지는 옵션 패키지 설치 전에 일정 순서에 따라 설치해야 합니다. 필수 패키지가 설치되면 순서에 상관없이 옵션 패키지를 설치하고 제거할 수 있습니다.

옵션 SUNWkcl2a 패키지는 Apache를 웹 서버로 사용하려는 경우에만 설치합니다.

옵션 SUNWkcl2o 패키지는 Apache Web Server의 다른(지원되지 않는) 버전으로 다시 연결하려는 경우에만 설치합니다.

옵션 SUNWvcav 패키지는 SunVTS 테스트를 수행하려는 경우에만 설치합니다. SUNWvcav 패키지를 설치하려면 SunVTS 4.4 이상에서 5.x까지의 버전이 설치되어 있어야 합니다.

참고 – 옵션 SUNWkcl2i.u 패키지는 Sun Crypto Accelerator 4000CD 상에서만 .u 확장자를 가지고 있습니다. 일단 패키지가 설치되면 이름이 SUNWkcl2로 변경됩니다. CD에 있는 본 패키지의 .u 확장자는 패키지를 sun4u 아키텍처 전용으로 정의합니다.

1. 다음을 입력하여 필수 소프트웨어를 설치합니다.

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2r SUNWkcl2u SUNWkcl2m SUNWvcar SUNWvcau SUNWvcaa SUNWvcamn
SUNWvcafw
```

2. (옵션) 소프트웨어가 올바르게 설치되었는지 확인하려면 pkginfo **명령을 실행합니다.**

```
# 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. (옵션) 드라이버가 부착되었는지 확인하려면 prtconf **명령을 실행합니다.**

prtdiag(1m) 온라인 매뉴얼 페이지를 참조하십시오.

```
# prtdiag -v
```

4. (옵션) modinfo **명령을 실행하여 모듈이 로드되었는지 확인합니다.**

```
# 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)
```

옵션 패키지 설치

Apache Apache Web Server에 대한 SSL 지원과 Sun Crypto Accelerator 4000 온라인 매뉴얼 페이지를 제공하는 옵션 패키지만 설치하려면 다음을 입력하십시오.

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2a SUNWkcl2m
```

옵션 소프트웨어 패키지 모두 설치하려면 다음을 입력합니다.

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2a SUNWkcl2m SUNWvcamn SUNWvcav SUNWkcl2o SUNWkcl2i.u
```

이전 예제의 옵션 패키지 내용에 대한 설명은 표 B-1을 참조하십시오.

디렉토리 및 파일

표 B-2는 Sun Crypto Accelerator 4000 소프트웨어의 기본 설치시 생성되는 디렉토리를 나타냅니다.

표 B-2 Sun Crypto Accelerator 4000디렉토리

디렉토리	내용
/etc/opt/SUNWconn/vca/keydata	키스토어 데이터(암호화)
/opt/SUNWconn/cryptov2/bin	유틸리티
/opt/SUNWconn/cryptov2/lib	지원 라이브러리
/opt/SUNWconn/cryptov2/sbin	관리 명령

그림 B-1은 이런 디렉토리 및 파일의 계층 구조를 설명합니다.

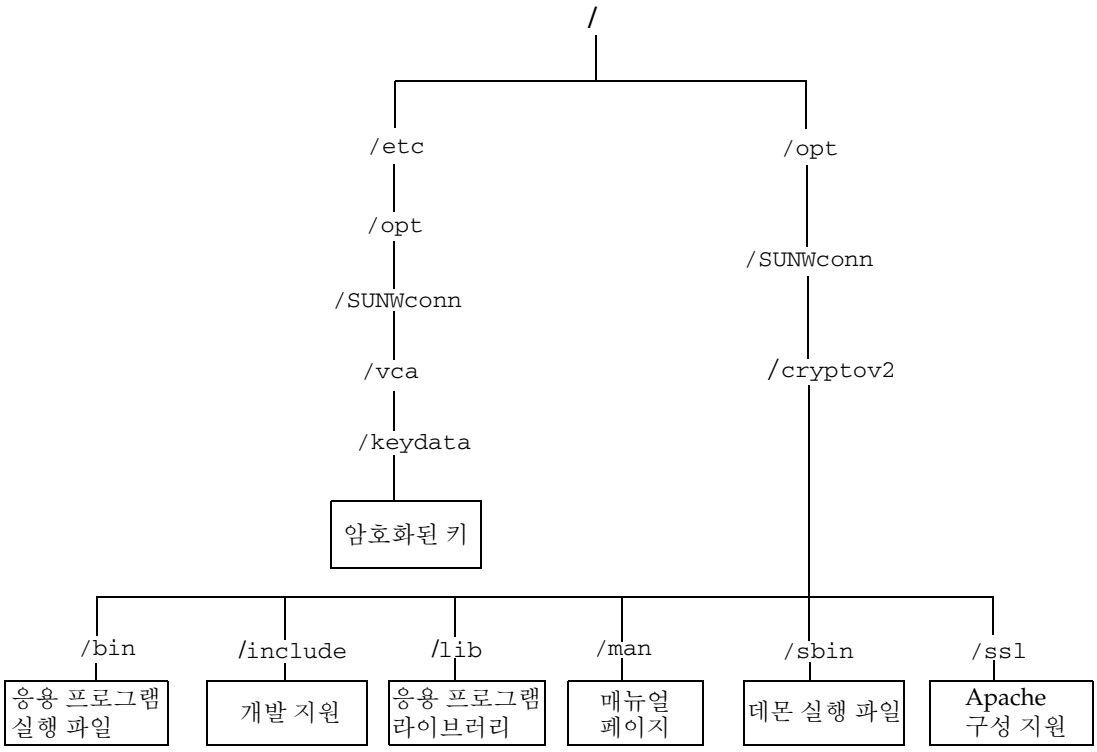

그림 B-1 Sun Crypto Accelerator 4000디렉토리 및 파일

참고 – 보드의 하드웨어와 소프트웨어가 설치되면 구성 및 키스토어 정보로 보드를 초기화해야 합니다. 보드 초기화 방법에 대한 내용은 64페이지의 "vcaadm을 통해 보드 초기화"를 참조하십시오.

소프트웨어 수동 제거

키스토어를 생성한 경우(67페이지의 "vcaadm을 통한 키스토어 관리" 참조) 소프트웨어를 삭제하기 전에 Sun Crypto Accelerator 4000 보드에 구성된 키스토어 정보를 삭제해야 합니다. `zeroize` 명령은 모든 키 요소를 제거하지만 보드가 설치된 물리적 호스트의 파일 시스템에 저장된 키스토어 파일을 삭제하지 않습니다. `zeroize` 명령에 대한 자세한 내용은 78페이지의 "보드에서 소프트웨어 초기화 수행"을 참조하십시오. 시스템에 저장된 키스토어 파일을 삭제하려면 수퍼유저 권한으로 이를 제거해야 합니다. 키스토어를 아직 생성하지 않은 경우 이 절차를 건너뛸 수 있습니다.

주의 – 현재 사용 중이거나 다른 사용자 또는 키스토어가 공유한 키스토어를 삭제하면 안됩니다. 키스토어에 대한 참조를 해제하려면 웹 서버 및/또는 관리 서버를 종료해야 할 수도 있습니다.

주의 – Sun Crypto Accelerator 4000 소프트웨어를 제거하기 전에 Sun Crypto Accelerator 4000 보드 사용을 위해 활성화한 모든 웹 서버를 비활성화해야 합니다. 그렇게 하지 않으면, 해당 웹 서버의 기능이 작동되지 않습니다.

▼ 소프트웨어 수동 제거

- **수퍼유저인 상태에서 `pkgrm` 명령을 사용하여 본인이 설치한 소프트웨어 패키지만 제거합니다.**

주의 – 설치된 패키지는 반드시 아래에 표시된 순서대로 제거해야 합니다. 그렇지 않으면 종속 경고가 발생하고 커널 모듈이 로드된 채로 남아있을 수 있습니다.

패키지를 모두 설치한 경우에는 다음 방법으로 제거합니다.

```
# pkgrm SUNWkcl2o SUNWvcav SUNWvcar SUNWkcl2a SUNWkcl2u SUNWkcl2r
SUNWvcamn SUNWkcl2m SUNWkcl2i SUNWvcaa SUNWvcafw SUNWvcau
```

참고 – Sun Crypto Accelerator 4000 보드를 위한 SunVTS 테스트(`SUNWdcav`)를 설치하거나 제거한 후에 SunVTS가 이미 실행 중인 경우에는 시스템을 재검사하여 사용 가능한 테스트를 업데이트해야 할 수 있습니다. 자세한 내용은 SunVTS 설명서를 참조하십시오.

부록 **C**

Apache Web Server를 위한 SSL 구성 지시어

본 부록에서는 Sun Crypto Accelerator 4000 소프트웨어를 사용하여 Apache Web Server를 위해 SSL 지원을 구성하는 데 필요한 지시어를 설명합니다. 지시어를 `http.conf` 파일에 구성합니다. 자세한 내용은 Apache Web Server 설명서를 참조하십시오.

1. `SSLPassPhraseDialog exec:`*program*

   컨텍스트: 전역

   이 지시어는 Apache Web Server에게 키 파일의 암호를 수집하기 위해서 지정된 *program*을 실행하도록 알립니다. *program*은 수집된 암호를 표준 출력으로 인쇄해야 합니다.

   다수의 키 파일이 표시되고 공통 암호가 있을 경우, *program*은 한 번만 실행됩니다 (각각의 수집된 암호는 *program*을 다시 실행하기 전에 이를 사용하여 시도함).

   *program*은 두 개의 인수로 실행되며 그 첫번째 인수는 서버 이름으로서 *서버 이름*:*포트*의 형식으로 나타납니다. 예를 들면 `www.fictional-company.com:443` (포트 443은SSL 기반 웹 서버의 일반 포트임)과 같습니다. 두번째 인수는 키 파일의 키 유형입니다(*keytype*). *keytype*은 RSA 또는 DSA가 될 수 있습니다.

참고 – 이 프로그램은 시스템을 시작하는 동안 실행될 수 있으므로, 콘솔이 `tty` 장치가 아닐 경우(즉, `tty`(3c)가 false를 반환하는 경우)에 대처하도록 설계되었는지 확인하십시오.

제공된 프로그램인 `/opt/SUNWconn/cryptov2/bin/apgetpass`는 *program* 실행용으로 사용할 수 있습니다. 이 프로그램은 암호 입력 프롬프트를 자동으로 표시하고 입력된 암호가 표시되지 않도록 합니다.

제공된 sslpassword 프로그램은 또한 파일 내에서 암호를 자동으로 검색하여 웹 서버 시작 시 사용자가 관여하지 않은 상태에서 수행될 수 있습니다. 키 파일의 암호는 이름이 /etc/apache/*servername*:*port*.*keytype*.pass인 파일에서 검색됩니다. 이 파일이 없는 경우 /etc/apache/default.pass 파일이 사용됩니다. 이 암호 파일은 암호화되지 않은 암호 자체를 한 행에 담고 있습니다.

참고 – 암호 파일은 웹 서버가 실행하는 UNIX 사용자만이 읽을 수 있도록 권한을 부여하여 보호해야 합니다. 이 사용자는 표준 Apache User 지시어로 구성된 사용자와 동일해야 합니다.

지정되지 않은 경우는 기본 작동은 내부 프롬프트 메커니즘을 사용합니다. 시스템 시작 시 상호 작용 문제를 방지하려면 이를 대신 sslpassword 프로그램을 사용하십시오.

2. SSLEngine (on|off)

   컨텍스트: 전역, 가상 호스트

   이 지시어는 SSL 프로토콜을 활성화합니다. 일반적으로 가상 호스트에서 서버의 하위 집합에 SSL을 활성화하는 데 사용됩니다. 공통적으로 사용되는 형식은 다음과 같습니다.

```
<VirtualHost _default_:443>
SSLEngine on
</VirtualHost>
```

   위 구문은 443 포트를 수신하는 모든 서버에 대한 SSL 사용을 구성합니다(표준 HTTPS 포트). 표시되지 않을 경우, 기본적으로 비활성화됩니다.

3. SSLProtocol [+-]*protocol*

   컨텍스트: 전역, 가상 호스트

   이 지시어는 SSL 트랜잭션을 위해 사용할 프로토콜을 구성합니다. 사용 가능한 프로토콜은 표 C-1에서 나열되어 설명됩니다.

표 C-1 SSL 프로토콜

프로토콜	설명
SSLv2	Netscape의 원본 표준 SSL 프로토콜
SSLv3	대부분의 웹 브라우저에서 지원되는 SSL 프로토콜의 업데이트 버전
TLSv1	최소 브라우저 지원을 통해 현재 IETF 표준화를 수행 중인 SSLv3로 업데이트
all	모든 프로토콜 활성화

플러스(+) 또는 마이너스(-) 기호를 사용하여 프로토콜을 추가하거나 제거할 수 있습니다. 예를 들어, SSLv2에 대한 지원을 비활성화하려면 다음 지시어를 사용할 수 있습니다.

```
SSLProtocol all -SSLv2
```

위 구문은 다음과 동일합니다.

```
SSLProtocol +SSLv3 +TLSv1
```

4. `SSLCipherSuite` *cipher-spec*

   컨텍스트: 전역, 가상 호스트, 디렉토리, `.htaccess`

   SSLCipherSuite 지시어는 사용 가능한 SSL 암호와 이들의 선호 설정을 구성할 때 사용됩니다. 전체 컨텍스트 또는 가상 호스트 컨텍스트에서는 이 지시어는 초기 SSL 핸드셰이크 중 사용됩니다. 디렉토리별 컨텍스트에서는 SSL 재교섭을 강제로 수행하여 이름이 지정된 암호를 사용합니다. 재교섭은 요청을 읽고 응답을 보내기 전 사이에 이루어집니다.

   *cipher-spec*은 표 C-2에 설명되어 있는 콜론으로 구분된 암호 목록입니다. 표 C-2에서 DH는 Diffie-Hellman을 의미하며, DSS는 Digital Signature Standard를 의미합니다.

표 C-2 사용 가능한 SSL 암호

암호-태그	프로토콜	키 교환	승인	암호화	MAC	유형
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES(168비트)	SHA1	
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES(168비트)	MD5	
RC4-SHA	SSLv3	RSA	RSA	ARCFOUR(128비트)	SHA1	
RC4-MD5	SSLv3	RSA	RSA	ARCFOUR(128비트)	MD5	
RC4-MD5	SSLv2	RSA	RSA	ARCFOUR(128비트)	MD5	
RC2-CBC-MD5	SSLv2	RSA	RSA	ARCTWO(128비트)		
DES-CBC-SHA	SSLv3	RSA	RSA	DES(56비트)	SHA1	
RC4-64-MD5	SSLv2	RSA	RSA	ARCFOUR(64비트)	MD5	
DES-CBC-MD5	SSLv2	RSA	RSA	DES(56비트)	MD5	
EXP-DES-CBC-SHA	SSLv3	RSA(512비트)	RSA	DES(40비트)	SHA1	내보내기
EXP-RC2-CBC-MD5	SSLv2	RSA(512비트)	RSA	ARCTWO(40비트)	SHA1	내보내기
EXP-RC2-CBC-MD5	SSLv3	RSA(512비트)	RSA	ARCTWO(40비트)	SHA1	내보내기
EXP-RC4-MD5	SSLv3	RSA(512비트)	RSA	ARCFOUR(40비트)	MD5	내보내기

표 C-2 사용 가능한 SSL 암호*(계속)*

암호-태그	프로토콜	키 교환	승인	암호화	MAC	유형
EXP-RC4-MD5	SSLv2	RSA(512비트)	RSA	ARCFOUR(40비트)	MD5	내보내기
NULL-SHA	SSLv3	RSA	RSA	없음	SHA1	
NULL-MD5	SSLv3	RSA	RSA	없음	MD5	
ADH-DES-CBC3-SHA	SSLv3	DH	없음	3DES(168비트)	SHA1	
ADH-DES-CBC-SHA	SSLv3	DH	없음	DES(56비트)	SHA1	
ADH-RC4-MD5	SSLv3	DH	없음	ARCFOUR(128비트)	MD5	
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES(168비트)	SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES(168비트)	SHA1	
EDH-RSA-DES-CBC-SHA	SSLv3	DH	RSA	DES(56비트)	SHA1	
EDH-DSS-DES-CBC-SHA	SSLv3	DH	DSS	DES(56비트)	SHA1	
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH(512비트)	RSA	DES(40비트)	SHA1	내보내기
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	DH(512비트)	DSS	DES(40비트)	SHA1	내보내기
EXP-ADH-DES-CBC-SHA	SSLv3	DH(512비트)	없음	DES(40비트)	SHA1	내보내기
EXP-ADH-RC4-MD5	SSLv3	DH(512비트)	없음	ARCFOUR(40비트)	MD5	내보내기

표 C-3에서는 매크로와 유사한 그룹화를 제공하는 별칭을 설명합니다.

표 C-3 SSL 별칭

별칭	설명
SSLv2	모든 SSL 버전 2.0 암호
SSLv3	모든 SSL 버전 3.0 암호
EXP	모든 내보내기 수준의 암호
EXPORT40	모든 40비트의 내보내기 암호
EXPORT56	모든 56비트의 내보내기 암호
LOW	강도가 낮은 암호(DES, 40비트 RC4)
MEDIUM	모든 128비트 암호
HIGH	3중 DES를 사용하는 모든 암호
RSA	RSA 키 교환을 사용하는 모든 암호
DH	Diffie-Hellman 키 교환을 사용하는 모든 암호
EDH	Ephemeral Diffie-Hellman 키 교환을 사용하는 모든 암호

표 C-3 SSL 별칭*(계속)*

별칭	설명
ADH	익명의 Diffie-Hellman 키 교환을 사용하는 모든 암호
DSS	DSS 인증을 사용하는 모든 암호
NULL	암호화를 사용하지 않는 모든 암호

암호의 선호도는 표 C-4에 나와 있는 특수 문자를 사용하여 구성할 수 있습니다.

표 C-4 암호 선호도를 구성하기 위한 특수 문자

문자	설명
<없음>	목록에 암호 추가
!	전체 목록에서 암호 제거 — 다시 추가할 수 없음
+	암호를 목록에 추가하고 현재 위치로 끌어냄(암호 강등)
-	목록에서 암호 제거(나중에 추가 가능)

cipher-spec 의 기본값은 다음과 같습니다.

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
```

기본값은 익명(인증되지 않은) Diffie-Hellman을 제외한 모든 암호를 구성하고 ARCFOUR 및 RSA에 선호도를 부여하여 낮은 수준에 대해 더 높은 수준의 암호화를 제공합니다.

5. `SSLCertificateFile` *file*

   컨텍스트: 전역, 가상 호스트

   이 지시어는 서버에 대한 PEM 암호화 X.509 인증 파일의 위치를 지정합니다.

6. `SSLCertificateKeyFile` *file*

   컨텍스트: 전역, 가상 호스트

   이 지시어는 서버에 대한 PEM 암호화 개인 키 파일을 지정하며, 이는 `SSLCertificateFile` 지시어로 구성된 인증서에 해당합니다.

7. `SSLCertificateChainFile` *file*

   컨텍스트: 전역, 가상 호스트

   이 지시어는 서버의 인증 경로를 만드는 PEM 암호화 인증서를 포함하는 파일의 위치를 지정합니다. 서버 인증서가 클라이언트가 인식하는 기관에 의해 직접 서명되지 않은 경우, 지시어를 사용하여 클라이언트가 서버 인증서를 확인하도록 도울 수 있습니다.

클라이언트 인증(SSLVerifyClient)을 사용할 때 체인에 있는 인증서 역시 클라이언트 인증에 유효합니다.

8. SSLCACertificateFile *file*

   컨텍스트: 전역, 가상 호스트

   이 지시어는 클라이언트 인증에 사용된 인증 기관(CA)에 대해 일련의 인증서를 포함하는 파일의 위치를 지정합니다.

9. SSLCARevocationFile *file*

   컨텍스트: 전역, 가상 호스트

   이 지시어는 클라이언트 인증에 사용된 일련의 CA 인증 거부 목록을 포함하는 파일의 위치를 지정합니다.

10. SSLVerifyClient *level*

    컨텍스트: 전역, 가상 호스트, 디렉토리, .htaccess

    이 지시어는 서버에 클라이언트 인증을 구성합니다. 일반적으로 전자상거래 응용 프로그램에 꼭 필요하지는 않지만 기타 응용 프로그램에서 사용됩니다.

    *level*에 대한 값은 표 C-5에서 나열하고 설명합니다.

표 C-5 SSL 검증 클라이언트 레벨

레벨	설명
none	클라이언트 인증서 필요 없음
optional	클라이언트는 유효한 인증서 제공 가능
require	클라이언트는 *반드시* 유효한 인증서를 제공해야 함
optional_no_ca	클라이언트가 인증서를 제공할 수 있으나 유효할 필요 없음

일반적으로 none 또는 require가 사용됩니다. 기본값은 none입니다.

11. SSLVerifyDepth *depth*

    컨텍스트: 전역, 가상 호스트, 디렉토리, .htaccess

    이 지시어는 클라이언트 인증에 대해 서버가 허용하는 인증서 체인의 최대 깊이를 지정합니다. 값이 0인 경우 자체 서명된 인증서가 적합함을 의미하며, 값이 1인 경우 클라이언트 인증서가 서버에 직접 알려진 CA에 의해 서명되어야 함을 의미합니다 (SSLCACertificateFile을 통해서). 그 이상의 값은 CA의 위임을 허용합니다.

12. `SSLLog` *filename*

    컨텍스트: 전역, 가상 호스트

    이 지시어는 SSL 관련 정보가 기록될 로그 파일을 지정합니다. 지정(기본값)되지 않을 경우, SSL 관련 정보가 기록되지 않습니다.

13. `SSLLogLevel` *level*

    컨텍스트: 전역, 가상 호스트

    이 지시어는 SSL 로그 파일에 기록된 정보의 상세 정도를 지정합니다. *level*에 대한 값은 표 C-6에서 나열하고 설명합니다.

표 C-6 SSL 로그 레벨 값

값	설명
`none`	기록되지는 않지만 오류 메시지는 표준 Apache 오류 로그로 전송됩니다.
`warn`	경고 메시지를 포함합니다.
`info`	정보 메시지를 포함합니다.
`trace`	추적 메시지를 포함합니다.
`debug`	디버그 메시지를 포함합니다.

14. `SSLOptions` [`+-`] *option*

    컨텍스트: 전역, 가상 호스트, 디렉토리, `.htaccess`

    이 지시어는 디렉토리를 기준으로 SSL 실행 시간 옵션을 구성합니다. 플러스 기호(+)를 앞에 붙여 현재 구성에 옵션을 추가하거나 마이너스 기호(-)를 사용하여 제거할 수 있습니다. 여러 옵션을 디렉토리에 적용할 수 있는 경우 가장 제한적인 옵션이 사용되며, 옵션은 결합되지 않습니다.

표 C-7에서 옵션을 나열하고 설명합니다.

표 C-7 사용 가능한 SSL 옵션

옵션	설명
`StdEnvVars`	SSL 관련 CGI/SSI 환경 변수의 표준 집합을 생성합니다. 이에 따라 성능이 저하될 수 있습니다.
`ExportCertData`	`SSL_SERVER_CERT`, `SSL_CLIENT_CERT` 및 `SSL_CLIENT_CERT_CHAIN`*n*(*n* = 0, 1, ...) 환경 변수를 내보냅니다. 이 변수는 클라이언트 및 서버에 대하 PEM 암호화 인증서를 포함합니다.
`FakeBasicAuth`	클라이언트 인증서의 고유 이름(DN)은 HTTP 기본 인증 사용자 이름으로 전환되며 인증된 것처럼 "가장"합니다. 이로 인해 암호에 대한 사용자 입력 없이 SSL 클라이언트 인증으로 표준 Apache 액세스 제어 메커니즘을 사용할 수 있습니다. Apache 암호 파일에서 사용자 항목으로 암호화된 암호 `xxj31ZMTZzkVA`를 사용해야 합니다. 이 암호는 단지 "password"라는 단어의 암호화된 형식(`crypt`(3c))입니다.
`StrictRequire`	`Satisfy Any`와 같은 SSLRequireSSL을 무시하는 지시어가 있다 하더라도 `SSLRequireSSL`로 인해 강제로 금지된 액세스가 거부되도록 합니다.

15. `SSLRequireSSL`

컨텍스트: 디렉토리, `.htaccess`

이 지시어는 HTTPS를 사용하지 않으면 해당 디렉토리에 액세스하는 것을 금지합니다. 이 지시어를 사용하여 디렉토리의 내용이 인증되지 않고 암호화되지 않은 액세스에 노출될 수 있는 잘못된 구성으로부터 보호하는 데 사용합니다.

부록 **D**

보드 사용을 위한 주문형 응용 프로그램 구성

본 부록은 보드와 함께 제공되는 소프트웨어에 대해 설명합니다. 이 소프트웨어는 보드의 암호 가속화 기능을 활용하기 위해 OpenSSL 호환 응용 프로그램을 구축하는 데 사용할 수 있습니다. 모든 OpenSSL 응용 프로그램을 이러한 방식으로 컴파일할 수 있는 것은 아닙니다. 일부 응용 프로그램은 `http://www.openssl.org`에서 다운로드하여 OpenSSL 라이브러리로 구축합니다.

보드 사용을 위한 주문형 응용 프로그램 구성

Sun Crypto Accelerator 4000 소프트웨어 및 하드웨어를 사용하기 위한 응용 프로그램의 구축에 대한 정보는 오직 있는 그대로 제공되며 이 제품에서 공식적으로 지원받은 부분이 아닙니다. 이 정보는 고객의 편리를 위한 목적으로 보증 없이 제공됩니다. Sun이 지원하는 솔루션이 필요할 경우, Sun Professional Services에 문의하여 옵션에 대한 정보를 받으십시오.

▼ 보드 사용을 위한 주문형 응용 프로그램 구성

1. **먼저 필요한 헤더 파일 및 라이브러리가 포함된** `SUNWkcl2o` **패키지를 설치해야 합니다.**
2. **다음과 같이** `/opt/SUNWconn/crypto/include`**에서 컴파일러 플래그와 함께 OpenSSL 헤더를 포함하도록 응용 프로그램을 구성해야 합니다.**

```
-I/opt/SUNWconn/cryptov2/include
```

3. **적절한 라이브러리에 참조 파일이 포함되도록 링커를 지정해야 합니다.**

   대부분의 OpenSSL 호환 응용 프로그램은 `libcrypto.a` 및 `libssl.a` 라이브러리 중 하나 또는 두 가지 모두 참조합니다. Sun 암호화 라이브러리도 포함해야 합니다. 다음 링커 속성은 이를 수행합니다.

```
-L/opt/SUNWconn/cryptov2/lib -R/opt/SUNWconn/cryptov2/lib \
-lcrypto -lssl -lkcl
```

부록 **E**

소프트웨어 라이센스

본 부록에서는 Sun Binary Code 라이센스 계약과 타사 소프트웨어 통지 및 라이센스 조항을 설명합니다.

참고 – 본 부록에서 제공하는 타사 라이센스 및 통지는 해당 소프트웨어 라이센스 및 통지 소유업체가 제공하는 바와 일치합니다.

Sun Microsystems, Inc.

Binary Code 라이센스 계약

소프트웨어 매체 패키지를 개봉하기 전에 본 계약의 조항 및 기타 추가 라이센스 조항(집합적으로 "계약"으로 통칭)을 상세히 읽으십시오. 본 소프트웨어 매체 패키지를 개봉함으로서 귀하는 본 계약의 조항에 동의하게 됩니다. 전자적으로 소프트웨어에 접근한 경우 계약 하단에 "동의" 단추를 선택하면 본 조항을 수용하게 됩니다. 모든 조항에 동의하지 않는 경우 즉시 사용하지 않은 소프트웨어를 구매처에 반납하여 환불을 받거나 전자적으로 접근한 경우 계약 하단의 "동의 안함" 단추를 선택하십시오.

1. 사용 라이센스. Sun은 지불한 요금에 해당하는 사용자 수와 컴퓨터 하드웨어 종류에 따라 해당 소프트웨어 및 설명서와 함께 내부에서만 사용할 수 있는 비독점, 이양 불가한 라이센스와 자사가 제공하는 오류 수정(이를 모두 "소프트웨어"라고 함) 에 대한 권리를 구매자에게 부여합니다.

2. 제한 사항. 소프트웨어는 기밀 사항이며 저작권의 보호를 받습니다. Sun 및/또는 기타 인가자는 소프트웨어 타이틀 및 모든 관련 지적 재산권을 보유합니다. 추가 라이센스 조항을 통해 명확히 허가한 경우를 제외하고 보관을 위한 복사본을 1개만 만들어야 합니다. 관련 법규에 따라 허용되지 않는 한 소프트웨어를 수정, 디컴파일 또는 리버스 엔지니어링할 수 없습니다. 이 소프트웨어는 원자력 시설의 설계, 건축 및 응용 등의 목적으로 설계되거나 및 인가되지 않았다는 것을 인정합니다. Sun은 이런 경우의 사용 적절성을 명시적 또는 암묵적으로 보증하지 않습니다. 본 계약에서는 Sun 또는 인가자의 상표, 서비스 마크, 로고 또는 상표 이름에 대한 권리나 타이틀, 이권을 부여하지 않습니다.

3. 제한 보증. Sun은 영수증 사본을 그 증거로 하여 구매일로부터 90일 간 소프트웨어를 제공하는 매체에 물질적인 결함이 없으며 정상적인 환경에서 올바르게 기능을 발휘함을 보증합니다. 위의 경우를 제외하고 소프트웨어는 "있는 그대로" 제공됩니다. 본 제한 보증 하에서 사용자의 배타적 배상과 Sun의 전면 책임은 소프트웨어 매체를 교환하거나 소프트웨어 구매 금액을 환불하는 Sun의 선택에 따릅니다.

4. 보증 거부. 본 계약서에 명시하지 않은 경우, 상품성의 묵시적 보증 및 특정 목적 또는 비침해성에 대한 적합성을 포함한 일체의 명시적 또는 묵시적 조건, 진술 및 보증에 대해 책임을 지지 않습니다. 이러한 보증 거부는 법적으로 허용된 범위 내에서만 적용됩니다.

5. 책임 제한. 법률에서 금하지 않는 범위까지 어떤 경우에도 Sun과 인가자는 수익, 순익, 데이터 등의 손실과, 책임 이론과 상관 없이 손상 가능성을 사전에 통지했음에도 불구하고 이 소프트웨어의 사용과 관련하여 발생한 특수적, 간접적, 필연적, 우발적 또는 징계적 손해에 대해 책임을 지지 않습니다. 본 계약 하에서 Sun의 책임 범위는 계약을 통한 것이든 불법이든(과실 포함) 어떠한 경우에도 소프트웨어 구매 금액을 넘지 않습니다. 위의 한계 조항은 앞서 말한 보증이 필수 목적을 달성하지 못한 경우에도 적용됩니다.

6. 파기. 본 계약은 파기되기 전까지 유효합니다. 본 소프트웨어의 모든 사본을 폐기하여 이 계약을 언제든 파기할 수 있습니다. 구매자가 본 계약의 조항에 응하지 않으면 Sun의 사전 경고 없이 본 계약은 즉시 파기됩니다. 파기 시에는 모든 소프트웨어 사본을 폐기해야 합니다.

7. 수출 법규. 본 계약 하에 전달되는 모든 소프트웨어와 기술 데이터는 미국 수출관리법의 적용 대상이며 다른 국가에서 수출입 법률의 적용 대상이 될 수 있습니다. 본 계약으로 사용자는 이와 같은 모든 법률과 규칙을 엄수할 것에 동의하고 이후 수출, 재수출, 수입을 위해 필요한 허가를 획득할 책임이 있음을 인지하는 것입니다.

8. 미국정부의 제한 권리. 미국 정부, 정부 주요 도급 업체 및 하도급 업체(전 단계)가 본 소프트웨어를 구입한 경우 정부의 소프트웨어 및 동반 문서에 대한 권리는 본 계약 안에서만 밝힐 수 있습니다. 이는 48 CFR 227.7201에서 227.7202-4(국방부(DOD) 구입물 대상)과 48 CFR 2.101 및 12.212(비국방부(non-DOD) 구입물 대상)에 따릅니다.

9. 관할법. 본 계약과 관련한 모든 조치는 캘리포니아법과 미국 관할법에 따릅니다. 연방법. 선택적 법률 적용은 유효하지 않습니다.

10. 분리 가능성본 계약의 어떤 조항이 집행 불가인 경우, 생략된 조항이 계약 당사자의 의도를 침해하지 않으면 본 동의는 해당 조항을 제외하고 유효합니다. 생략된 조항이 계약 당사자의 의도를 침해하는 경우, 본 계약은 즉시 파기됩니다.

11. 통합본 동의는 해당 사안에 대한 구매자와 Sun 간의 완전 합의입니다. 본 계약은 모든 이전 혹은 동시 발생한 구두 또는 서면 전달, 제안, 진정 및 보증을 대체하며 계약 기간 중 관련 사안에 해당하는 계약 당사자 간의 인용, 주문, 승인 또는 기타 의사 교환의 상충 또는 추가 조건보다 우위에 있습니다. 계약 당사자 간의 권한을 가진 대표가 서명하지 않은 한 본 계약서의 수정은 효력이 없습니다.

질의 사항은 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054로 연락주시기 바랍니다.

(양식 ID#011801)

Sun Microsystems, Inc.

Sun Crypto Accelerator 4000에 대한 추가 조항

Sun Crypto Accelerator 4000에 대한 본 추가 조항은 Binary Code 라이센스 계약("BCL")을 보충합니다. 여기서 정의되지 않은 대문자로 시작하는 조항은 BCL의 해당 의미로 간주합니다. 이 추가 조항은 BCL의 불일치되거나 모순되는 조항보다 우선합니다. 소프트웨어의 사용은 여기서 보충하는 BCL의 수용을 의미합니다.

1. 타사 라이센스 조항. 소프트웨어의 일부는 사용을 관할하는 타사로부터 통지 및/또는 라이센스를 제공받습니다.

타사 라이센스 조항

OPENSSL 라이센스 공표

OpenSSL 툴킷은 이중 라이센스 하에 있습니다(예: OpenSSL 라이센스 및 툴킷에 적용되는 원본 SSLeay 라이센스 약관). 현행 라이센스 내용을 보려면 아래를 참조하십시오. 두 라이센스는 모두 BSD 유형의 오픈 소스 라이센스입니다. OpenSSL에 관련된 라이센스 발행에 대한 문의는 openssl-core@openssl.org로 연락하십시오.

OpenSSL 라이센스

Copyright (c) 1998-2001 The OpenSSL Project. 모든 권리는 저작권자의 소유입니다.

소스 및 바이너리 형식의 재배포 및 사용은 수정의 여부에 관계 없이 다음 조건에 적합할 경우에만 허용됩니다.

1. 소스 코드의 재배포 시에는 상기 판권 소유 경고, 약관 목록 및 권리 포기 문서(아래)를 따라야 합니다.

2. 바이너리 형식의 재배포 시에는 함께 제공될 문서 및/또는 기타 자료에 상기 판권 소유 경고, 약관 목록 및 권리 포기 문서를 포함해야 합니다.

3. 본 소프트웨어를 사용하거나 해당 기능에 대해 언급하는 모든 광고용 자료에는 다음을 명시해야 합니다. "본 제품에는 OpenSSL Toolkit(http://www.openssl.org/)에 사용할 목적으로 OpenSSL Project가 개발한소프트웨어가 포함되어 있습니다."

4. "OpenSSL Toolkit" 및 "OpenSSL Project"라는 명칭은 사전 서면 허가 없이 소프트웨어에서 파생된 제품을 보증하거나 홍보할 목적에 사용될 수 없습니다. 서면 허가에 대한 문의는 openssl-core@openssl.org로 연락하십시오.

5. 이 소프트웨어에서 파생된 제품은 OpneSSL Project의 사전 서면 허가 없이 "OpenSSL"로 호칭하거나 "OpenSSL"이라는 이름으로 표기될 수 없습니다.

6. 어떠한 형태로든 재배포 시에는 다음을 명시해야 합니다. "본 제품에는 OpenSSL Toolkit(http://www.openssl.org/)에 사용할 목적으로 OpenSSL Project가 개발한 소프트웨어가 포함되어 있습니다."

이 소프트웨어는 OpenSSL Project에 의해 "있는 그대로" 제공되며 상품성의 암시적 보증 및 특정 목적에의 적합성을 포함한 일체의 암시적 또는 묵시적 보증에 대해 책임지지 않습니다. 손상 가능성을 사전에 통지했음에도 불구하고 이 소프트웨어의 사용 범위를 벗어나 발생한 직접적, 간접적, 우발적, 특수적, 징계적 또는 필연적인 손해(대체 상품 또는 서비스의 획득, 사용권, 데이터, 또는 수익 상실, 또는 업무적 방해 포함) 및 책임성, 계약상에 포함되는지 여부와 관계없이, 또는 불법 행위(과실 또는 기타 방식)에 대해 OpenSSL Project 또는 기타 공헌자는 배상에 대한 책임을 지지 않습니다.

이 제품에는 Eric Young(eay@cryptsoft.com)이 작성한 암호화 소프트웨어가 포함되어 있습니다. 이 제품에는 Tim Hudson(tjh@cryptsoft.com)이 작성한 소프트웨어가 포함되어 있습니다.

원본 SSLeay 라이센스

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

이 패키지는 Eric Young(eay@cryptsoft.com)이 개발한 SSL 구현물입니다. Netscapes SSL과 호환되도록 작성되었습니다.

이 라이브러리는 다음 약관을 준수하는 조건 하에 상업용 또는 비상업용으로 사용될 수 있습니다. 다음 약관은 SSL 코드 뿐만 아니라 배포물에 포함된 모든 코드, 즉 RC4, RSA, lhash, DES 코드 등에 적용됩니다. 배포물에 포함된 SSL 문서는 소유자가 Tim Hudson (tjh@cryptsoft.com)이라는 점을 제외하고는 동일한 판권 소유 약관이 적용됩니다.

코드의 판권 소유 경고가 제거되지 않는한 판권 소유는 Eric Young에게 있습니다.

이 패키지를 제품에 사용할 경우, 사용된 일부 라이브러리의 저자로 Eric Young을 언급해야 합니다. 프로그램 시작 시 텍스트 메시지 형식으로 또는 패키지에 함께 제공되는 문서(온라인 또는 텍스트) 형식 등으로 할 수 있습니다.

소스 및 바이너리 형식의 재배포 및 사용은 수정의 여부에 관계 없이 다음 조건에 적합할 경우에만 허용됩니다.

1. 소스 코드의 재배포 시에는 판권 소유 경고, 약관 목록 및 권리 포기 문서(아래)를 따라야 합니다.
2. 바이너리 형식의 재배포 시에는 함께 제공될 문서 및/또는 기타 자료에 상기 판권 소유 경고, 약관 목록 및 권리 포기 문서를 포함해야 합니다.
3. 본 소프트웨어를 사용하거나 해당 기능에 대해 언급하는 모든 광고용 자료에는 다음을 명시해야 합니다. "본 제품에는 Eric Young (eay@cryptsoft.com)이 작성한 암호화 소프트웨어가 포함되어 있습니다." ('암호화'라는 단어는 사용 중인 라이브러리의 루틴이 암호화 관련 내용이 아닐 경우에는 무시할 수 있습니다).
4. 응용 프로그램 디렉토리(응용 프로그램 코드)로부터 Windows 고유 코드(또는 Windows에서 파생된)를 포함할 경우, 다음을 명시해야 합니다. "본 제품에는 Tim Hudson (tjh@cryptsoft.com)이 작성한 소프트웨어가 포함되어 있습니다."

이 소프트웨어는 Eric Young에 의해 "있는 그대로" 제공되며 상품성의 암시적 보증 및 특정 목적에의 적합성을 포함한, 그러나 국한되지 않고, 일체의 암시적 또는 묵시적 보증에 대해 책임지지 않습니다. 손상 가능성을 사전에 통지했음에도 불구하고 이 소프트웨어의 사용 범위를 벗어나 발생한 직접적, 간접적, 우발적, 특수적, 징계적 또는 필연적인 손해(대체 상품 또는 서비스의 획득, 사용권, 데이터, 또는 수익 상실, 또는 업무적 방해 포함) 및 책임성, 계약상에 포함되는지 여부와 관계없이, 또는 불법 행위(과실 또는 기타 방식)에 대해 저자 또는 기타 공헌자는 배상에 대한 책임을 지지 않습니다.

출시된 모든 버전 및 파생 코드에 대한 라이센스 및 배포 약관은 변경할 수 없습니다. 즉, 이 코드를 복사하거나 다른 배포 라이센스 하[GNU Public Licence 포함]에서 사용할 수 없습니다.

> ``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 라이센스

mod_ssl 패키지는 BSD 유형의 라이센스 하에 배포되므로 오픈 소스 소프트웨어 레이블에 해당됩니다. 라이센스에 대한 자세한 정보가 아래에 나와 있습니다.

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

소스 및 바이너리 형식의 재배포 및 사용은 수정의 여부에 관계 없이 다음 조건에 적합할 경우에만 허용됩니다.

1. 소스 코드의 재배포 시에는 상기 판권 소유 경고, 약관 목록 및 권리 포기 문서(아래)를 따라야 합니다.

2. 바이너리 형식의 재배포 시에는 함께 제공될 문서 및/또는 기타 자료에 상기 판권 소유 경고, 약관 목록 및 권리 포기 문서를 포함해야 합니다.

3. 본 소프트웨어를 사용하거나 해당 기능에 대해 언급하는 모든 광고용 자료에는 다음을 명시해야 합니다. "본 제품에는 mod_ssl 프로젝트(http://www.modssl.org/)에 사용할 목적으로 Ralf S. Engelschall <rse@engelschall.com>이 개발한 소프트웨어가 포함되어 있습니다."

4. "mod_ssl"라는 명칭은 사전 서면 허가 없이 소프트웨어에서 파생된 제품을 보증하거나 홍보할 목적에 사용될 수 없습니다. 쓰기 권한에 대한 문의는 rse@engelschall.com으로 연락하십시오.

5. 이 소프트웨어에서 파생된 제품은 Ralf S.의 사전 서면 허가 없이 "mod_ssl"로 호칭하거나 "mod_ssl"이라는 이름으로 표기될 수 없습니다. Engelschall.

6. 어떠한 형태로든 재배포 시에는 다음을 명시해야 합니다. "본 제품에는 mod_ssl 프로젝트(http://www.modssl.org/)에 사용할 목적으로 Ralf S. Engelschall <rse@engelschall.com>이 개발한 소프트웨어가 포함되어 있습니다."

이 소프트웨어는 Ralf S. Engelschall에 의해 "있는 그대로" 제공되며 상품성의 암시적 보증 및 특정 목적에의 적합성을 포함한, 그러나 국한되지 않고, 일체의 암시적 또는 묵시적 보증에 대해 책임지지 않습니다. 손상 가능성을 사전에 통지했음에도 불구하고이 소프트웨어의 사용 범위를 벗어나 발생한 직접적, 간접적, 우발적, 특수적, 징계적 또는 필연적인 손해(대체 상품 또는 서비스의 획득, 사용권, 데이터, 또는 수익 상실, 또는 업무적 방해 포함) 및 책임성, 계약상에 포함되는지 여부와 관계없이, 또는 불법 행위(과실 또는 기타 방식)에 대해 Ralf S. Engelschall 또는 기타 공헌자는 배상에 대한 책임을 지지 않습니다.

부록 **F**

매뉴얼 페이지

본 부록은 보드 소프트웨어의 Sun Crypto Accelerator 4000 명령 및 유틸리티에 대해 설명하고 각각의 온라인 매뉴얼 페이지를 나열합니다.

다음 명령을 입력하여 온라인 매뉴얼 페이지를 볼 수 있습니다.

```
man -M /opt/SUNWconn/man 페이지 이름
```

표 F-1은 사용 가능한 온라인 매뉴얼 페이지를 설명합니다.

표 F-1 Sun Crypto Accelerator 4000 온라인 매뉴얼 페이지

man 페이지	설명
vca(7d)	내재된 하드웨어 암호화 가속기에 액세스 컨트롤을 제공하는 리프 드라이버
vcad(1m)	키스토어 서비스를 제공하는 데몬
vcaadm(1m)	구성, 계정 및 보드와 연결된 키 관련 데이터베이스를 관리하는 유틸리티
vcadiag(1m)	수퍼유저가 보드를 재설정하고 키 요소를 원상 복구하며 기본 진단을 수행할 수 있게 해주는 유틸리티
kcl2(7d)	kcl2은 암호화 하드웨어 드라이버를 지원하는 커널 모듈입니다.
apsslcfg(1m)	Apache Web Server용 구성 유틸리티
iplsslcfg(1m)	Sun ONE Web Server용 구성 유틸리티
pk11export(1m)	PKCS#11 인터페이스를 사용하는 키 내보내기 유틸리티

부록 **G**

하드웨어 초기화

본 부록은 Sun Crypto Accelerator 4000 보드의 하드웨어를 초기화하여 보드를 출하 시 상태로 복구하는 방법을 설명합니다. 보드를 출하 시 상태로 복구하면 failsafe 모드가 됩니다.

주의 – 하드웨어 초기화는 반드시 필요한 경우에만 수행해야 합니다. 모든 키 요소만 제거하려는 경우 `vcaadm` 프로그램에서 `zeroize` 명령으로 소프트웨어 초기화를 수행합니다. `zeroize` 명령에 대한 자세한 내용은 78페이지의 "보드에서 소프트웨어 초기화 수행"을 참조하십시오. 또한 모든 키 요소 삭제에 대해서는 `vcadiag`(4)의 온라인 매뉴얼 페이지를 참조하십시오.

참고 – 보드에서 하드웨어 초기화를 수행하면 Sun Crypto Accelerator 4000 펌웨어도 제거됩니다. Sun Crypto Accelerator 4000 소프트웨어와 함께 제공된 펌웨어를 다시 설치해야 합니다.

Sun Crypto Accelerator 4000 하드웨어를 출하 시 상태로 초기화

어떤 경우에는 보드를 `failsafe` 모드로 복구하고 모든 키 요소와 구성 정보를 삭제해야 할 때가 있습니다. 이 작업은 표준 SCSI 하드웨어 점퍼(션트)를 통해서만 수행할 수 있습니다.

참고 – vcaadm 프로그램과 zeroize 명령을 사용하여 Sun Crypto Accelerator 4000 보드에서 모든 키 요소를 제거할 수 있습니다. 그러나 zeroize 명령은 업데이트된 펌웨어를 보존합니다. 78페이지의 "보드에서 소프트웨어 초기화 수행"를 참조하십시오. 또한 vcadiag(4) 온라인 매뉴얼 페이지도 참조하십시오.

▼ 하드웨어 점퍼를 통한 Sun Crypto Accelerator 4000 보드 초기화

1. **시스템 전원을 끕니다.**

참고 – 일부 시스템에서는 본 절차에 대해 전원을 끄는 대신에 동적 재구성(DR)을 통해 필요한 보드를 제거하고 교체할 수 있습니다. 적절한 DR 절차는 시스템과 함께 제공된 설명서를 참조하십시오.

주의 – 점퍼를 조정하는 동안 보드에 전력이 공급되면 안됩니다.

2. **컴퓨터 덮개를 제거하여 보드의 상단 중앙에 있는 점퍼에 접근합니다.**
3. **점퍼를 점퍼 블록의 0 및 1 핀에 끼웁니다.**

   1 및 2 핀은 브래킷에 가장 가까운 핀입니다. 2핀씩 4조로 구성되어 있으며, 점퍼는 그림 G-1에서처럼 1과 2핀에 끼워야 합니다.

주의 – 보드는 1 및 2핀의 점퍼와 동작하지 않습니다.

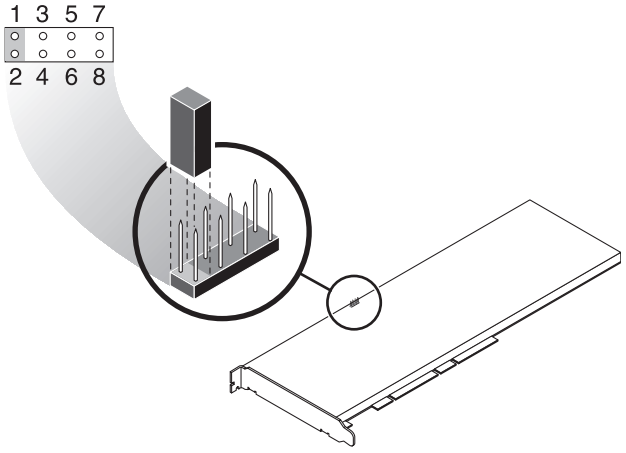

그림 G-1 하드웨어 점퍼 블록 핀

4. **시스템을 켭니다.**

주의 – 점퍼를 조정한 후 시스템의 전원을 켜면 모든 펌웨어, 키 요소 및 구성 정보가 삭제됩니다. 이 절차를 통해 보드는 출하 시 상태로 복구되고 failsafe 모드로 전환됩니다.

5. **시스템 전원을 끕니다.**
6. **점퍼 블록의 0과 1핀에서 점퍼를 제거하고 점퍼를 원래 위치에 보관합니다.**
7. **시스템을 켭니다.**
8. **`vcaadm`으로 Sun Crypto Accelerator 4000 보드에 연결합니다.**

   `vcaadm` 프롬프트가 나타나면 펌웨어 업그레이드 경로를 입력합니다.
9. **펌웨어 설치 경로로 `/opt/SUNWconn/cryptov2/firmware/sca4000fw`를 입력합니다.**

   펌웨어가 자동 설치되고 `vcaadm`에서 로그아웃됩니다.
10. **`vcaadm`으로 Sun Crypto Accelerator 4000 보드에 다시 연결합니다.**

    `vcaadm` 프롬프트는 새 키스토어로 보드를 초기화할 것인지, 기존 키스토어로 초기화할 것인지를 묻습니다. 64페이지의 "`vcaadm`을 통해 보드 초기화"를 참조하십시오.

색인

심볼

숫자

A

P

R

S

T

U

V

W

Z

ㄱ

ㄴ

ㄷ

ㄹ

ㅁ