Sun™ Crypto Accelerator 1000 보드 설치 및 사용자 설명서

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054 U.S.A.
650-960-1300

부품 번호816-4568-10
2002년 3월, 개정판 A

이 문서에 대한 의견은 다음 주소로 보내 주십시오. docfeedback@sun.com

재활용
하십시오.

Adobe PostScript

Declaration of Conformity

EMC

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

European Union

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

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

Safety

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

EC Type Examination Certificates:

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

Supplementary Information

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

/S/

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

/S/

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

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.

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

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

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

*Sun Crypto Accelerator 1000 보드 설치 및 사용자 설명서*는 Sun™ Crypto Accelerator 1000 보드의 기능 및 시스템에 보드를 설치하고 사용하는 방법에 대해 설명합니다.

이 설명서는 Solaris 운영 환경에 익숙한 시스템 관리자를 대상으로 합니다.

UNIX 명령 사용

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

이러한 정보를 보려면 다음 문서를 참조하십시오.

- *Solaris 하드웨어 플랫폼 안내서*
- Solaris™ 운영 환경에 대한 AnswerBook2™ 온라인 서적
- 시스템과 함께 제공된 소프트웨어 설명서

활자체 규약

활자체	의미	예
AaBbCc123	명령어, 파일 및 디렉토리 이름 (컴퓨터 화면에 출력)	.login 파일을 편집합니다. 모든 파일을 나열하려면 ls -a를 사용합니다. % You have mail.
AaBbCc123	화면의 컴퓨터 출력과 구별되는 사용자가 입력하는 값입니다.	% **su** Password:
AaBbCc123	문서 제목, 새 단어 또는 용어, 강조할 단어	*사용자 설명서*의 6장을 참조하십시오. 이것을 *클래스* 옵션이라고 합니다. 이 작업을 수행하려면 *반드시* 수퍼유저이어야 합니다.
	실제 이름이나 값으로 대체되는 명령행 변수	파일을 삭제하려면 rm *filename*을 입력하십시오.

쉘 프롬프트

쉘	프롬프트
C 쉘	*machine_name*%
C 쉘 수퍼유저	*machine_name*#
Bourne 쉘 및 Korn 쉘	$
Bourne 쉘 및 Korn 쉘 수퍼유저	#

Sun 온라인 설명서 액세스

다음 웹 사이트에서 다양한 종류의 Sun 시스템 설명서를 볼 수 있습니다.

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

다음 웹 사이트에서 전체 Solaris 설명서 및 다양한 기타 책자를 볼 수 있습니다.

`http://docs.sun.com`

Sun에 대한 고객 의견을 보내주십시오

Sun은 문서의 품질을 향상하기 위한 고객의 의견 및 제안을 환영합니다. 다음 전자 우편 주소로 의견을 보내실 수 있습니다.

`docfeedback@sun.com`

전자 우편의 제목에 문서 부품 번호(816-4568-10)를 기재해 주십시오.

1 장

제품 개요

이 장에서는 Sun Crypto Accelerator 1000 보드에 대해 설명합니다.

이 장은 다음 절로 구성되어 있습니다.

하드웨어 개요

Sun Crypto Accelerator 1000 보드는 짧은 PCI 보드로 공용 키와 대칭 암호화를 가속시키는 암호 보조 처리기 역할을 합니다. 이 제품에는 외부 인터페이스가 없습니다. 보드는 내부 PCI 버스 인터페이스를 통해 호스트와 통신합니다. 이 보드의 목적은 전자 상거래 응용 프로그램의 보안 프로토콜을 위한 다양한 계산 집중 암호화 알고리즘을 가속화하는 데 있습니다.

.

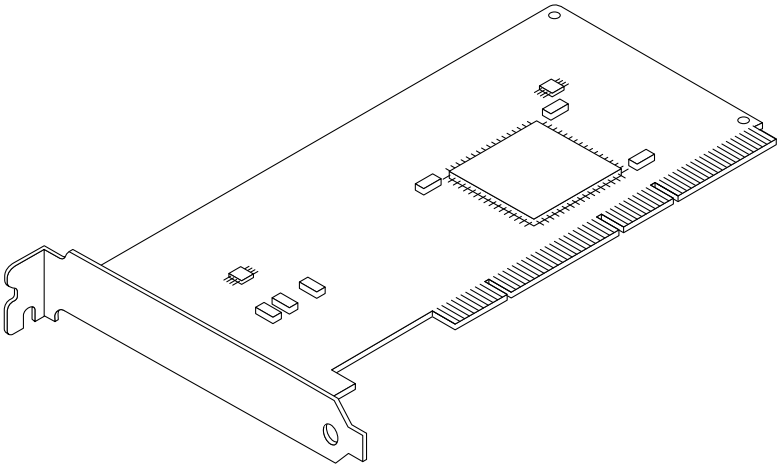


그림 1-1 Sun Crypto Accelerator 1000 보드

제품 기능

Sun Crypto Accelerator 1000은 Sun 플랫폼에서 SSL의 성능을 향상시키는 암호 가속기 보드입니다. Sun Crypto Accelerator 1000은 하드웨어와 소프트웨어 모두에서 암호화 알고리즘을 가속화합니다. 이렇게 복잡한 이유는 암호화 알고리즘을 가속화하는 데 드는 비용이 모든 알고리즘에서 동일한 것이 아니기 때문입니다. 일부 암호화 알고리즘은 하드웨어에서 구현되도록 특별히 설계된 반면 다른 알고리즘은 소프트웨어에서 구현되도록 설계되었습니다. 하드웨어 가속화에서 있어서 추가로, 데이터를 사용자 응용 프로그램 공간에서 하드웨어 가속 장치로 이동하고 그 결과를 다시 사용자 응용 프로그램으로 이동하는 데 큰 비용이 듭니다.

일부 암호화 알고리즘(예: ARCFOUR)은 전용 하드웨어에서 수행될 수 있는 것과 마찬가지로 신속하게 고도로 조정된 소프트웨어에서 수행될 수 있습니다. Sun Crypto Accelerator 1000 제품은 각 암호화 요청을 검사하고 최상의 가속 위치(호스트 프로세서 또는 Sun Crypto Accelerator 1000)를 결정하여 최대 처리량을 달성합니다. 부하 분산은 암호화 알고리즘, 현재 작업 로딩 및 데이터 크기를 기반으로 합니다.

표 1-1에는 하드웨어로 부하 이동될 가속 알고리즘 및 iPlanet 및 아파치 웹 서버에 제공될소프트웨어 알고리즘이 표시되어 있습니다.

표 1-1 SSL 지원 알고리즘

	IPlanet 웹 서버		Apache 웹 서버	
알고리즘	**하드웨어**	**소프트웨어**	**하드웨어**	**소프트웨어**
RSA	X	X	X	X
DSA	X	X	X	X
Diffie-Hellman			X	X
DES	X	X	X	X
3DES	X	X	X	X
ARCFOUR		X		X

동적 재구성 및 고 가용성 고려 사항

Sun Crypto Accelerator 1000 하드웨어 및 관련 소프트웨어는 동적 재구성(DR) 및 핫 플러깅을 지원하며 Sun 플랫폼에서 효과적으로 작동됩니다. DR 또는 핫 플러그 작업이 발생할 경우, Sun Crypto Accelerator 1000 계층은 보드의 추가나 제거를 자동으로 검사하고 일정 알고리즘을 조정하여 하드웨어 리소스에서 변경 사항을 수용합니다.

고 가용성(HA) 구성을 하려면, 시스템 또는 도메인에 여러 개의 Sun Crypto Accelerator 1000 보드를 설치하여 하드웨어 가속을 계속적으로 사용할 수 있습니다. Sun Crypto Accelerator 1000 하드웨어에 장애가 발생할 경우, 소프트웨어 계층이 장애를 검사하고 사용 가능한 하드웨어 암호화 가속기 목록에서 카드를 제거합니다. Sun Crypto Accelerator 1000이 일정 알고리즘을 조절하여 하드웨어 리소스에서의 감소를 제공합니다. 그 이후의 암호화 요청은 남아있는 카드로 넘어갑니다.

추가로, Sun Crypto Accelerator 1000 소프트웨어 라이브러리는 소프트웨어에서 모든 암호화 작업을 수행할 수 있는 능력을 제공합니다. 시스템 도메인 내에서 역기능 결과 없이 Sun Crypto Accelerator 1000 보드 전체의 DR 또는 핫 플러그 제거를 지원합니다. Sun Crypto Accelerator 1000 하드웨어 구성이 복구될 때까지 현저한 성능 저하가 발생될 것입니다.

Sun Crypto Accelerator 1000 하드웨어는 장기적 키 작성을 위한 고품질의 엔트로피 소스를 제공합니다. 하나의 도메인 또는 시스템 내의 Sun Crypto Accelerator 1000 보드가 모두 제거되면 장기적 키는 저품질의 엔트로피로 작성됩니다.

부하 공유

Sun Crypto Accelerator 1000 소프트웨어는 Solaris 도메인 또는 시스템 내에 설치된 여러 보드로 부하를 분산시킵니다. 입력되는 암호화 요청은 정해진 길이의 작업 대기열에 기초한 보드로 분산됩니다. 요청된 유형을 수용할 수 있는 첫 번째 보드의 대기열에 들어갑니다. 대기 메커니즘은 보드에서 요청의 결합을 통해 최적화하도록 설계되었습니다.

하드웨어 및 소프트웨어 요구 사항

표 1-2에는 Sun Crypto Accelerator 1000보드에 대한 하드웨어 및 소프트웨어 요구사항이 나와 있습니다.

표 1-2 하드웨어 및 소프트웨어 요구 사항

하드웨어 및 소프트웨어	요구 사항
하드웨어	Sun Blade™ 1000 Sun Enterprise™ 220R, 250, 420R, 450 Sun Fire™ 280R, V480, V880, 4800, 4810, 6800 Sun Netra™ T1 AC200/DC200, Netra 20, Netra t 1400/1405 Sun Ultra™ 60, 80
운영 환경	Solaris 8 7/01 이상의 호환 릴리스
PCI 슬롯	32비트 또는 64비트 33 MHz 또는 66 MHz
소프트웨어	iPlanet™ 웹 서버 4.1 SP9, 6.0 SP1 또는 아파치 웹 서버 1.3.12 iPlanet 웹 서버 또는 아파치 웹 서버를 실행하는 데 필요한 모든 패치

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

필요한 패치

다음 패치는 시스템에서 Sun Crypto Accelerator 1000을 실행하는 데 필요합니다. Solaris 업데이트에 이전 릴리스에 대한 패치가 포함되어 있습니다. `showrev -p` 명령을 사용하여 나열된 패치가 설치되어 있는지 결정합니다.

필요할 경우, 다음 웹사이트에서 패치를 다운로드할 수 있습니다. `http://sunsolve.sun.com`.

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

필요한 패치가 SunSolve℠에 없는 경우는 지역 영업 센터 또는 서비스 대리점으로 연락하십시오.

다음 표에는 이 제품과 함께 사용할 수 있는 필요하고 권장되는 패치가 나열되어 있습니다. 표 1-3에는 필요 패치가 나열되어 있습니다.

표 1-3 Sun Crypto Accelerator 1000 소프트웨어에 필요한 패치

패치 ID	설명
110383-01	`libnvpair`
108528-05	`KU-05` (`nvpair` 지원)
112438-01	`/dev/random`

주 – 아파치 1.3.12 웹 서버를 사용하려면 패치 번호 109234-02를 설치해야 합니다.

표 1-4에는 권장 패치가 나열되어 있습니다.

표 1-4 Sun Crypto Accelerator 1000 소프트웨어의 권장 패치

패치 ID	설명
108528-13	`KU-13` (`nvpair` 보안 수정)

2 장

Sun Crypto Accelerator 1000 보드의 설치와 제거

이 장에서는 Sun Crypto Accelerator 1000 하드웨어 및 소프트웨어 설치 방법을 설명합니다.

이 장은 다음 절로 구성되어 있습니다.

보드 사용법

각 보드는 운반 또는 보관 기간 동안 특수 정전기 방지용 봉지에 포장하여 보호합니다. 보드의 정전기에 민감한 부분이 손상되지 않도록 하려면, 보드를 만지기 전에 다음 방법을 사용하여 신체상의 정전기를 감소시킵니다.

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

주의 – 보드의 민감한 부분이 손상되지 않도록 하려면, 보드를 다룰 때 정전기 방지용 손목 띠를 착용하고, 보드를 들 때는 가장자리를 사용하며, 항상 정전기가 없는 곳(예: 포장에 사용된 플라스틱 봉지)에 보관해야 합니다.

보드 설치

Sun Crypto Accelerator 1000 보드보드 설치에는 시스템에 보드를 끼우고 소프트웨어 도구를 로드하는 것이 포함됩니다. 하드웨어 설치 지침에는 보드 설치에 대한 일반적인 단계가 포함됩니다. 특정 설치 지침에 대해서는 시스템과 함께 제공된 설명서를 참고하십시오.

▼ 하드웨어 설치 방법

1. **수퍼유저로 시스템과 함께 제공된 지침에 따라 컴퓨터를 종료하고 전원을 끈 다음, 전원 코드를 뽑고 컴퓨터 덮개를 벗깁니다.**
2. **사용하지 않은 PCI 슬롯(권장 64비트, 66MHz 슬롯)을 장착합니다.**
3. **정전기 방지용 손목 띠를 손목 및 접지된 금속 표면 끝에 부착합니다.**
4. **Phillips 헤드 나사돌리개를 사용하여 PCI 슬롯 덮개에서 나사를 제거합니다.**
   단계 5에서 브래킷을 지탱하도록 나사를 그대로 둡니다.
5. **Sun Crypto Accelerator 1000 보드의 가장자리를 잡고 플라스틱 봉지에서 꺼낸 다음, PCI 슬롯에 삽입하고 후면 브래킷의 나사를 고정시킵니다.**
6. **컴퓨터 덮개를 씌운 다음 전원 코드를 다시 연결하고 시스템 전원을 켭니다.**
7. **ok프롬프트에** `show-devs` **명령을 입력하여 보드가 제대로 설치되었는지 확인합니다.**

```
ok show-devs
. . .
/pci@1f,2000/pci108e,5455@1
/pci@1f,4000/pci108e,5455@5
. . .
```

`/pci@1f,2000/pci108e,5455@`*n* 행은 보드가 설치되고 시스템에서 인식되었음을 표시합니다.

Sun Crypto Accelerator 1000 소프트웨어 설치

Sun Crypto Accelerator 1000 소프트웨어는 *Sun Crypto Accelerator 1000* CD에 포함되어 있습니다. SunSolve 웹 사이트에서 패치를 다운로드해야 할 경우도 있습니다. 더 자세한 정보는 5페이지의 "필요한 패치" 를 참고하십시오.

▼ 소프트웨어 설치 방법

1. **시스템에 연결된 CD-ROM 드라이브에** *Sun Crypto Accelerator 1000* **CD를 삽입하십시오.**
   - 시스템에 Sun Enterprise Volume Manager™가 실행 중일 경우, CD-ROM이 `/cdrom/cdrom0` 디렉토리에 자동으로 설치됩니다.
   - 시스템에 Volume Manager가 실행 중이 아닐 경우, CD-ROM은 다음과 같이 설치됩니다.

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

/cdrom/cdrom0 디렉토리에 다음 파일 및 디렉토리가 표시됩니다.

파일 또는 디렉토리	내용	
Copyright	U.S. 저작권 파일	
FR_Copyright	프랑스 저작권 파일	
Docs	Sun Crypto Accelerator 1000 보드 설치 및 사용자 설명서	
Packages	Sun Crypto Accelerator 1000 소프트웨어 패키지에 다음이 포함됩니다.	
	SUNWcrypr	Cryptography Kernel Components(암호화 커널 구성 요소)
	SUNWcrypu	Cryptographic Administration Utility and Libraries (암호화 관리 유틸리티 및 라이브러리)
	SUNWcrysu	SSL Support for Apache(아파치용 SSL 지원(옵션))
	SUNWcrypm	Cryptographic Administration Manual Pages(암호화 관리 매뉴얼 페이지)
	SUNWdcar	DCA Crypto Accelerator(루트)
	SUNWdcamn	DCA Crypto Accelerator Manual Page(DCA Crypto Accelerator 매뉴얼 페이지)
	SUNWdcav	SunVTS Test of DCA Crypto Accelerator(DCA Crypto Accelerator의 SunVTS 테스트(옵션))
	SUNWcrysl	SSL Development Tools and Libraries for Apache (아파치용 SSL 개발 도구 및 라이브러리 (옵션))

웹 서버로 아파치를 사용하려면 SUNWcrysu 패키지만 설치하십시오.

다른(지원되지 않는) 아파치 웹 서버 버전에 다시 연결하려면 SUNWcrysl 패키지만 설치하십시오.

SunVTS™ 테스트를 수행하려면 SUNWdcav 패키지만 설치하십시오. SUNWdcav 패키지를 설치하려면 SunVTS 4.4, 4.5 또는 4.6이 설치되어 있어야 합니다.

2. 다음을 입력하여 소프트웨어를 설치합니다.

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

3. **소프트웨어가 제대로 설치되었는지 확인하려면** pkginfo **명령을 실행합니다.**

```
# pkginfo SUNWcrypr SUNWcrypu SUNWcrysl SUNWcrysu SUNWcrypm SUNWdcar SUNWdcamn
SUNWdcav
system  SUNWcrypr   Cryptography Kernel Components
system  SUNWcrypu   Cryptographic Administration Utility and Libraries
system  SUNWcrysl   SSL Development Tools and Libraries
system  SUNWcrysu   SSL Support for Apache
system  SUNWcrypm   Cryptographic Administration Manual Pages
system  SUNWdcar    DCA Crypto Accelerator (Root)
system  SUNWdcamn   DCA Crypto Accelerator Manual Page
system  SUNWdcav    SunVTS Test of DCA Crypto Accelerator
```

4. **(옵션) 부착된 드라이버를 확인하려면** prtconf **명령을 실행합니다.**

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

5. **(옵션)** modinfo **명령을 실행하여 로드된 모듈을 봅니다.**

```
# modinfo | grep Crypto
130 1033e946   6df0  79   1  cryptio (Cryptographic IOCTL v1.58)
131 1030240c   2d93   -   1  kcl (Cryptographic Library v1.64)
132 10313ac8   131e   -   1  kcpi (Crypto Provider Interface v1.27)
135 103178be   8684  82   1  dca (PCI Crypto Accelerator v1.156)
```

실제로 Sun Crypto Accelerator 1000을 사용하여 암호화 작업을 수행할 때까지 kcl 및 cryptio가 로드되지 않거나 나타나지 않을 수 있습니다.

디렉토리 및 파일

표 2-1에는 Sun Crypto Accelerator 1000 소프트웨어 설치 시 기본값으로 생성되는 디렉토리가 표시되어 있습니다.

표 2-1 Sun Crypto Accelerator 1000디렉토리

디렉토리	내용
/etc/opt/SUNWconn/crypto/realms	영역 및 사용자 데이터
/opt/SUNWconn/crypto/bin	응용 프로그램 실행 파일
/opt/SUNWconn/crypto/lib	응용 프로그램 라이브러리
/opt/SUNWconn/crypto/sbin	정적으로 연결된 실행 파일

그림 2-1에는 디렉토리 및 파일의 계층 구조를 보여줍니다.

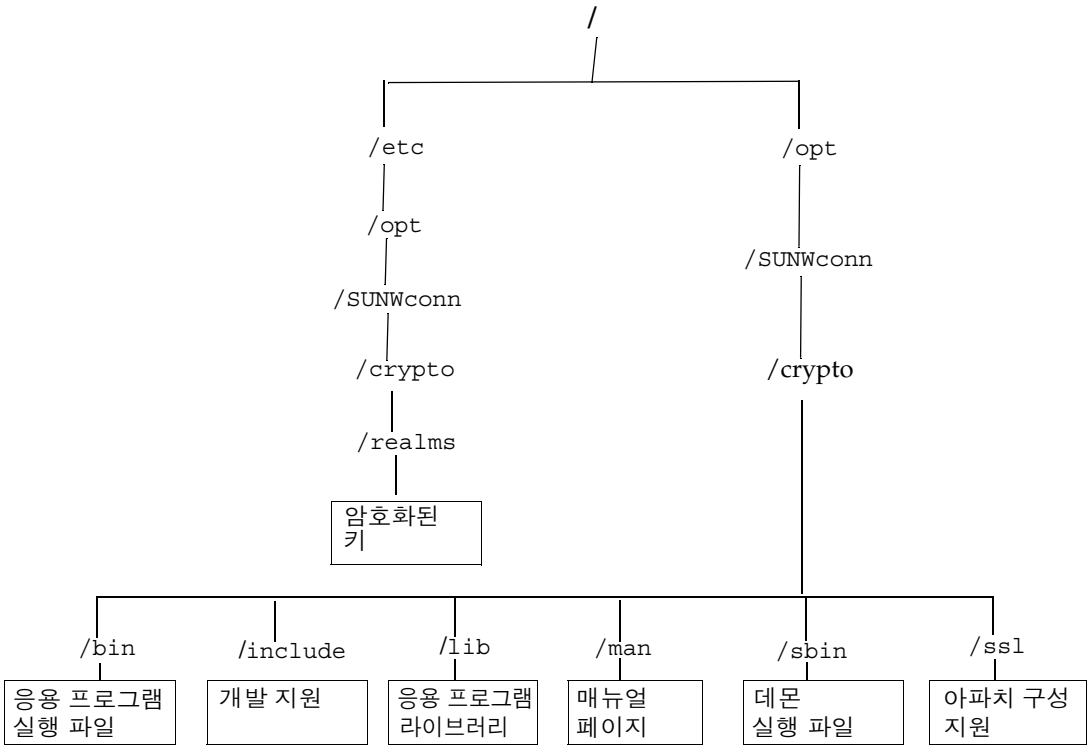


그림 2-1 Sun Crypto Accelerator 1000 디렉토리 및 파일

소프트웨어 제거

영역을 생성했으면 소프트웨어를 제거하기 전에 반드시 영역을 삭제해야 합니다. 영역을 생성하지 않았으면 다음 절차는 무시해도 됩니다. 현재 사용 중인 영역은 삭제할 수 없습니다. 영역에 대한 참조를 해제하려면 웹 서버 및/또는 관리 서버를 종료해야 합니다.

주의 – Sun Crypto Accelerator 1000 소프트웨어를 제거하기 전에 Sun Crypto Accelerator 1000 보드와 함께 사용할 목적으로 활성화한 모든 웹 서버를 반드시 비활성화해야 합니다. 그렇게 하지 않을 경우, 해당 웹 서버의 기능이 작동되지 않습니다.

▼ 영역 삭제 방법

1. **수퍼유저로** `secadm` **유틸리티에 엑세스합니다.**

```
# /opt/SUNWconn/crypto/bin/secadm
secadm>
```

2. `secadm` **유틸리티를 사용하여 각 영역을 삭제합니다.**

```
secadm> delete realm=realm-name
Delete realm realm-name? [Y/N]: Y
System Administrator Login Required
Login: root
Password:
Realm realm-name deleted successfully.
```

키 관련 자료를 포함한 모든 사이트의 특정 영역 데이터를 제거합니다.

▼ 소프트웨어 제거 방법

- **수퍼유저로 `pkgrm` 명령을 사용하여 설치된 소프트웨어 패키지만 제거합니다.**

  설치된 패키지는 반드시 아래에 표시된 순서대로 제거해야 합니다. 그렇게 하지 않을 경우, 종속 경고가 발생하고 커널 모듈이 로드된 채로 남아있을 수 있습니다.

  패키지를 모두 설치한 경우에는 다음 방법으로 제거합니다.

```
# pkgrm SUNWcrysl SUNWdcav SUNWdcar SUNWcrysu SUNWcrypu SUNWcrypr
SUNWdcamn SUNWcrypm
```

주 – SunVTS Test of DCA Crypto Accelerator(DCA Crypto Accelerator의 SunVTS 테스트)(`SUNWdcav`)를 설치 또는 제거한 후, SunVTS가 실행 중이면 SunVTS로 시스템을 다시 검색하여 사용 가능한 테스트를 업데이트합니다. 자세한 정보는 SunVTS 문서를 참고하십시오.

---

3 장

iPlanet 웹 서버에 대한 보드 사용

이 장에서는 iPlanet 웹 서버용 Sun Crypto Accelerator 1000 보드 사용 방법에 대해 설명합니다.

이 장은 다음 절으로 구성되어 있습니다.

암호

iPlanet 웹 서버(iWS)를 작동하는 과정에서 여러 암호를 입력하도록 요청을 받게 됩니다. 표 3-1에는 각 암호에 대한 설명이 나와 있습니다. 이러한 암호는 장 전체에서 언급됩니다. 암호 사용에 혼동이 있으면 표 3-1을 참고하십시오.

표 3-1 iPlanet 웹 서버에 필요한 암호

암호 유형	설명
iWS 관리 서버	iPlanet 관리 서버를 시작하는 데 필요합니다. 이 암호는 iPlanet을 설치하는 동안 할당됩니다.
Web 서버 트러스트 데이터베이스	안전 모드로 실행할 경우, 인증서가 요청될 경우, 인증서를 설치할 경우에 내부 암호화 모듈을 시작하는 데 필요합니다. 이 암호는 iPlanet 웹 서버에서 키 쌍 파일 암호 및 모듈의 내부 암호가 될 수 있습니다.
시스템 관리	`secadm` 권한을 부여받은 작업 수행 시 필요합니다. UNIX 호스트 암호입니다.
user@realm-name	안전 모드로 실행 시 Sun Crypto Accelator 1000 모듈을 시작하는 데 필요합니다. `secadm` 을 사용하는 영역에 대해 사용자 작성 시 할당됩니다.

영역 작성 및 배치

iPlanet 웹 서버용으로 보드를 사용할 수 있도록 하기 전에 우선 영역을 설정하고 배치해야 합니다. 그렇게 하지 않은 경우는 하나 이상의 영역 및 사용자를 설정해야 합니다. 영역에 대한 자세산 정보는 부록 A를 참고하십시오.

▼ 영역 작성 및 배치 방법

1. **영역을 설정하고 배치하려면 다음 예와 같이 Sun Crypto Accelerator 1000 도구 디렉토리를 검색 경로에 위치시킵니다.**

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

2. `secadm` **유틸리티에 액세스합니다.**

```
$ secadm
```

3. secadm 유틸리티를 사용하여 새 영역을 만듭니다.

```
secadm> create realm=realm-name
System Administrator Login Required
Login: root
Password:
Realm realm-name created successfully.
```

4. 영역에 사용자를 배치합니다.

이 사용자 이름은 Sun Crypto Accelerator 1000의 도메인 내에서만 알려져 있으며, 웹 서버 프로세스 실행에 사용되는 UNIX 사용자 이름과 동일할 필요는 없습니다. 사용자를 작성하기 전에 현재 작동 중인 영역을 설정한 다음 시스템 관리자로 로그인해야 합니다.

사용자를 작성하기 전에 사용자를 작성할 영역을 먼저 설정해야 합니다.

```
secadm> set realm=realm-name
secadm{realm-name}> su
System Administrator Login Required
Login: root
Password:
secadm{root@realm-name}#
```

a. 하나의 영역사용자만 필요할 경우, "nobody"라는 사용자 이름을 사용하면 설정을 하지 않아도 됩니다. 자세한 정보는 57페이지의 "슬롯 파일"을 참조하십시오.

```
secadm{root@realm-name}# create user=nobody
Initial password:
Confirm password:
User nobody created successfully.
```

웹 서버를 시작하는 동안 사용자 인증에 반드시 이 암호를 사용해야 합니다. 암호는 *user@realm-name*입니다.

주의 – 입력한 암호는 반드시 기억해야 합니다. 암호가 없으면 액세스할 수 없습니다. 잊어버린 암호는 검색할 수 없습니다.

5. secadm을 종료합니다.

```
secadm> exit
```

iPlanet 웹 서버의 작동 개요

iPlanet 웹 서버를 작동하려면 다음 두 장에 설명되어 있는 절차를 완료해야 합니다.

1. iPlanet 서버 설치
2. 트러스트 데이터베이스 작성
3. 인증서 요청
4. 인증서 설치
5. iPlanet 웹 서버 구성

주의 – 상기 절차는 반드시 순서대로 수행되어야 합니다. 그렇게 하지 않으면 구성이 잘못될 수 있습니다.

- iPlanet 웹 서버 4.1을 사용하는 경우는 4장을 보십시오.
- iPlanet 웹 서버 6.0을 사용하는 경우는 5장을 보십시오.

4 장

iPlanet 웹 서버 4.1 설치 및 구성

이 장에서는 iPlanet 웹 서버 4.1을 설치하고 구성하는 방법에 대해 설명합니다.

이 장은 다음 절로 구성되어 있습니다.

iPlanet 웹 서버 4.1 설치

다음 절은 iPlanet 웹 서버 4.1의 설치 방법에 대해 설명합니다. 반드시 나열된 순서대로 절차를 수행해야 합니다. iPlanet 웹 서버 사용에 대한 자세한 정보는 iPlanet 웹 서버 문서를 참고하십시오.

▼ iPlanet 웹 서버 4.1 설치 방법

1. **iPlanet 웹 서버 4.1 소프트웨어 설치**

   웹 서버 소프트웨어는 다음 URL에 있습니다.

   `http://www.iplanet.com`

2. **웹 서버 설치**

   지침이 하나의 예제에 대한 것이므로 웹 서버를 다르게 구성할 수도 있습니다. 서버에 대한 기본 경로 이름은 다음과 같습니다. `/usr/netscape/server4`

   iPlanet 웹 서버가 설치되는 동안 기본 경로를 허용합니다. 이 설명서에는 기본 경로가 사용됩니다. 다른 위치에 웹 서버를 설치하려면 설치한 위치를 기록해 두십시오.

3. **설치 프로그램을 실행합니다.**

4. **설치 스크립트에서 프롬프트에 응답합니다.**

   다음 프롬프트 이외에는 편리상 기본값을 허용할 수 있습니다.

   a. `yes`**를 입력하여 라이센스 조건에 동의합니다.**

   b. 정식 *hostname.domain***을 입력합니다.**

   c. iWS 관리 서버 암호를 두 번 입력합니다.

   d. 프롬프트가 나오면 Return(돌아가기)을 누릅니다.

▼ 트러스트 데이터베이스 작성

1. **관리 서버를 시작합니다.**

   - iPlanet 웹 서버를 시작하려면 설정 요청으로 `startconsole`를 실행하는 대신에 다음 명령을 사용합니다.

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

   응답 메시지에는 서버를 관리하기 위해 연결할 URL이 제공됩니다.

2. **웹 브라우저를 열고 다음을 입력하여 iPlanet 관리 서버를 시작합니다.**

```
http://hostname.domain:admin_port
```

   팝업 창이 뜨고 사용자 ID 및 암호를 물어봅니다. 설치하는 동한 선택한 iWS 관리 서버의 사용자 이름 및 암호를 입력합니다.

주 – iPlanet 웹 서버를 설치하는 동안 기본 설정을 사용한 경우에는 사용자 ID 또는 iWS 관리 서버 사용자 이름에 `admin`을 입력합니다.

---

3. **OK(확인)를 누릅니다.**

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

   하나 이상의 웹 서버 인스턴스에서 보안을 사용할 수 있습니다. 각 웹 서버 인스턴스에 대해 이 절차를 반복합니다.

주 – 관리 서버에 SSL을 실행하려는 경우에도 트러스트 데이터베이스를 설치하는 절차는 비슷합니다. 자세한 정보는 iPlanet 문서를 참고하십시오.

---

   a. **관리 서버에서 Servers(서버) 탭을 누릅니다.**

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

   c. **페이지의 맨 윗부분에 있는 Security(보안) 탭을 누른 다음 Create Database(데이터베이스 작성) 옵션을 선택합니다.**

   d. **두 개의 대화 상자에 나오는 암호(웹 서버 트러스트 데이터베이스)를 입력하고 OK(확인)를 누릅니다.**

      8개 이상의 문자로 된 암호를 선택합니다. 이 암호는 iPlanet 웹 서버가 안전 모드로 실행될 때 내부 암호화 모듈을 시작하는 데 사용됩니다.

5. **다음 스크립트를 실행하여 Sun Crypto Accelerator 1000 보드를 사용합니다.**

```
# /opt/SUNWconn/crypto/bin/sslconfig
```

   이 스크립트에서 웹 서버를 저장할지 묻습니다. 여기서 iPlanet 웹 서버 또는 아파치 웹 서버에 대한 Sun Crypto Accelerator 1000 암호화 모듈을 설치합니다. 스크립트가 구성 파일을 업데이트하고 Sun Crypto Accelerator 1000 보드를 사용할 수 있습니다.

6. **1을 입력하여 SSL을 사용할 iPlanet 웹 서버를 구성한 다음 Enter를 누릅니다.**

```
Sun Crypto Accelerator Installation
------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for iPlanet Web Server
or Apache.

Please select the type of web server you wish to configure
to use the Sun Crypto Accelerator:
------------------------------------------------------
1. Configure iPlanet Web Server for SSL
2. Configure Apache for SSL
3. Work with iPlanet and Apache keys
Your selection (0 to quit): 1
```

7. 웹 서버 루트 디렉토리의 경로를 입력한 다음 Enter를 입력합니다.

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

8. 계속 진행하려면 y를 입력하고 Enter를 누릅니다.

```
This script will update your iPlanet 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

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


<Press ENTER to continue>
```

9. 0을 입력하여 종료합니다.

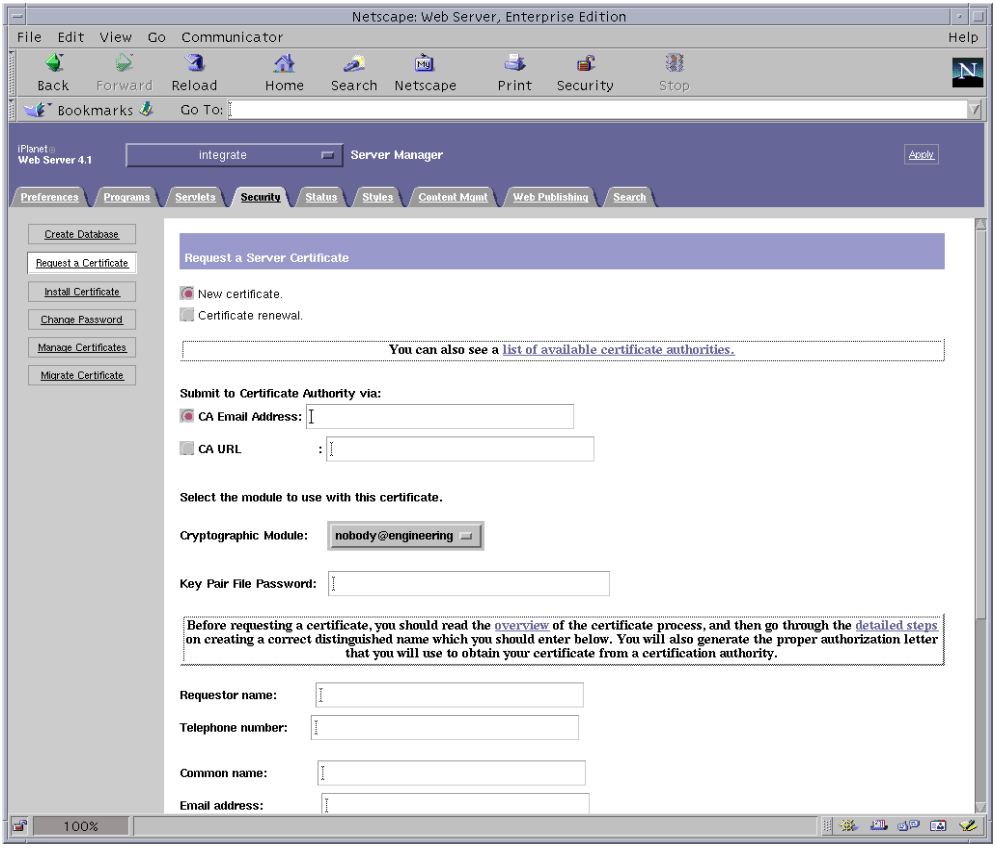
▼ 서버 인증서 작성

1. 다음 명령을 입력하여 관리 서버를 다시 시작합니다.

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

2. 요청하려면 페이지 맨 윗부분에 있는 Security(보안) 탭을 누릅니다.
Create Trust Database(트러스트 데이터베이스 작성) 창이 표시됩니다.

3. **페이지의 왼쪽에 있는 Request Certificate(인증서 요청) 링크를 선택합니다.**



4. **다음 정보를 사용하여 인증서 요청을 작성합니다.**

   a. **새 인증서를 선택합니다.**

      웹으로 가능한 인증 기관 또는 등록 기관에 인증서를 직접 보낼 수 있을 경우, CA URL 옵션을 선택합니다. 그렇지 않을 경우는 CA Email Address(CA 전자 우편 주소)를 선택한 다음 인증서 요청을 받을 전자 메일 주소를 선택합니다.

   b. **사용하려는 암호화 모듈을 선택합니다.**

      풀다운 메뉴의 각 영역은 고유 엔트리를 갖고 있습니다. 올바른 영역을 선택했는지 확인합니다. Sun Crypto Accelerator 1000을 사용하려면 반드시 *user@realm-name* 형식의 모듈을 선택해야 합니다.

   c. **Key Pair File Password(키 쌍 파일 암호) 대화 상자에서 키를 소유할 *user@realm-name*에 대한 암호를 제공합니다.**

d. 다음 필드에 적절한 정보를 제공합니다.

- Requestor Name(요청자 이름): 요청자의 연락 정보
- Telephone Number(전화 번호): 요청자의 연락 정보
- Common Name(공용 이름): 방문자 브라우저에 입력될 웹사이트 도메인 *hostname.domain*
- Email Address(전자 우편 주소): 요청자의 연락 정보
- Organization(소속 기관): 인증서에 표시될 소속 기관 값
- Organizational Unit(소속 기관 단위): (옵션) 인증서에 표시될 소속 기관 단위 값
- Locality(지방): (옵션) 제공될 경우 인증서에 표시될 도시, 국가
- State(주): (옵션) 주 이름(정확한 이름)
- Country(국가): 인증서에 표시될 필수 필드 항목인 알파벳 두 글자로 된 ISO 국가 코드

e. 정보를 모두 입력했으면 OK(확인) 단추를 눌러 전송합니다.

5. 인증 기관을 이용하여 인증서를 작성합니다.

- 인증서를 CA URL에 보내도록 선택하면 인증서 요청이 CA URL에 자동으로 전송됩니다.
- CA Email Address(CA 전자 우편 주소)를 선택하면 헤더와 함께 메일로 받은 인증서 요청을 복사하여 인증 기관에 전송합니다.

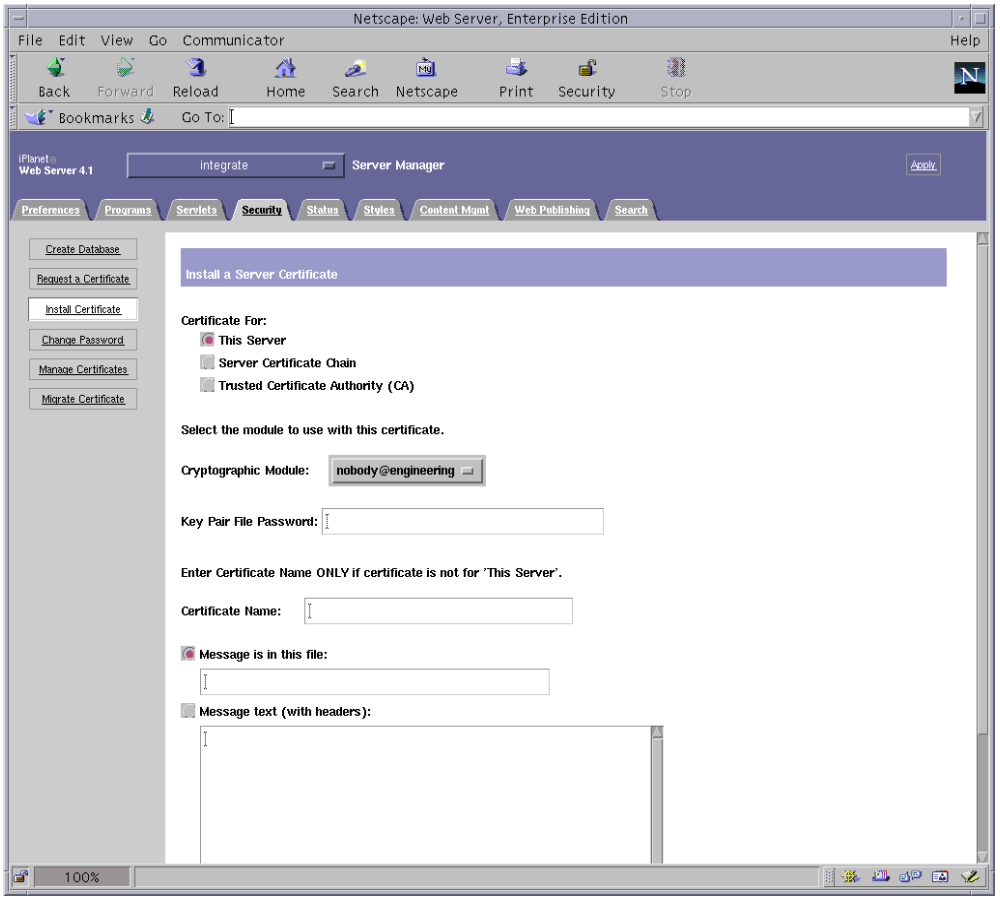
6. 인증서가 작성되면 헤더와 함께 클립보드에 복사합니다.

인증서는 인증서 요청과는 다르며 일반적으로 텍스트 형식으로 제공됩니다.

▼ 서버 인증서 설치 방법

1. **페이지 왼쪽에 있는 Install Certificate(인증서 설치) 링크를 선택합니다.**
   인증 기관의 승인을 받고 인증서가 발급되면 iPlanet 웹 서버에 인증서를 설치합니다.

2. **Security(보안) 탭을 선택한 후 왼쪽 프레임에서 Install Certificate(인증서 설치) 옵션을 선택합니다.**



3. **양식을 작성하여 인증서를 설치합니다.**
   - 인증 대상: 해당 서버
   - 암호화 모듈: 적절한 *user@realm-name*을 선택합니다.
   - 키 쌍 파일 암호: 이전에 작성된 키를 소유하는 *user@realm-name*의 암호를 제공합니다.

- 인증서 이름: 일반적으로 공백으로 둡니다. 이름을 입력하도록 선택한 경우, SSL의 지원으로 실행할 때 웹 서버가 사용하는 이름을 변경하여 인증서와 키에 액세스합니다.

4. **Message text(with headers)(메시지 텍스트(헤더 포함))를 선택한 다음 이전에 복사한 인증서를 붙입니다.**

5. **페이지 하단의 OK(확인) 단추를 눌러 인증 기관으로부터 복사한 인증서를 Message box(메시지 상자)에 붙입니다.**

   인증서에 대한 일부 기본 정보가 표시됩니다.

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

   화면에 서버를 다시 시작하라는 메시지가 표시됩니다. 웹 서버 인스턴스가 완전히 종료 상태였으므로 이 메시지는 꼭 따르지 않아도 됩니다. 또한 웹 서버에 SSL을 사용하려면 웹 서버를구성하라는 메시지가 표시됩니다. 웹 서버를 구성하려면 다음 절차를 따르십시오.

iPlanet 웹 서버 4.1 구성

웹 서버 및 서버 인증서가 설치 완료되었으면 SSL에 대한 웹 서버를 구성해야 합니다.

▼ iPlanet 웹 서버 4.1 구성 방법

1. **메인 관리 페이지에서 작업하려는 웹 서버 인스턴스를 선택한 다음 Manage(관리)를 누릅니다.**

   기본값으로 페이지 맨 위의 Preferences(등록 정보) 탭이 표시됩니다. 그렇지 않은 경우는 Preferences(등록 정보) 탭을 누릅니다.

2. **페이지 맨 위의 Preferences 탭을 누릅니다. 페이지 왼쪽에 있는 Encryption On/Off(암호 설정/해제) 링크를 선택합니다. 암호화를 On(설정)으로 설정합니다.**

   대화 상자의 포트 필드는 기본 SSL 포트 번호 443으로 업데이트됩니다. 필요한 경우 포트 번호를 변경합니다.

3. **OK(확인) 단추를 누릅니다.**

4. **Save(저장) 단추를 눌러 변경 사항을 적용합니다.**

   웹 서버가 보안 모드에서 실행되도록 구성되었습니다.

5. **다음 행을 추가하여** `/usr/netscape/server4/https-`*hostname*`/config/magnus.conf` **파일을 편집합니다.**

```
CERTDefaultNickname user@realm-name:Server-Cert
```

hostname 위치에 웹 서버의 이름이 옵니다.

기본값으로 단계 2 및 단계 3에 작성한 인증서의 이름은 `Server-Cert`가 됩니다. 인증서의 이름이 다를 경우, `Server-Cert`로 변경합니다.

6. **관리하려는 서버를 선택한 다음 페이지의 오른쪽 맨 위의 Apply(적용) 단추를 누릅니다.**

관리 서버를 통해 변경 사항이 적용됩니다.

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

서버가 꺼진 상태에서 Apply Changes(변경 사항 적용) 단추를 누르면 암호를 입력하라는 팝업 창이 표시됩니다. 이 창은 크기 조절이 불가능하며, 변경 사항을 전송하는 데 어려움이 있을 수 있습니다. 이 문제는 다음 두 가지 방법으로 해결할 수 있습니다.

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

8. **웹 서버 페이지에서 페이지 왼쪽에 있는 On/Off(설정/해제) 링크를 선택합니다. 서버에 대한 암호를 입력한 다음 OK(확인) 단추를 누릅니다.**

하나 이상의 암호를 입력하게 됩니다. Module Internal 프롬프트에서 웹 트러스트 데이터베이스에 대한 암호를 제공합니다.

Module *user@realm-name* 프롬프트에서 `secadm`을 사용하여 *realm-name* 에서 *user*를 만들 때 설정한 암호를 입력합니다.

9. **다음 웹 사이트에서 새 SSL 작동 웹 서버를 확인하십시오.**

`https://`*hostname.domain*`:`*server_port*`/`

기본 *server_port* 는 443입니다.

5 장

iPlanet 웹 서버 6.0 설치 및 구성

이 장은 iPlanet 웹 서버 6.0용 Sun Crypto Accelerator 1000 보드 사용 방법을 설명합니다.

이 장은 다음 절로 구성되어 있습니다.

iPlanet 웹 서버 6.0 설치

다음 절은 iPlanet 웹 서버의 설치 및 구성 방법에 대해 설명합니다. 반드시 나열된 순서대로 절차를 수행해야 합니다. iPlanet 웹 서버 사용에 대한 자세한 정보는 iPlanet 웹 서버 문서를 참고하십시오.

▼ iPlanet 웹 서버 6.0 설치 방법

1. **iPlanet 웹 서버 6.0 소프트웨어 설치**

   웹 서버 소프트웨어는 다음 URL에 있습니다.

   `http://www.iplanet.com`

2. **웹 서버 설치**

   지침이 하나의 예제에 대한 것이므로 웹 서버를 다르게 구성할 수도 있습니다. 서버에 대한 기본 경로 이름은 다음과 같습니다. `/usr/iplanet/servers`

   iPlanet 웹 서버가 설치되는 동안 기본 경로를 허용합니다. 이 설명서에는 기본 경로가 사용됩니다. 다른 위치에 웹 서버를 설치하려면 설치한 위치를 기록해 두십시오.

3. **설치 프로그램을 실행합니다.**

4. **설치 스크립트에서 프롬프트에 응답합니다.**

   다음 프롬프트 이외에는 편리상 기본값을 허용할 수 있습니다.

   a. `yes`**를 입력하여 라이센스 조건에 동의합니다.**

   b. 정식 *hostname.domain***을 입력합니다.**

   c. iWS 관리 서버 암호를 두 번 입력합니다.

   d. 프롬프트가 나오면 Return(돌아가기)을 누릅니다.

▼ 트러스트 데이터베이스 작성

1. **관리 서버를 시작합니다.**

   iPlanet 웹 서버를 시작하려면 `setup` 요청으로 `startconsole`를 실행하는 대신에 다음 명령을 사용합니다.

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

   응답 메시지에는 서버를 관리하기 위해 연결할 URL이 제공됩니다.

2. **웹 브라우저를 열고 다음을 입력하여 iPlanet 관리 서버를 시작합니다.**

```
http://hostname.domain:admin_port
```

   팝업 창이 뜨고 사용자 ID 및 암호를 물어봅니다. 설치하는 동한 선택한 iWS 관리 서버의 사용자 이름 및 암호를 입력합니다.

주 – iPlanet 웹 서버를 설치하는 동안 기본 설정을 사용한 경우는 사용자 ID 또는 iWS 관리 서버 사용자 이름에 `admin`을 입력합니다.

---

3. **OK(확인)를 누릅니다.**

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

   하나 이상의 웹 서버 인스턴스에서 보안을 사용할 수 있습니다. 각 웹 서버 인스턴스에 대해 이 절차를 반복합니다.

   주 – 관리 서버에 SSL을 실행하려는 경우에도 트러스트 데이터베이스를 설치하는 절차는 비슷합니다. 자세한 정보는 iPlanet 문서를 참고하십시오.

   ---

   a. **관리 서버에서 Servers(서버) 탭을 누릅니다.**

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

   c. **페이지의 맨 윗부분에 있는 Security(보안) 탭을 누른 다음 Create Database(데이터베이스 작성) 옵션을 선택합니다.**

   d. **두 개의 대화 상자에 나오는 암호(웹 서버 트러스트 데이터베이스)를 입력하고 OK(확인)를 누릅니다.**

      8개 이상의 문자로 된 암호를 선택합니다. 이 암호는 iPlanet 웹 서버가 안전 모드로 실행될 때 내부 암호화 모듈을 시작하는 데 사용됩니다.

5. **다음 스크립트를 실행하여 Sun Crypto Accelerator 1000 보드를 사용합니다.**

```
# /opt/SUNWconn/crypto/bin/sslconfig
```

   이 스크립트에서 웹 서버를 저장할지 묻습니다. 여기서 iPlanet 웹 서버 또는 아파치 웹 서버에 대한 Sun Crypto Accelerator 1000 암호화 모듈을 설치합니다. 스크립트가 구성 파일을 업데이트하고 Sun Crypto Accelerator 1000 보드를 사용할 수 있습니다.

6. 1을 입력하여 SSL을 사용할 iPlanet 웹 서버를 구성한 다음 Enter를 누릅니다.

```
Sun Crypto Accelerator Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for iPlanet Web Server
or Apache.

Please select the type of web server you wish to configure
to use the Sun Crypto Accelerator:
------------------------------------------------------------
1. Configure iPlanet Web Server for SSL
2. Configure Apache for SSL
3. Work with iPlanet and Apache keys
Your selection (0 to quit): 1
```

7. 웹 서버 루트 디렉토리의 경로를 입력한 다음 Enter를 입력합니다.

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

8. 계속 진행하려면 y를 입력하고 Enter를 누릅니다.

```
This script will update your iPlanet 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

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


<Press ENTER to continue>
```

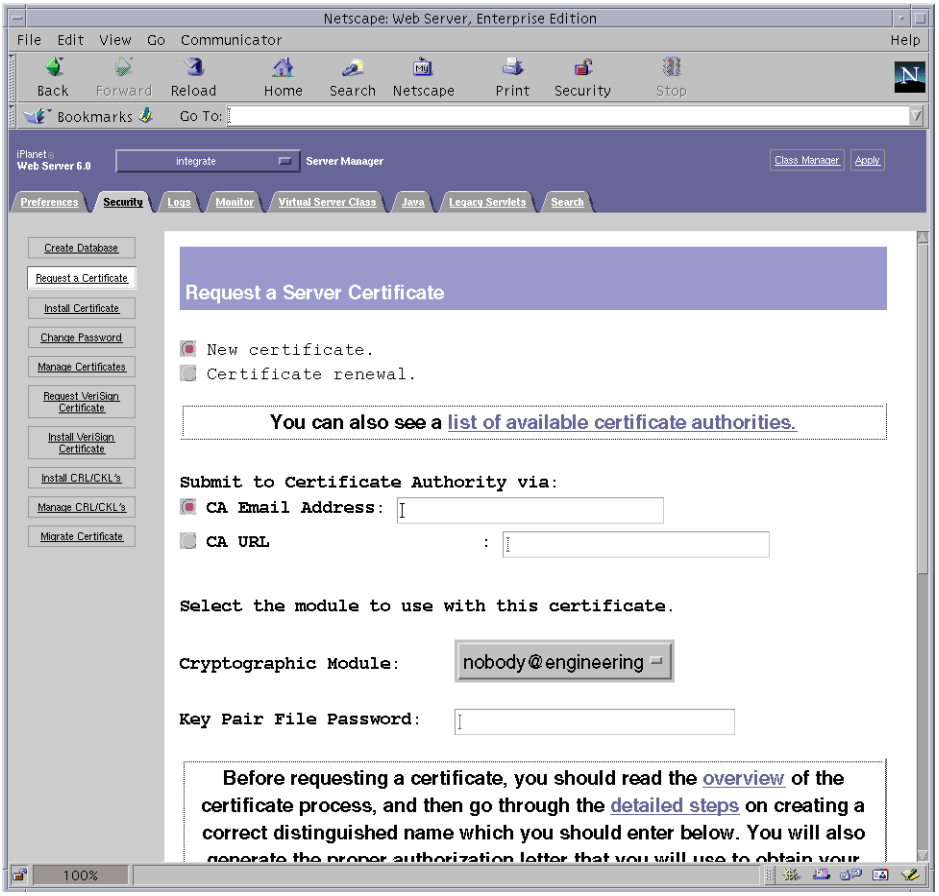
9. 0을 입력하여 종료합니다.

▼ 서버 인증서 작성

1. **다음 명령을 입력하여 관리 서버를 다시 시작합니다.**

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

2. **서버 인증서를 요청하려면 페이지 맨 윗부분에 있는 Security(보안) 탭을 누릅니다.**
   Create Database(데이터베이스 작성) 창이 표시됩니다.
3. **페이지의 왼쪽에 있는 Request Certificate(인증서 요청) 링크를 선택합니다.**



4. 다음 정보를 사용하여 인증서 요청을 작성합니다.

a. 새 인증서를 선택합니다.

웹으로 가능한 인증 기관 또는 등록 기관에 인증서를 직접 보낼 수 있는 경우, CA URL 옵션을 선택합니다. 그렇지 않을 경우는 CA Email AddressCA(전자 우편 주소)를 선택한 다음 인증서 요청을 받을 전자 메일 주소를 선택합니다.

b. 사용하려는 암호화 모듈을 선택합니다.

풀다운 메뉴의 각 영역은 고유 엔트리를 갖고 있습니다. 올바른 영역을 선택했는지 확인합니다. Sun Crypto Accelerator 1000을 사용하려면 *user@realm-name* 형식으로 모듈을 선택해야 합니다.

c. Key Pair File Password(키 쌍 파일 암호) 대화 상자에서 키를 소유할 *user@realm-name*에 대한 암호를 제공합니다.

d. 다음 필드에 적절한 정보를 제공합니다.

- Requestor Name(요청자 이름): 요청자의 연락 정보
- Telephone Number(전화 번호): 요청자의 연락 정보
- Common Name(공용 이름): 방문자 브라우저에 입력될 웹사이트 도메인 *hostname.domain*
- Email Address(전자 우편 주소): 요청자의 연락 정보
- Organization(소속 기관): 인증서에 표시될 소속 기관 값
- Organizational Unit(소속 기관 단위): (옵션) 인증서에 표시될 소속 기관 단위 값
- Locality(지방): (옵션) 제공될 경우 인증서에 표시될 도시, 국가
- State(주): (옵션) 주 이름(정확한 이름)
- Country(국가): 인증서에 표시될 필수 필드 항목인 알파벳 두 글자로 된 ISO 국가 코드

e. 정보를 모두 입력했으면 OK(확인) 단추를 눌러 전송합니다.

5. 인증 기관을 이용하여 인증서를 작성합니다.

- 인증서를 CA URL에 보내도록 선택하면 인증서 요청이 CA URL에 자동으로 전송됩니다.
- CA Email AddressCA(전자 우편 주소)를 선택하면 헤더와 함께 메일로 받은 인증서 요청을 복사하여 인증 기관에 전송합니다.

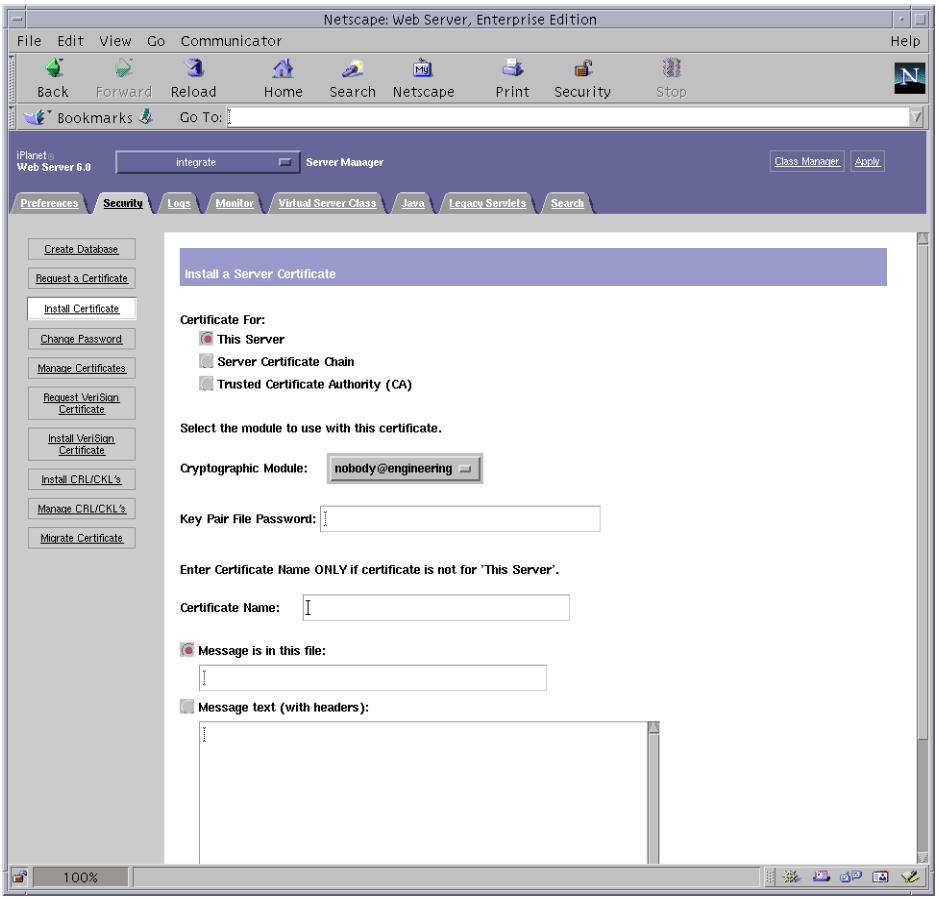
6. 인증서가 작성되면 헤더와 함께 클립보드에 복사합니다.

인증서는 인증서 요청과는 다르며 일반적으로 텍스트 형식으로 제공됩니다.

▼ 서버 인증서 설치 방법

1. **페이지 왼쪽에 있는 Install Certificate(인증서 설치) 링크를 선택합니다.**
   인증 기관의 승인을 받고 인증서가 발급되면 iPlanet 웹 서버에 인증서를 설치합니다.

2. **Security(보안) 탭을 선택한 후 왼쪽 프레임에서 Install Certificate(인증서 설치) 옵션을 선택합니다.**



3. **양식을 작성하여 인증서를 설치합니다.**
   - 인증 대상: 해당 서버
   - 암호화 모듈: 적절한 *user@realm-name*을 선택합니다.
   - 키 쌍 파일 암호: 이전에 작성된 키를 소유하는 *user@realm-name*의 암호를 제공합니다.

- 인증서 이름: 일반적으로 공백으로 둡니다. 이름을 입력하도록 선택한 경우, SSL의 지원으로 실행할 때 웹 서버가 사용하는 이름을 변경하여 인증서와 키에 액세스합니다.

4. **Message text(with headers)(메시지 텍스트(헤더 포함))를 선택한 다음 이전에 복사한 인증서를 붙입니다.**

5. **페이지 하단의 OK(확인) 단추를 눌러 인증 기관으로부터 복사한 인증서를 Message box(메시지 상자)에 붙입니다.**

   인증서에 대한 일부 기본 정보가 표시됩니다.

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

   화면에 서버를 다시 시작하라는 메시지가 표시됩니다. 웹 서버 인스턴스가 완전히 종료 상태였으므로 이 메시지는 꼭 따르지 않아도 됩니다. 또한 웹 서버에 SSL을 사용하려면 웹 서버를구성하라는 메시지가 표시됩니다. 웹 서버를 구성하려면 다음 절차를 따르십시오.

iPlanet 웹 서버 6.0 구성

웹 서버 및 서버 인증서가 설치 완료되었으면 SSL에 대한 웹 서버를 구성해야 합니다.

▼ iPlanet 웹 서버 6.0 구성 방법

1. **페이지 맨 위의 Preferences(등록 정보) 탭을 누릅니다. 왼쪽 프레임에 있는 Edit Listen Sockets(수신 대기 소켓 편집) 옵션을 선택합니다.**

   메인 프레임은 웹 서버 인스턴스에 대해 설정된 모든 수신 대기 소켓을 나열합니다.

   a. **다음 필드를 수정합니다.**
      - Port(포트): SSL 작동 웹 서버를 실행할 포트로 설정합니다(일반적으로 443 포트).
      - Security(보안): On(설정)으로 설정합니다.

   b. **OK(확인) 단추를 눌러 변경 사항을 적용합니다.**

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

2. **Attributes(속성) 링크를 누릅니다.**

3. ***user@realm-name* 암호를 입력하여 시스템에서 *user@realm-name*에 대한 인증을 받습니다.**

4. **팝업 창에서 SSL settings(SSL 설정)를 선택합니다.**

   Cipher Default settings(암호 기본값 설정), SSL2 또는 SSL3/TLS를 선택합니다. Default(기본값)를 선택해도 기본 설정이 표시되지 않습니다. 다른 2개의 선택에서 사용하려는 알고리즘을 선택합니다.

5. **`:Server-Cert`(다를 경우는 선택한 이름) 다음에 나오는 *user@realm-name*에 대한 인증서를 선택합니다.**

   적합한 *user@realm-name*이 소유한 키만 Certificate Name(인증서 이름) 필드에 나타납니다.

6. **인증서를 선택하고 보안 설정을 모두 확인했으면 OK(확인) 버튼을 클릭합니다.**

7. **오른쪽 맨 위 모서리에 있는 Apply(적용) 링크를 눌러 서버를 시작하기 전에 변경 사항을 적용합니다.**

8. **Load Configuration Files(구성 파일 로드) 링크를 눌러 변경 사항을 적용합니다.**

   웹 서버 인스턴스를 시작할 수 는 페이지로 다시 돌아갑니다.

   서버가 꺼진 상태에서 Apply Changes(변경 사항 적용) 단추를 누르면 암호를 입력하라는 팝업 창이 표시됩니다. 이 창은 크기 조절이 불가능하며, 변경 사항을 전송하는 데 어려움이 있을 수 있습니다.

   이 문제는 다음 두 가지 방법으로 해결할 수 있습니다.

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

9. **대화 상자에서 요청받은 암호를 제공하고 서버를 시작합니다.**

   하나 이상의 암호를 입력하게 됩니다. Module Internal 프롬프트에서 웹 트러스트 데이터베이스에 대한 암호를 제공합니다.

   Module *user@realm-name* 프롬프트에서 `secadm`을 사용하여 *realm-name* 에서 *user*를 만들 때 설정한 암호를 입력합니다.

10. **다음 웹 사이트에서 새 SSL 작동 웹 서버를 확인하십시오.**

    `https://`*hostname.domain*`:`*server_port*`/`

    기본 *server_port* 는 443입니다.

6 장

아파치 웹 서버 작동

이 장은 아파치 웹 서버용 Sun Crypto Accelerator 1000 보드 사용 방법에 대해 설명합니다.

이 장은 다음 절로 구성되어 있습니다.

아파치 웹 서버 작동

아파치 웹 서버 1.3.12는 Solaris 8 7/01 운영 환경과 함께 제공됩니다. 다음은 아파치 웹 서버의 특정 릴리스에 대한 지침입니다. 아파치 웹 서버 사용에 대한 자세한 정보는 아파치 웹 서버 문서를 참고하십시오.

▼ 아파치 웹 서버 작동 방법

1. `httpd` **구성 파일 작성**

Solaris 시스템에서 `httpd.conf-example` 파일은 일반적으로 `/etc/apache` 경로 안에 있습니다. 이 파일을 템플릿으로 사용하고 다음 방법으로 복사할 수 있습니다.

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

파일의 `ServerName` 위치에 서버 이름을 입력합니다.

2. sslconfig를 시작합니다.

```
# /opt/SUNWconn/crypto/bin/sslconfig
```

3. 2를 선택하여 SSL을 사용할 아파치 웹 서버를 구성합니다.

```
Sun Crypto Accelerator Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for iPlanet Web Server
or Apache.

Please select the type of web server you wish to configure
to use the Sun Crypto Accelerator:
------------------------------------------------------------
1. Configure iPlanet Web Server for SSL
2. Configure Apache for SSL
3. Work with iPlanet and Apache keys

Your selection (0 to quit):
```

4. 아파치 바이너리가 존재하는 디렉토리를 제공합니다.

Solaris 시스템에서 일반적으로 /usr/apache가 사용됩니다.

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

5. 아파치의 구성 파일의 위치를 제공합니다.

Solaris 시스템에서 일반적으로 /etc/apache가 사용됩니다.

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

6. 작성합니다.

작성하지 않도록 선택할 경우, 나중에 뒤로 이동하여 sslconfig를 사용하여 키를 작성합니다.

```
Do you wish to create a new RSA keypair and certificate request?
[Y/N]:
```

No에 응답한 경우에는 44페이지의 "인증서 작성 방법"으로 건너뜁니다.

7. 키를 저장할 디렉토리를 제공합니다.

이 디렉토리가 존재하지 않을 경우에는 새로 작성됩니다.

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

8. 키 요소에 대한 기본 이름을 선택합니다.

이 이름에는 키 파일, 인증서 요청 파일, 그리고 이후에 인증서 파일과 서로 구별되도록 다른 접미사가 추가됩니다.

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

9. 키의 길이는 512 비트에서 2,048 비트 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
Generating RSA private key, 1024 bit long modulus
..........++++++
......++++++
e is 65537 (0x10001)
```

10. PEM 패스 문구 작성.

이 패스 문구는 키를 보호하기 위한 것입니다. 강력하지만 기억할 수 있는 패스 문구를 선택해야 합니다. 암호를 잊어 버리면 키에 액세스할 수 없습니다.

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

주의 – 입력한 패스 문구는 반드시 기억해야 합니다. 패스 문구가 없으면 키에 액세스할 수 없습니다. 잊어버린 패스 문구를 검색할 방법이 없습니다.

인증서 작성

다음 절차는 Sun Crypto Accelerator 1000 보드와 함께 아파치 웹 서버를 작동하는 데 필요한 인증서 작성 방법에 대해 설명합니다.

▼ 인증서 작성 방법

1. 작성 완료한 키를 사용하여 인증서 요청을 작성합니다.

키에 액세스하려면 먼저 암호를 입력해야 합니다. 그런 다음 아래 필드에 적합한 정보를 입력합니다.

- Country Name(국가 이름): 인증서에 표시될 필수 필드 항목인 알파벳 두 글자로 된 ISO 국가 코드
- State or Province Name(주/도 이름): (옵션) 정확한 주 또는 도 이름(또는 .을 입력하고 Return을 누릅니다)
- Locality(지방): (옵션) 제공할 경우 인증서에 표시될 도시, 국가
- Organizational Name(소속 기관 이름): 인증서에 증명될 소속기관 정보
- Organizational Unit Name(소속 기관 단위 이름): (옵션) 인증서에 표시될 소속 기관 단위 개체의 값
- SSL Server Name(SSL 서버 이름): 방문자 브라우저에 입력된 웹 사이트 도메인
- 전자 우편 주소: 요청자의 연락 정보

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

2. `/etc/apache/httpd.conf` **파일을 지침에 따라 수정합니다.**

키 및 인증서 파일에 대한 정보가 표시됩니다. 또한 Sun Crypto Accelerator 1000과 함께 사용하기 위한 `/etc/apache/httpd.conf` 파일의 수정 방법에 대한 지침이 표시되어 있습니다.

```
The keyfile is stored in /etc/apache/keys/ap6-key.pem.
The certificate request is in /etc/apache/keys/ap6-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.1.3.12

In the AddModule section, add the following:

AddModule mod_ssl.c
```

3. VirtualHost**를 설정하지 않도록 선택한 경우,** SSLEngine**,** SSLCertificateFile **및** SSLCertificateKeyFile **지시문이** SSLPassPhraseDialog **지시문 바로 위의** httpd.conf **파일에 위치합니다.**

```
You may need a virtual host directive similar to
what is shown below:

<VirtualHost _default_:443>
        SSLEngine on
        SSLCertificateFile /etc/apache/keys/ap6-cert.pem
        SSLCertificateKeyFile /etc/apache/keys/ap6-key.pem
</VirtualHost>

You must add the following line after all of your VirtualHost
definitions:

SSLPassPhraseDialog exec:/opt/SUNWconn/crypto/bin/sslpassword

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>
```

단계 6의 질문에 아니오라고 대답한 경우, 나중에 키 요소 작성에 대한 추가 정보를 받게 됩니다.

```
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 iPlanet and Apache keys" from the
sslconfig main menu.
```

4. sslconfig**이 완료되면** 0**을 선택하여 종료합니다.**

5. /etc/apache/keys/*base_name*-certreq.pem**(base_name이 단계 8에서 설정됨)에서 헤더와 함께 인증서 요청을 복사한 다음 인증 기관으로 전송합니다.**

6. **인증서가 작성되면 인증서 파일** `/etc/apache/keys/`*base_name*`-cert.pem`**을 만들어 인증서를 붙여넣습니다.**

7. **아파치 웹 서버를 시작합니다.**

   아파치 바이너리 위치를 `/usr/apache/bin`라고 가정합니다. 바이너리 디렉토리가 잘못된 경우에는 올바른 디렉토리를 입력합니다.

```
# /usr/apache/bin/apachectl start
```

8. **프롬프트가 나오면 PEM 패스 문구를 입력합니다.**

9. **다음 웹 사이트에서 새 SSL 작동 웹 서버를 확인하십시오.**

   `https://`*server_name*`:`*server_port*`/`

   기본 *server_port* 는 443입니다.

7 장

진단 및 문제 해결

이 장에서는 Sun Crypto Accelerator 1000 소프트웨어에 대한 진단 테스트 및 문제 해결에 대해 설명합니다. 이 장은 다음 절로 구성되어 있습니다.

SunVTS 진단 소프트웨어

Sun Crypto Accelerator 1000 CD의 `SUNWdcav` 패키지에 포함된 SunVTS 테스트 `dcatest`는 Solaris Supplement CD의 `SUNWvts` 및 `SUNWvtsx` 패키지에 포함된 주요 SunVTS 테스트 컨트롤 및 사용자 인터페이스와 함께 작동하여 Sun Crypto Accelerator 1000 보드에 대한 진단을 제공합니다.

이 진단 테스트를 실행 및 모니터링하는 방법에 대한 지침은 SunVTS 문서를 참고하십시오. 이 문서는 시스템에 Solaris를 설치하기 위해 Solaris Supplement CD에 제공되는 Solaris on Sun Hardware AnswerBook에서 사용할 수 있습니다.

주 – SunVTS는 Solaris Supplement CD에서 SunVTS 패키지를 설치한 경우에만 사용하실 수 있습니다.

▼ dcatest 실행 방법

1. **수퍼유저로 SunVTS를 시작합니다.**

```
# /opt/SUNWvts/bin/sunvts
```

   SunVTS 시작에 대한 자세한 지침은 *SunVTS User's Guide*를 참고하십시오.

   다음은 CDE 사용자 인터페이스를 사용하여 SunVTS를 시작한 가정 하의 지침입니다.

2. **SunVTS Diagnostic(SunVTS 진단) 기본 창에서 System Map(시스템 맵)을 Logical 모드로 설정합니다.**

3. **체크란을 해제하여 모든 테스트를 비활성화합니다.**

4. **OtherDevices의 체크란을 선택한 다음 OtherDevices의 플러스란을 선택하여 OtherDevices 그룹의 모든 테스트를 표시합니다.**

5. **dcatest의 이름이 지정되지 않은 OtherDevices 그룹에서 체크란을 해제합니다.**

   - dcatest가 표시될 경우, 단계 6으로 이동하십시오.
   - dcatest가 표시되지 않을 경우, Commands(명령)드롭다운 메뉴에서 Reprobe system(시스템 검색)을 선택하여 시스템을 검색하여 dcatest를 찾습니다.

   정확한 절차는 SunVTS 문서를 참고하십시오. 검색이 완료되고 dcatest가 표시되면, 단계 6을 계속합니다.

6. **dcatest 인스턴스 중 하나를 누른 다음 마우스 오른쪽으로 누르고 끌어서 Test Parameter(테스트 매개 변수) 옵션을 표시합니다.**

   dcatest에만 관련되는 이 옵션은 51페이지의 "dcatest에 대한 테스트 매개 변수 옵션"에 설명되어 있습니다.

7. **선택을 모두 완료하면 Within Instance Apply(인스턴스 내에서 적용)를 눌러 선택한 dcatest 인스턴스를 변경하거나 Across All Instances Apply(인스턴스 전체 적용)를 눌러 체크 표시한 모든 dcatest 인스턴스를 변경합니다.**

   팝업 창이 제거되고 Sun Diagnostic(Sun 진단) 기본 창으로 돌아옵니다.

8. **dcatest 인스턴스 중 하나를 누른 다음 마우스 오른쪽으로 누르고 끌어서 Test Execution Options(테스트 실행 옵션)를 표시합니다.**

   Test Execution Options(테스트 실행 옵션)를 표시하는 다른 방법으로 Options(옵션) 팝업을 누른 다음 Test Executions(테스트 실행)를 누릅니다. 이 옵션은 모든 테스트에 영향을 주는 일반적인 SunVTS 컨트롤입니다. 자세한 정보는 SunVTS 문서를 참고하십시오.

9. **선택이 완료되면 Apply(적용)를 눌러 팝업 창을 제거하고 Sun Diagnostic(Sun 진단) 기본 창으로 돌아옵니다.**

10. **Start(시작)를 눌러 선택한 테스트를 실행합니다.**

11. Stop(중지)을 눌러 모든 테스트를 중지합니다.

dcatest에 대한 테스트 매개 변수 옵션

표 7-1 에서는 50페이지의 "dcatest 실행 방법"의 단계 6에 자세히 설명된 dcatest에 대한 테스트 매개 변수 옵션을 표시합니다. 테스트할 보드 유형은 팝업 창의 Configuration(구성) 영역에 표시됩니다.

표 7-1 dcatest에 대한 테스트 매개 변수 옵션

옵션 레이블	설명
Test_Sel	실행할 하위 테스트의 조합을 지정할 10진수 값 값을 0으로 하면 모든 테스트가 선택됩니다. 각 하위 테스트는 두 자리 수로 할당됩니다. 하위 테스트에 할당된 숫자를 입력하여 개별 하위 테스트를 선택할 수 있습니다. 여러 하위 테스트는 필요한 하위 테스트에 할당된 숫자의 합계를 입력하여 선택할 수 있습니다. 기본 설정은 0입니다.
Info_Print	정보(INFO 유형) 메시지의 출력을 활성화 또는 비활성화합니다. 기본 설정은 0입니다.

표 7-2 dcatest 하위 테스트에 대해 설명합니다.

표 7-2 dcatest 하위 테스트

테스트 이름	번호	설명
ALL	0	테스트 실행이 완료되었습니다.
SHOWINFO	1	테스트 정보 아래에 프로바이더 및 장치를 표시하고 INFO 유형 메시지를 출력합니다.
3DES	2	3DES Bulk Encryption(3DES 대용량 암호)을 테스트합니다.
RSA	4	RSA Public and Private Keys(RSA 공용 및 개인 키)를 테스트합니다.
DSA	32	DSA Signature Verification(DSA 서명 인증)을 테스트합니다.
Random	64	Random(임의) 및 Pseudo-Random Number Generation(무작위 번호 생성)을 테스트합니다. 생성된 번호를 표시하고 INFO 유형 메시지를 출력합니다.

하위 테스트에 의해 생성된 메시지는 SunVTS Diagnostic(SunVTS 진단) 기본 창의 Test Messages(테스트 메시지) 영역에 표시됩니다. 하위 테스트에 의해 생성된 메시지를 다음과 같이 유형별로 그룹화합니다.

- Test Parameters(테스트 매개 변수) 팝업에서 Info_Print 옵션이 활성화되어 있을 경우, INFO 유형 메시지가 Test Message(테스트 메시지) 영역에 출력되고 Information Log(정보 로그)에 기록됩니다. INFO 유형의 메시지는 비중요 메시지를 제공합니다.
- FATAL 오류 유형 메시지가 항상 표시되고 Test Error Log(테스트 오류 로그) 및 Information Log(정보 로그)에 기록됩니다.
- 하위 테스트를 통해 경과를 추적하는 VERBOSE 유형 메시지는 VERBOSE 옵션이 Test Execution(테스트 실행) 팝업 창에서 활성화된 경우에만 선택할 수 있습니다. VERBOSE 메시지는 로그 파일에 기록되지 않습니다.

  `dcatest` FATAL 오류 메시지를 표시하고 기록하는 테스트의 조용한 모드는 VERBOSE 및 `Info_Print` 옵션을 비활성화하여 선택할 수 있습니다.

dcatest 명령행 구문

CDE 환경 대신 명령행에서 `dcatest`를 실행하도록 선택할 경우, 모든 인수가 명령행 문자열에 지정되어야 합니다.

32비트 모드에서 `dcatest` 경로는 `/opt/SUNWvts/bin/`입니다. 64비트 모드에서 `dcatest` 경로는 `/opt/SUNWvts/bin/sparcv9/`입니다.

다음 예제는 32비트 모드 명령에 대한 구문을 표시합니다.

```
/opt/SUNWvts/bin/dcatest -f [Standard Command-Line Arguments]
[-o [dev=dcan][,testsel=n][,infodis]]
```

표준 명령행 인수의 정의는 *SunVTS 테스트 참조 설명서* 을 참조하십시오. `dcatest`가 Functional Mode(기능 모드) 테스트이므로 `-f`가 포함되어야 합니다. 메시지 사용을 표시하려면 `-u`를, VERBOSE 메시지를 표시하려면 `-v`를 포함합니다. 위의 대괄호에 포함된 항목은 옵션 엔트리를 나타냅니다. 표 7-3에 설명된 바와 같이 옵션을 생략하면 해당 옵션에 대한 기본 동작이 만들어 집니다.

표 7-3 `dcatest` 명령행 구문

인수	설명
`dev=dcan`	테스트에 장치의 인스턴스를 dca0 또는 dca2로 지정합니다. 포함되지 않을 경우는 기본값이 dca0으로 설정됩니다.
`testsel=n`	n이 0과 127 사이의 값이 될 수 있을 때 하위 테스트가 실행되도록 지정합니다. 포함되지 않을 경우는 기본값이 zero로 설정됩니다.
`infodis`	INFO 유형 메시지가 비활성화될 경우 포함. 포함되지 않을 경우에는 기본값이 Info_Print Enabled로 설정됩니다.

Sun Crypto Accelerator 1000 문제 해결

Sun Crypto Accelerator 1000 장치가 시스템에 나열되어 있는지 결정하려면 OpenBoot PROM(OBP) 프롬프트에서 `show-devs`를 입력하여 장치 목록을 표시합니다. 장치 목록의 Sun Crypto Accelerator 1000 보드에 관련된 아래 예제와 유사한 행을 참조해야 합니다.

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

위의 예제에서 `pci108e,5455`는 Sun Crypto Accelerator 1000 보드의 장치 경로를 식별합니다. 이 보드에는 펌웨어가 없으므로 OBP 수준의 진단을 사용할 수 없습니다.

Sun Crypto Accelerator 1000은 보드에서 암호화 작업을 반영하는 신호 또는 표시기를 포함하지 않습니다. 암호화 작업 요청이 보드에서 실제로 수행되고 있는지를 결정하려면 `kstat`(1M) 명령을 사용하여 장치 사용을 표시합니다.

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

module: dca                             instance: 0
name:   dca0                        class:    misc
    3desbytes                       3040
    3desjobs                        5
    crtime                          65.342725895
    dsasign                         0
    dsaverify                       0
    rngbytes                        10592
    rngjobs                         187
    rngsha1bytes                    16328
    rngsha1jobs                     327
    rsaprivate                      9
    rsapublic                       0
    snaptime                        106956.467004482
```

kstat 정보를 표시하여 암호화 요청 또는 "작업"이 Sun Crypto Accelerator 1000 보드에 전송되고 있는지 나타냅니다. 시간 경과에 따른 "작업" 값의 변경은 보드가 Sun Crypto Accelerator 1000 보드에 전송된 암호화 작업 요청을 가속화하고 있음을 의미합니다. 암호화 작업 요청이 보드로 전송되지 않을 경우, 웹 서버의 각 특정 구성별로 웹 서버 구성을 확인하십시오.

암호화 요청이 수행된 위치를 항상 결정할 수 있는 것은 아니며, 요청 신청 시 하위 시스템의 로딩에 따라 암호화 요청이 다른 위치에서 수행될 수 있습니다.

kstat(1M)가 반환하는 커널/드라이버 정적 값은 해석하지 마십시오. 이 값은 드라이버 내에 남아 필드 지원을 도와줍니다. 의미 및 실제 이름은 시간에 따라 변경됩니다.

부록 **A**

iPlanet 웹 서버에서 Sun Crypto Accelerator 1000 보드 관리

이 부록은 iPlanet 웹 서버에서 관리할 경우 Sun Crypto Accelerator 1000 보드의 보안 기능에 대한 개요를 제공합니다.

주 – 영역을 관리하려면 시스템의 시스템 관리자 계정에 대한 액세스가 있어야 합니다.

이 부록은 다음 절로 구성되어 있습니다.

개념 및 용어

iPlanet 웹 서버와 같은 PKCS#11 인터페이스를 통해 Sun Crypto Accelerator 1000과 통신하는 응용 프로그램에 대한 영역 및 사용자를 작성해야 합니다.

Sun Crypto Accelerator 1000 컨텍스트 내의 사용자는 암호 키 요소에 대한 고유 소유자입니다. 각 사용자는 다수의 키를 소유할 수 있습니다. 사용자는 각기 다른 구성을 지원하기 위해 다수의 키를 소유하려 하거나(예: "production" 키 및 "development" 키(사용자의 각기 다른 소속 기관을 반영하도록)), 고 가용성(HA) 구성을 용이하게 하기 위해 다수의 키를 필요로 할 수 있습니다. "사용자" 또는 "사용자 계정"이라는 용어는 Sun Crypto Accelerator 1000 사용자를 의미하며 일반 UNIX 사용자 계정을 의미하지 않습니다. UNIX 사용자 이름 및 Sun Crypto Accelerator 1000 사용자 이름 사이에 고정된 매핑이 없습니다.

영역은 사용자 및 키 요소의 논리적 분할을 의미합니다. 영역은 다수의 사용자를 포함할 수 있는 능력을 제공합니다. 영역으로 사용자를 분할하면 각 영역에 대한 고유의 이름 공간을 유지하여 영역 내용을 독립적으로 관리할 수 있습니다.

일반적인 설치에서는 단일 사용자를 가진 단일 영역이 작성됩니다. 예를 들어, "nobody"라는 단일 사용자를 가진 "webserver"라는 단일 영역이 구성됩니다. 여기서 사용자 "nobody"는 단일 영역 내의 서버 키에 대한 액세스 컨트롤을 소유하고 유지할 수 있습니다.

사용자 및 키 요소를 분할하도록 추가 영역을 만들 수 있습니다. "finance", "legal", "engineering"의 예와 같이 더 복잡하게 구성할 수 있습니다. 각 영역은 고유의 이름 공간을 유지합니다. 예를 들면, finance 영역의 사용자인 "webserv"와 engineering 영역의 사용자인 "webserv"는 각각 다른 사용자 계정입니다.

관리 도구인 `secadm`은 Sun Crypto Accelerator 1000의 영역 및 사용자 관리에 사용됩니다.

영역, 사용자 및 iPlanet 웹 서버

iPlanet 웹 서버가 Sun Crypto Accelerator 1000이 관리하는 키를 참조할 경우에는 "토큰 이름"을 사용하여 키 관리가 내부 소프트웨어 데이터베이스가 아닌 하드웨어에 의해 관리됨을 나타냅니다.

Sun Crypto Accelerator 1000은 사용자 계정 및 영역 이름을 "@" 기호와 결합하여 토큰 이름을 만듭니다. 앞에서 예로 든 바와 같이 일반적인 설치에서 "nobody"라는 단일 사용자와 함께 "webserver"라는 단일 영역이 작성되었습니다. iPlanet 웹 서버가 "webserver" 영역의 사용자인 "nobody"가 소유한 키를 참조하기 위해 사용하는 토큰 레이블은 "nobody@webserver"입니다. 사용자 "nobody"의 암호(`secadm`으로 사용자를 작성할 때 설정됨)는 인증서 요청 시, 인증서 설치 시 또는 iPlanet 웹 서버 시작을 위한 인증 시 사용됩니다.

토큰 및 슬롯 파일

iPlanet 웹 서버는 토큰(슬롯이라고도 함)을 통해 키 요소에 액세스합니다. 슬롯 파일은 Sun Crypto Accelerator 1000 관리자가 특정 토큰을 선택적으로 해당 응용 프로그램에 제공할 수 있는 기술입니다.

슬롯 파일이 존재하지 않을 경우는 Sun Crypto Accelerator 1000 소프트웨어가 iPlanet 웹 서버에 토큰을 기본 설정으로 제공합니다. 이 경우에 토큰은 `nobody@`*`realm-name`*이라는 이름으로 각 영역에 제공됩니다.

예제

engineering, finance, legal로 이루어진 세 개의 영역이 있습니다. 다음 토큰이 iPlanet 웹 서버에 제공됩니다.

- nobody@engineering
- nobody@finance
- nobody@legal

상기 이름을 모두 사용하려면 사용자 "nobody"가 각 영역에 존재해야 합니다.

슬롯 파일

기본 설정을 무시하려면 슬롯 파일이 필요합니다. 슬롯 파일은 각 행별로 하나 이상의 토큰 이름을 포함한 텍스트 파일입니다. iPlanet 웹 서버는 이 파일에 나열된 토큰만 제공합니다. 슬롯 파일을 지정하는 방법은 다음과 같습니다(서열순).

1. `$HOME/.SUNWconn_crypto_slots` 파일

   이 파일이 iPlanet 웹 서버가 실행하는 UNIX 사용자의 홈 디렉토리 내에 존재해야 합니다. iPlanet 웹 서버는 홈 디렉토리를 갖고 있지 않는 UNIX 사용자로도 실행이 가능하며 그럴 경우 이러한 접근은 불가능합니다.

2. `/etc/opt/SUNWconn/crypto/slots` 파일

   `/etc/opt/SUNWconn/crypto/slots` 파일은 글로벌 파일로 `.SUNWconn_crypto_slots` 파일이 사용자 홈 디렉토리에 존재하지 않을 경우에 사용됩니다.

다음은 슬롯 파일 내용에 대한 예제입니다.

```
webserv@engineering
webserv@finance
```

상기 파일이 존재하지 않을 경우는 56페이지의 "토큰 및 슬롯 파일"에 설명된 기본 방법을 사용합니다.

토큰 이름에 대한 정보는 iPlanet 웹 서버 구성에 관련된 3장을 참고하십시오.

secadm 사용

secadm 프로그램은 Sun Crypto Accelerator 1000에 명령행 인터페이스를 제공합니다.

secadm 프로그램에 쉽게 액세스하려면 검색 경로 내에 다음 예제와 같이 Sun Crypto Accelerator 1000 도구 디렉토리를 넣습니다.

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

secadm 명령 구문은 다음과 같습니다.

secadm [-h]

secadm [-y] [-f *filename*]

secadm [-y] [-r *realm-name*] [-u *username* | -s *admin-name*] *command*

명령이 /opt/SUNWconn/crypto/bin/ 디렉토리에 위치합니다.

표 A-1은 secadm 도구에 대한 옵션을 표시합니다.

표 A-1 secadm 옵션

옵션	의미
-h	secadm에 대한 명령어 도움말을 표시하고 종료합니다.
-f *filename*	*filename*에서 하나 이상의 명령어를 읽어오고 종료합니다.
-r *realm-name*	단일 명령 모드에서만 사용됩니다. -r 옵션은 secadm이 *realm-name* 영역 내에서 제공된 명령어를 실행하도록 지시합니다.
-s *admin-name*	단일 명령 모드에서만 사용됩니다. -s 옵션은 secadm이 로그인 이름으로 *admin-name*을 사용하여 시스템 관리자로 로그인하도록 지시합니다. *admin-name*은 UID 0 UNIX 사용자(예: root)여야 합니다. 제공된 명령어가 실행되기 전에 로그인됩니다.
-u *username*	단일 명령 모드에서만 사용됩니다. -u 옵션은 secadm이 *username*으로 로그인하도록 지시합니다. 제공된 명령어가 실행되기 전에 로그인됩니다.
-y	일반적으로 확인을 묻는 프롬프트를 표시하는 명령에 모두 "yes"로 대답하도록 강제 설정합니다.

작동 모드

secadm은 다음 세 가지 모드에서 실행될 수 있습니다. 이 모드는 명령어가 secadm에 전달되는 방법에 따라 다릅니다. 세 가지 모드는 단일 명령 모드, 파일 모드 및 대화형 모드입니다. 각 모드마다 서로 다른 암호가 필요합니다.

단일 명령 모드

단일 명령 모드에서 사용자는 명령행 스위치가 모두 지정되면 secadm이 실행할 명령을 지정합니다. 예를 들어 다음 명령은 존재하는 모든 영역을 표시하고 사용자를 명령 쉘 프롬프트로 되돌립니다.

```
$ secadm show realm
```

다음 명령으로 시스템 관리자로 로그인한 다음 engineering 영역 내에서 webserv 사용자를 작성합니다.

```
$ secadm -r engineering -s root create user=webserv
Password:
Initial password:
Confirm password:
User webserv created successfully.
```

"Initial password:" 및 "Confirm password:" 프롬프트에 입력된 암호는 새로 작성된 사용자 암호를 필요로 하는 반면 "Password:" 프롬프트에 입력된 암호는 시스템 관리자 암호를 필요로 합니다.

단일 명령 모드의 모든 출력이 표준 출력 스트림으로 이동합니다. 이 출력은 표준 UNIX 쉘 기반 메서드를 사용하여 다시 보낼 수 있습니다.

파일 모드

파일 모드에서 사용자는 secadm이 하나 이상의 명령을 읽어올 파일을 지정합니다. 파일은 각 행마다 하나의 명령으로 구성된 ASCII 코드의 텍스트여야 합니다. 각 주석은 "#" 문자로 시작합니다. 파일 모드 옵션이 설정되면 secadm은 최종 옵션 이후의 모든 명령행 인수를 무시합니다. 다음 예제는 deluser.scr에 있는 명령을 실행하고 모든 프롬프트에 긍정적으로 응답합니다.

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

대화형 모드

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

secadm로 명령어 입력

secadm 프로그램은 Sun Crypto Accelerator 1000 보드와 상호 작용하는 데 사용할 명령 언어를 갖고 있습니다. 명령어는 단어의 전체 또는 일부(기타 가능성 없이 유일할 경우)를 사용하여 입력합니다. "show" 대신 "sh"는 사용할 수 있지만 "lo"의 경우는 "login" 또는 "logout"이 될 수 있으므로 의미가 모호합니다.

다음은 전체 단어를 사용하여 명령어를 입력하는 예제입니다.

```
secadm{root@engineering}# show user
User                                          Status
------------------------------------------------------
webserv                                       enabled
alice                                         enabled
bob                                           enabled
------------------------------------------------------
```

sh, us와 같이 단어의 일부를 명령어로 사용해도 동일한 정보를 얻을 수 있습니다.

모호한 명령을 입력하면 다음과 같이 설명 메시지가 표시됩니다.

```
secadm{root@engineering}# lo
Ambiguous command: lo
```

secadm를 사용한 인증

사용자 계정 및 키를 다루는 다수의 명령어는 시스템 관리자 또는 사용자로서 인증하도록 요청합니다. 시스템 관리자는 영역 작성, 사용자 계정 작성, 사용자 계정의 활성화 및 비활성화, 그리고 영역 및 사용자 계정의 삭제와 같은 동작을 수행하도록 Sun Crypto Accelerator 1000에 인증해야 합니다. 사용자로서의 인증은 암호를 변경하거나 해당 사용자가 소유한 키 객체를 나열하기 위해 반드시 필요합니다. 표 A-2에는 시스템 관리자 및 사용자가 사용할 수 있는 명령이 표시되어 있습니다.

표 A-2 명령어 행렬

명령어	인증	인증서 보유	인증된 사용자
`create user=`*username*	아니오	예	시스템 관리자
`create realm=`*realm-name*	예	아니오	시스템 관리자
`delete user=`*username*	아니오	예	시스템 관리자
`delete realm=`*realm-name*	예	아니오	시스템 관리자
`disable user=`*username*	아니오	예	시스템 관리자
`enable user=`*username*	아니오	예	시스템 관리자
`exit`	아니오	아니오	모두
`login`	예	아니오	사용자
`logout`	아니오	아니오	모두
`passwd`	예	예	사용자
`set realm=`*realm-name*	아니오	아니오	모두
`show class`	아니오	아니오	모두
`show key`	아니오	예	사용자
`show realm`	아니오	아니오	모두
`show user`	아니오	예	시스템 관리자
`su`	예	아니오	시스템 관리자
`quit`	아니오	아니오	모두
`unset realm`	아니오	아니오	모두

시스템 관리자로서 인증하려면 UID 0(예: root)인 UNIX 사용자 이름을 제공한 다음 프롬프트에서 암호를 입력해야 합니다. 사용자는 사용자 작성 시 설정한 암호가 필요합니다. 시스템 관리자 또는 사용자로 로그인할 때 영역을 가장 먼저 선택해야 합니다.

사용자로 로그인하려면 다음을 입력하십시오.

```
secadm{realm-name}> login user=username
```

시스템 관리자로 로그인하려면 다음을 입력하십시오.

```
secadm{realm-name}> su
```

사용자 또는 시스템 관리자로 로그인하면 secadm 프롬프트에 현재 로그인 중인 사용자가 표시됩니다. 사용자 로그인과 시스템 관리자 로그인은 프롬프트에서 마지막 문자에 의해 구별됩니다. 시스템 관리자에게는 샤프(#)가 표시되고 사용자에게는 꺾쇠 괄호(>)가 표시됩니다. 사용자 또는 시스템 관리자로 로그인한 다음 다른 사용자 또는 시스템 관리자로 로그인할 경우, 아래 예제에서와 같이 새 로그인이 완료될 때 현재 인증서는 상실됩니다.

```
secadm> set realm=engineering
secadm{engineering}> login user=webserv
Password:
secadm{webserv@engineering}> su
System Administration Login Required
Login: root
Password:
secadm{root@engineering}# logout
secadm{engineering}>
```

명령어에 대한 도움말 보기

secadm에는 기본 제공 도움말 기능이 포함되어 있습니다. 도움말을 보려면 도움말이 필요한 명령어 옆에 "?" 문자를 입력합니다. 전체 명령어가 입력되고 행에 "?"가 있을 경우, 아래 예제와 같이 명령어에 대한 구문이 표시됩니다.

```
secadm> create ?
Usage: create {user=<username> | realm=<realm-name>}

secadm> show ?
Sub-Command                     Description
-----------------------------------------------------
class                           Show all realm classes
key                             Show all key objects in a realm
realm                           Show all realms
user                            Show all system accounts
```

"?"를 입력하면 아래 예제와 같이 유효한 명령어 단어 목록이 표시됩니다.

```
secadm> ?
Sub-Command                     Description
-----------------------------------------------------
create                          Create users and accounts
delete                          Delete users and accounts
disable                         Disable a user
enable                          Enable a user
exit                            Exit secadm
login                           Login as a user
logout                          Logout current session
passwd                          Change password for a user
set                             Set current working realm
show                            Show system settings
su                              Authenticate as the System Administrator
quit                            Exit secadm
unset                           Unset secadm operating parameters
```

명령행 모드에서 도움말을 보려는 경우, 일부 경우에서 "?" 문자가 작업 중인 쉘에 의해 해석될 수 있습니다. 이 경우에는 물음표 앞의 명령어 쉘 이스케이프 문자를 사용합니다.

secadm 프로그램 종료

다음 두 명령어를 사용하여 secadm을 종료할 수 있습니다. quit 및 exit. CTRL-D 키를 눌러도 secadm이 종료됩니다.

영역 설치 및 관리

영역은 키 요소에 대한 리포지터리입니다. 관리자 및 사용자와 서로 연결되어 있습니다. 영역은 저장소를 제공할 뿐만 아니라 사용자 계정이 키 객체를 소유하도록 하는 수단을 제공합니다. 이로 인해 소유자로 인증되지 않은 응용 프로그램에서 키를 숨길 수 있습니다. 영역은 다음 두 구성 요소로 이루어져 있습니다.

- 키 객체: iPlanet 웹 서버와 같은 응용 프로그램을 위해 저장되는 장기적 키입니다.
- 사용자 계정: 이 계정은 응용 프로그램이 특정 키를 인증하고 액세스하는 수단을 제공합니다.

하나의 영역을 필요로 하지만 다수의 영역이 존재할 때, 각 영역은 고유의 사용자 계정 집합을 갖습니다. 예를 들어 응용 프로그램이 사용자로 webserv를 인증하고 영역 내에서 키에 액세스하려 할 경우, 사용자 계정 webserv는 해당 영역 내에 존재해야 합니다.

영역 작성

영역을 작성하면 장기적 키 객체를 저장하는 데 필요한 디렉토리, 파일 및 기타 자원이 작성됩니다. 영역를 작성하려면 관리자는create realm 명령을 사용하여 작성될 영역의 이름을 제공해야 합니다. 현재 보유한 인증서에 상관 없이 시스템 관리자는 해당 명령이 성공적으로 완료되도록 인증해야 합니다. 암호를 묻는 프롬프트에서 UNIX 시스템 관리자 암호를 입력합니다. 예:

```
secadm> create realm=engineering
System Administrator Login Required
Login: root
Password:
Realm engineering successfully created.
```

사용 용도에 맞게 영역 이름을 정할 수 있습니다. 금융(finance) 또는 공학(engineering)과 같은 다른 분야에 대한 영역를 설치하려면 영역 이름을 finance 및 engineering으로 정합니다. 예:

```
secadm> create realm=finance
System Administrator Login Required
Login: root
Password:
Realm finance successfully created
```

현재 작업 중인 영역 설정

secadm은 하나의 영역에서 키 및 사용자 계정을 한 번만 관리할 수 있습니다. 영역 및 사용자 계정을 다루는 대부분의 명령어는 영역을 먼저 선택하도록 요청합니다. 영역을 선택하려면 다음 예제와 같이 set realm 명령어를 실행합니다.

```
secadm> set realm=finance
secadm{finance}>
```

영역을 선택하면 secadm 프롬프트에 영역 이름이 중괄호({ }) 안에 표시됩니다.

작업하던 영역에서 더 이상 작업하지 않으려면 현재 작업 영역을 새 값으로 설정하거나 영역을 설정 해제합니다. 현재 작업 중인 영역을 변경 또는 설정 해제하면 해당 영역에서 인증받은 사용자 또는 시스템 관리자는 자동으로 로그아웃됩니다. 예:

```
secadm{finance}> set realm=engineering
secadm{engineering}> unset realm
secadm>
```

영역에 사용자 배치

이 사용자 이름은 Sun Crypto Accelerator 1000의 도메인 내에서만 알려져 있으며 웹 서버가 프로세스를 실제로 실행할 UNIX 사용자 이름과 동일할 필요는 없습니다. 사용자를 작성하려 하기 전에 먼저 올바른 영역을 선택하고 시스템 관리자로 로그인해야 합니다. 예:

```
secadm> set realm=engineering
secadm{engineering}> su
System Administrator Login Required
Login: root
Password:
secadm{root@engineering}#
```

영역 사용자가 하나만 필요할 경우, 영역 이름을 "nobody"로 사용하여 슬롯 파일을 설정하지 않을 수 있습니다. 다음 예제에서는 "engineering" 영역에서 사용자 "nobody"를 작성하고 표 3-1에서 *user@realm-name*로 정의된 "nobody@engineering"에 대한 암호를 설정합니다.

```
secadm{root@engineering}# create user=nobody
Initial password:
Confirm password:
User nobody successfully created.
```

웹 서버가 시작되는 동안 인증할 때 상기 암호를 사용해야 합니다.

주의 – 입력한 암호는 반드시 기억해야 합니다. 암호가 없으면 키에 액세스할 수 없습니다. 잊어버린 암호는 검색할 수 없습니다.

영역 나열

show realm=*realm-name* 명령을 입력하여 영역에 대한 정보를 나열할 수 있습니다.

```
secadm> show realm
Realm Name
-------------------------------------------------------
engineering
finance
-------------------------------------------------------
```

영역 클래스 나열

영역 클래스는 영역의 키 객체, 사용자 계정 및 인증 데이터에 대한 관리 방법을 제어하는 키 관리 모듈입니다. 현재 Sun Crypto Accelerator 1000이 지원하는 유일한 영역 클래스가 SUNW_filesys 영역 클래스입니다. 지원되는 영역 클래스를 모두 나열하려면 show class 명령을 사용합니다.

```
secadm> show class
Realm Class
-----------------------------------------------------
SUNW_filesys
-----------------------------------------------------
```

영역 삭제

delete realm 명령을 입력하고 제거할 영역 이름을 제공하여 영역을 삭제할 수 있습니다. 위 명령을 실행하면 secadm 프롬프트에 영역을 제거할지 묻는 yes/no 메시지가 표시됩니다. 영역의 작성되면 시스템 관리자는 해당 명령이 실행되기 전에 반드시 인증해야 합니다. 사용 중인 영역은 삭제할 수 없습니다. 영역에 대한 참조를 해제하려면 웹 서버 및/또는 관리 서버를 종료해야 할 수도 있습니다.

사용자 계정 설정과 관리

사용자 계정은 응용 프로그램이 Sun Crypto Accelerator 1000을 인증하는 방법 및 영역 내에서 키를 분리하는 수단을 제공합니다. 하나의 사용자 계정이 소유한 키는 인증되지 않았거나 다른 사용자로 해당 영역에 인증된 응용 프로그램에 액세스할 수 없습니다. 이러한 모든 명령에 대해 영역을 선택해야 하고 시스템 관리자는 secadm su 명령을 사용하여 해당 영역에 로그인해야 합니다.

사용자 생성

- `create user` **명령을 실행하여 사용자를 작성합니다.**

  이 명령에는 `create user=`*username* 형식의 사용자 이름이 필요합니다.

```
secadm{root@engineering}# create user=username
Initial password:
Confirm password:
User username created successfully.
```

주의 – 입력한 암호는 반드시 기억해야 합니다. 암호가 없으면 키에 액세스할 수 없습니다. 잊어버린 암호는 검색할 수 없습니다.

사용자 나열

시스템 관리자만 영역 내의 사용자를 나열할 수 있습니다. 시스템 관리자는 `show user` 명령을 실행해야 합니다. 이 명령은 현재 선택한 영역의 사용자만 나열합니다.

- `show user` **명령을 실행합니다.**

```
secadm{root@engineering}# show user
User                                        Status
-----------------------------------------------------------
webserv                                     enabled
alice                                       enabled
bob                                         enabled
-----------------------------------------------------------
```

사용자 암호 변경

`secadm login` 명령을 사용하여 로그인한 개인 로그인 사용자만 사용자 암호를 변경할 수 있습니다. 새 암호를 설정하기 전에 반드시 현재 암호를 알아야 합니다.

- passwd **명령을 실행합니다.**

```
secadm{username@realm-name}> passwd
Enter current password:
Enter Password:
Confirm Password:
Password successfully changed for user username.
```

주의 – 입력한 암호는 반드시 기억해야 합니다. 암호가 없으면 키에 액세스할 수 없습니다. 잊어버린 암호는 검색할 수 없습니다.

사용자 활성화 또는 비활성화

시스템 관리자만 사용자를 활성화 또는 비활성화할 수 있습니다. 기본값으로 각 사용자는 활성화 상태로 작성됩니다.

- **사용자 계정을 비활성화하려면** disable user=*username* **명령을 입력합니다.**

```
secadm{root@engineering}# disable user=username
User is now disabled.
```

비활성화된 사용자 계정에 대한 인증은 모두 실패하게 됩니다. 어떠한 방법으로도 키를 수정할 수 없습니다. 계정을 다시 활성화하면 해당 사용자가 소유한 키에 인증된 응용 프로그램으로 다시 액세스할 수 있습니다.

- **계정을 활성화하려면** enable user=*username* **명령을 입력합니다.**

```
secadm{root@engineering}# enable user=username
User is now enabled.
```

사용자 삭제

- **삭제할 사용자를 지정하여** `delete user` **명령을 실행합니다.**

  시스템 관리자는 삭제할 사용자 계정 이름을 제공해야 합니다.

  사용자에 관련된 키는 명령이 실행될 때 삭제됩니다. 사용자를 삭제하기 전에 `secadm` 프롬프트에 시스템 관리자에게 yes/no 확인을 묻는 메시지가 표시됩니다.

```
secadm{root@engineering}# delete user=username
Delete user webserv? [Y/N]: y
User username deleted successfully.
```

부록 **B**

매뉴얼 페이지

이 부록에는 Sun Crypto Accelerator 1000 소프트웨어에 포함된 man 페이지에 대한 설명을 제공합니다.

다음 명령어를 사용하여 man 페이지를 볼 수 있습니다.

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

표 B-1에서 사용 가능한 man 페이지를 열거하고 설명합니다.

표 B-1 Sun Crypto Accelerator 1000의 man 페이지

man 페이지	설명
cryptio(7d)	cryptio 장치 드라이버는 내재된 하드웨어 암호화 가속기에 액세스 컨트롤을 제공합니다. cryptio 드라이버는 제공된 서비스에 액세스하기 위해 응용 프로그램 및 커널 클라이언트에 대한 계층화된 소프트웨어 표시를 필요로 합니다.
dca(7d)	dca 장치 장치 드라이버는 내재된 하드웨어 암호화 가속기에 액세스 컨트롤을 제공하는 리프 드라이버입니다. dca 드라이버는 제공된 서비스에 액세스하기 위해 응용 프로그램 및 커널 클라이언트에 대한 계층화된 소프트웨어 표시를 필요로 합니다.
kcl(7d)	kcl 장치 드라이버는 Sun 암호화 프로바이더 드라이버를 지원하는 대량의 스레드를 갖춘 로드 가능 커널 모듈입니다. kcl 드라이버는 제공된 서비스에 액세스하기 위해 응용 프로그램 및 커널 클라이언트에 대한 계층화된 소프트웨어 표시를 필요로 합니다.
kcpi(7d)	kcpi 장치 드라이버는 Sun 암호화 프로바이더 드라이버를 지원하는 대량의 스레드를 갖춘 로드 가능 커널 모듈입니다. kcpi 드라이버는 제공된 서비스에 액세스하기 위해 응용 프로그램 및 커널 클라이언트에 대한 계층화된 소프트웨어 표시를 필요로 합니다.

표 B-1 Sun Crypto Accelerator 1000의 man 페이지

man 페이지	설명
secadm(1m)	secadm은 Sun Crypto Accelerator에 대한 관리 유틸리티입니다. secadm 명령은 Sun Crypto Accelerator와 관련된 구성, 계정 및 키 데이터베이스를 수동으로 관리하는 데 사용됩니다. secadm은 민감한 암호화 키 정보를 처리합니다.
secd(1m)	secd 데몬은 secadm 응용 프로그램에 관리 액세스 서비스를 제공합니다.
sslconfig(1m)	sslconfig는 Sun Crypto Accelerator 1000에 대한 구성 유틸리티입니다.

부록 **C**

아파치 웹 서버에 대한 SSL 구성 지시어

이 부록은 Sun Crypto Accelerator 1000 소프트웨어와 함께 사용할 아파치 웹 서버의 SSL 지원 구성에 대한 지시어를 나열합니다. `http.conf` 파일에서 지시어 구성에 대한 자세한 정보는 아파치 문서를 참고하십시오.

1. `SSLPassPhraseDialog exec:`*program*

   컨텍스트: global

   이 지시어는 키 파일을 수집하려면 특정 *program*을 수행해야 한다는 정보를 아파치 웹 서버에 제공합니다. *program*은 수집된 암호를 표준 결과로 출력합니다.

   다수의 키 파일이 표시되고 공통 암호가 있을 경우, *program*은 한 번만 실행됩니다(각 수집된 암호는 *program*을 다시 실행하기 전에 시도함).

   *program*은 *servername*:*port*의 형식(예: `www.fictional-company.com:443`)으로 2개의 인수로 실행되며, 첫 번째 인수는 서버 이름입니다(443 포트는 전형적인 SSL 기반 웹 서버용 포트). 두 번째 인수는 키 파일에서의 키 유형(*keytype*)을 나타냅니다. *keytype*은 RSA 또는 DSA가 될 수 있습니다.

주 – 이 프로그램은 시스템을 시작하는 동안 실행될 수 있으므로, 콘솔이 `tty` 장치가 아닐 경우(즉, `tty`(3c)가 거짓값을 반환하는 경우)에 대처하도록 설계되었는지 확인하십시오.

공급된 프로그램인 `/opt/SUNWconn/crypto/bin/sslpassword`는 *program* 실행용으로 사용할 수 있습니다. 이 프로그램은 암호 입력 프롬프트를 자동으로 표시하고 입력된 암호가 표시되지 않도록 합니다.

제공된 sslpassword 프로그램은 파일 내에서 암호를 자동으로 검색하므로 웹 서버 시작 시 사용자 상호 작용을 방지하는 데 사용될 수 있습니다. 키 파일의 암호는 /etc/apache/*servername*:*port*.*keytype*.pass의 형식으로 검색됩니다. 이 파일이 표시되지 않을 경우에는 /etc/apache/default.pass 파일이 사용됩니다. 이 암호 파일은 자동으로 해독된 암호로 구성되어 있습니다.

주 – 암호 파일은 웹 서버를 실행하는 UNIX 사용자만이 읽을 수 있도록 권한을 부여하여 보호해야 하며 표준 아파치 User 지시어로 구성된 것과 동일한 사용자여야 합니다.

지정되지 않은 경우는 내부 프롬프트 메커니즘을 사용하는 것이 기본 동작이 됩니다. Sun 고객의 경우, 시스템 시작 시 상호 작용 문제를 방지하려면 기본 대신에 sslpassword 프로그램을 사용하는 것이 좋습니다.

2. SSLEngine (on|off)

   컨텍스트: global, virtual host

   이 지시어는 SSL 프로토콜을 활성화하는 데 사용됩니다. 일반적으로 가상 호스트에서 서버의 하위 집합에 SSL을 활성화하는 데 사용됩니다. 공통적으로 사용되는 형식은 다음과 같습니다.

```
<VirtualHost _default_:443>
SSLEngine on
</VirtualHost>
```

위의 형식으로 443 포트를 수신 대기하는 모든 서버에 대한 SSL 사용을 구성합니다(표준 HTTPS 포트). 표시되지 않을 경우, 기본값으로 꺼진 상태가 됩니다.

3. SSLProtocol [+-] *protocol*

   컨텍스트: global, virtual host

   이 지시어는 SSL 트랜잭션을 위해 사용할 프로토콜을 구성합니다.

   표 C-1에서 사용 가능한 프로토콜을 나열하고 설명합니다.

표 C-1 SSL 프로토콜

프로토콜	설명
SSLv2	Netscape의 최초 디팩토 표준 SSL 프로토콜
SSLv3	대부분의 웹 브라우저에서 지원되는 SSL 프로토콜의 업데이트 버전
TLSv1	현재(문서 작성 시점) 소수의 브라우저에서만 지원되며, IETF 표준화가 진행중인 SSLv3의 업데이트 버전
all	모든 프로토콜 사용 가능

플러스(+)나 마이너스(-) 기호를 사용하여 프로토콜을 추가하거나 제거할 수 있습니다. 예를 들어 SSLv2에 대한 지원을 비활성화하려면 다음 지시어를사용할 수 있습니다.

```
SSLProtocol all -SSLv2
```

다음 지시어와 동일합니다.

```
SSLProtocol +SSLv3 +TLSv1
```

4. `SSLCipherSuite` *cipher-spec*

   컨텍스트: global, virtual host, directory, `.htaccess`

   SSLCipherSuite 지시어는 사용할 수 있고 선호하는 SSL 암호가 어떤 것인지 구성하는 데 사용됩니다. 전체 컨텍스트 또는 가상 호스트 컨텍스트에서는 초기 SSL 핸드셰이크 동안 사용됩니다. 디렉토리별 컨텍스트에서는 강제로 SSL 재협상하여 지정된 암호를 사용합니다. 요청을 읽은 후 응답을 보내기 전에 재협상이 발생합니다.

   *cipher-spec*은 표 C-2에 설명되어 있는 암호의 콜론 구분 목록입니다.

표 C-2 사용가능한 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

표 C-2 사용가능한 SSL 암호

암호-태그	프로토콜	키 교환	승인	암호화	MAC	유형
EXP-RC2-CBC-MD5	SSLv3	RSA (512비트)	RSA	ARCTWO (40비트)	SHA1	내보내기
EXP-RC4-MD5	SSLv3	RSA (512비트)	RSA	ARCFOUR (40비트)	MD5	내보내기
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-2에서 DH는 Diffie-Hellman를 의미하며 DSS는 Digital Signature Standard를 의미합니다.

표 C-3에서는 매크로와 유사한 그룹화를 제공하는 별칭을 나열하고 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

표 C-3 SSL 별칭

별칭	설명
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
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 나열하고 설명한 특수 문자를 사용하여 구성할 수 있습니다.

표 C-4 암호의 선호도를 구성하는 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 기본값

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
```

기본값은 익명(인증되지 않은)의 Diffie-Hellman을 제외한 모든 암호를 구성하고 ARCFOUR 및 RSA에 선호도를 부여하여 낮은 수준에 대해 더 높은 수준의 암호화를 제공합니다.

5. `SSLCertificateFile` *file*

   컨텍스트: global, virtual host

   이 지시어는 서버에 대한 PEM 암호화 X.509 인증 파일의 위치를 지정합니다.

6. `SSLCertificateKeyFile` *file*

   컨텍스트: global, virtual host

   이 지시어는 서버에 대한 PEM 암호화 개인 키 파일을 지정하며 `SSLCertificateFile` 지시어로 구성된 인증서에 해당됩니다.

7. `SSLCertificateChainFile` *file*

   컨텍스트: global, virtual host

   이 지시어는 서버의 인증 경로를 만드는 PEM 암호화 인증서를 포함하는 파일의 위치를 지정합니다. 서버 인증서가 클라이언트가 인식하는 기관에 의해 직접 서명되지 않은 경우, 클라이언트가 서버 인증서를 확인하도록 돕는 역할을 합니다.

   클라이언트 인증(`SSLVerifyClient`)을 사용할 때 체인에 있는 인증서 역시 클라이언트 인증에 유효합니다.

8. `SSLCACertificateFile` *file*

   컨텍스트: global, virtual host

   이 지시어는 클라이언트 인증에 사용된 인증 기관(CA)에 대해 일련의 인증서를 포함하는 파일의 위치를 지정합니다.

9. `SSLCARevocationFile` *file*

   컨텍스트: global, virtual host

   이 지시어는 클라이언트 인증에 사용된 일련의 CA 인증 거부 목록을 포함하는 파일의 위치를 지정합니다.

10. `SSLVerifyClient` *level*

    컨텍스트: global, virtual host, directory, `.htaccess`

    이 지시어는 서버에 클라이언트 인증을 구성합니다(일반적으로 전자상거래 응용 프로그램에 꼭 필요하지는 않지만 기타 응용 프로그램에서 사용됨).

    표 C-5에서 *level*에 대한 값을 나열하고 설명합니다.

표 C-5 SSL 검증 클라이언트 레벨

레벨	설명
없음	클라이언트 인증서 필요 없음
`optional`	클라이언트가 유효한 인증서를 제공할 수 있음
`require`	클라이언트가 유효한 인증서를 *반드시* 제공해야 함
`optional_no_ca`	클라이언트가 인증서를 제공할 수 있으나 유효할 필요 없음

일반적으로 `none` 또는 `require`이 사용됩니다. 기본값은 `none`입니다.

11. `SSLVerifyDepth` *depth*

    컨텍스트: global, virtual host, directory, `.htaccess`

    이 지시어는 클라이언트 인증에 대해 서버가 허용하는 인증서 체인의 최대 깊이를 지정합니다. 0 값은 자체 서명된 인증서가 적합함을 의미하며, 1 값은 클라이언트 인증서가 서버에 직접 알려진 CA에 의해 서명되어야 함을 의미합니다 (`SSLCACertificateFile`을 통해서). 그 이상의 값은 CA의 위임을 허용합니다.

12. `SSLLog` *filename*

    컨텍스트: global, virtual host

    이 지시어는 SSL 관련정보가 기록될 로그 파일을 지정합니다. 지정(기본값)되지 않을 경우, SSL 관련 정보가 기록되지 않습니다.

13. `SSLLogLevel` *level*

    컨텍스트: global, virtual host

    이 지시어는 SSL 로그 파일에 기록된 대량의 정보를 지정합니다. 표 C-6에서 *level*에 대한 값을 나열하고 설명합니다.

표 C-6 SSL 로그 레벨 값

값	설명
없음	기록하지는 않지만 오류 메시지를 표준 아파치 오류 로그에 보냅니다.
`warn`	경고 메시지를 포함합니다.
`info`	정보 메시지를 포함합니다.
`trace`	추적 메시지를 포함합니다.
`debug`	디버그 메시지를 포함합니다.

14. `SSLOptions` [`+-`] *option*

    컨텍스트: global, virtual host, directory, `.htaccess`

    이 지시어는 SSL의 고유 옵션을 구성합니다. 플러스 기호(+)를 앞에 붙여 현재 구성에 옵션을 추가하거나 마이너스 기호(-)를 사용하여 제거할 수 있습니다. 플러스 또는 마이너스 기호를 표시하지 않을 경우, 가장 근접한 옵션 집합이 사용됩니다.

표 C-7에서 옵션을 나열하고 설명됩니다.

표 C-7 사용 가능한 SSL 옵션

옵션	설명
`StdEnvVars`	SSL 관련 CGI/SSI 환경 변수의 표준 집합을 생성합니다. 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 아파치 액세스 컨트롤 메커니즘을 사용할 수 있습니다. 아파치 암호 파일에서 사용자 엔트리로 암호화된 암호 `xxj31ZMTZzkVA`를 사용해야 합니다. `xxj31ZMTZzkVA`은 "암호"라는 단어의 암호화된 형식(`crypt`(3c))입니다.
`StrictRequire`	`Satisfy Any`와 같은 SSLRequireSSL을 능가하는 지시어를 제공해도 `SSLRequireSSL`로 인해 강제로 금지된 액세스가 거부되도록 합니다.

15. `SSLRequireSSL`

    컨텍스트: directory, `.htaccess`

    이 지시어는 HTTPS를 사용하지 않으면 해당 디렉토리에 액세스하는 것을 금지합니다. 디렉토리의 내용을 인증되지 않고 암호화되지 않은 액세스에 노출될 수 있는 구성 오류로부터 보호하는 데 사용될 수 있습니다.

부록 **D**

Sun Crypto Accelerator 1000 보드와 함께 사용하기 위한 응용 프로그램 구축

이 부록에서는 Sun Crypto Accelerator의 암호화 가속 기능을 이용하여 일부 OpenSSL 호환 응용 프로그램을 구축하는 데 사용할 수 있는 Sun Crypto Accelerator 1000에 함께 제공되는 소프트웨어에 대해 설명합니다.

주 – Sun Crypto Accelerator 1000 소프트웨어 및 하드웨어를 사용하기 위한 응용 프로그램의 구축에 대한 정보는 있는 그대로 정확히 제공되며 이 제품에서 공식적으로 지원받은 부분은 아닙니다. 이 정보는 고객의 편리를 위한 목적으로 보증 없이 제공됩니다. Sun이 지원하는 솔루션이 필요할 경우, Sun Professional Services에 문의하여 옵션에 대한 정보를 받으십시오.

우선 필요한 헤더 파일 및 라이브러리가 포함된 `SUNWcrysl` 패키지를 설치해야 합니다.

다음과 같이 `/opt/SUNWconn/crypto/include`에서 컴파일러 플래그와 함께 OpenSSL 헤더를 포함하도록 응용 프로그램을 구성해야 합니다.

```
-I /opt/SUNWconn/crypto/include
```

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. 링커 플래그가 다음과 같이 수행합니다.

```
-L/opt/SUNWconn/crypto/lib -R/opt/SUNWconn/crypto/lib \
-lcrypto -lssl -lcryptography -lnvpair
```

모든 OpenSSL 응용 프로그램을 이러한 방식(www.openssl.org에서 다운로드하여 OpenSSL 라이브러리로 구축하는 방법의 반대 방법)으로 컴파일하는 것은 아닙니다.

부록 **E**

Sun Crypto Accelerator 1000 보드 규격

이 장에서는 Sun Crypto Accelerator 1000 보드의 다양한 사양에 대해 약술합니다.

이 부록은 다음 절로 구성되어 있습니다.

물리적 크기

표 E-1 물리적 크기

크기	치수	미터 치수
길이	6.875인치	174.625밀리미터
너비	4.2인치	106.680밀리미터

인터페이스 사양

표 E-2 인터페이스 사양

기능	사양
PCI 클럭	33MHz 또는 66MHz
호스트 인터페이스	33 MHz 또는 66 MHz의 클럭 속도 및 3.3V 또는 5V 전력을 지원하는 PCI 2.1
PCI 버스 너비	32비트 또는 64비트

전력 요구 사항

표 E-3 전력 요구 사항

사양	치수
최대 전력 소모량	10W @ 5V 700mW @ 3.3V
전압 안정도	5V +/- 5% 3.3V +/- 5%
작동 전류	2A @ 1.8V 150mA @ 3.3V

환경 사양

표 E-4 환경 사양

조건	동작 사양	보관 사양
온도	0° ~ 70°C, 32° ~ 160°F	-65° ~ +150°C, -85° ~ 300°F
상대 습도	5 ~ 85% 비응축	0 ~ 95% 비응축

부록 **F**

Third-Party Licenses (제삼자 라이센스 조항)

Some portions of Software are provided with notices and/or licenses from other parties which govern the use of those portions.

OPENSSL LICENSE ISSUES

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

OpenSSL License

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

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

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

Original SSLeay License

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

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

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

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

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

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

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

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

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

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

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

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

MOD_SSL LICENSE

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

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

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

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

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

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

색인