Sun™ Crypto Accelerator 4000
보드 릴리스 노트

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

일련 번호: 817-2349-10
2003년 5월, 개정판 A

본 설명서에 대한 의견은 docfeedback@sun.com으로 보내 주십시오.

재활용
가능

Adobe PostScript

Sun™ Crypto Accelerator 4000 보드 릴리스 노트

본 릴리스 노트에는 Sun Crypto Accelerator 4000 보드의 알려진 문제점에 대한 설명이 들어 있습니다.

Sun Crypto Accelerator 4000 소프트웨어 설치 시 114795-01 패치가 자동으로 설치됩니다. 향후 업데이트시 이 패치의 새 버전을 확인하려면 `showrev -p` 명령을 사용하십시오.

Sun Crypto Accelerator 4000 소프트웨어의 알려진 문제점

지원 플랫폼

Sun Fire™ 15K 플랫폼은 현재 Sun Crypto Accelerator 4000 보드를 지원하지 않습니다.

FCODE 버전

Sun Crypto Accelerator 4000 보드용 FCODE 버전은 12.11.13입니다. *Sun Crypto Accelerator 4000 보드 설치 및 사용 설명서* 15페이지의 `.properties` 출력에는 올바른 FCODE 버전이 나와있지 않습니다.

버그 ID 4757594 vca.conf 변수

Solaris 소프트웨어에서 이 버그가 수정될 때까지 버그에 대한 수동 해결책으로 vca.conf 변수가 제공됩니다. kernel/drv/vca.conf 파일에 다음 항목을 추가하십시오.

```
dma-mode=1;
```

이 해결책은 Sun Blade™ 100 및 150과 같은 하급(low-end) 플랫폼에서만 필요합니다.

버그 ID 4470196 Solaris 8 패치 필요

Solaris 8 운영 환경에서는 Sun Crypto Accelerator 4000 소프트웨어를 설치하기 전에 패치 번호 112438-01과 109234-09를 반드시 설치해야 합니다. 해당 패치는 제품 CD의 patches 하위 디렉토리에 들어 있으며 http://sunsolve.sun.com에서도 다운로드할 수 있습니다.

참고 – 이 패치를 적용한 다음 반드시 시스템을 재부팅한 ***후에*** Sun Crypto Accelerator 4000 소프트웨어를 설치하십시오.

버그 ID 4621453 키 추출

키 추출 소프트웨어 도구는 Sun ONE 웹 서버 6.x 릴리스에 들어 있기 때문에 Sun™ ONE 웹 서버 4.x에는 들어 있지 않습니다.

참고 – Sun ONE 웹 서버의 이전 이름은 iPlanet™ 웹 서버였습니다.

소프트웨어(내부) 데이터베이스 키 추출에 대해 다음 두 가지 임시 해결책이 있습니다.

- 다음 웹 사이트에서 NSPR 4.12 및 NSS 3.3(또는 이후 릴리스)을 다운로드합니다. http://www.mozilla.org

  소프트웨어 배포판을 설치한 다음 소프트웨어(내부) 데이터베이스에서 정확한 인증서 및 키를 추출하기 위해 pk12util을 실행합니다.
- Netscape Communicator 4.x 또는 6.x를 사용하여 소프트웨어(내부) 데이터베이스에서 정확한 키를 추출합니다.

버그 ID 4630250 키 및 인증 자료

이 문서를 작성한 시점에서는 Sun Crypto Accelerator 4000 보드에서 키 및 인증 자료를 추출하기 위한 메커니즘을 사용할 수 없었습니다. 패치가 이 문제 해결을 위해 작성되었는지 `http://sunsolve.sun.com`에서 패치 데이터베이스를 검사하십시오.

버그 ID 4796664 내부 되돌림 테스트

Sun Crypto Accelerator 4000 MMF 보드가 SunVTS™ 테스트의 내부 되돌림 테스트인 `netlbtest`에 실패하는 경우가 있습니다. 다음과 같은 오류 메시지가 나타날 수 있습니다.

```
"
12/19/02 17:20:03 username SunVTS4.5: VTSID 8003 netlbtest.
  FATAL vca1:    "Failed to get the link up.
  Probable_Cause(s):
    (1)Loopback cable not connected.
    (2)Faulty loopback cable.
  Recommended_Action(s):
    (1)Check and replace, if necessary, the loopback cable.
    (2)If problem persists, call your authorized Sun service
provider.
```

버그 ID 4826508 단일 명령 모드 로그인

단일 명령 모드에서 `vcaadm`을 사용하고 로그인에 실패한 경우, 이 프로그램에서 다음과 같이 출력합니다.

```
Security Officer Login: so
Security Officer Password:
Login failed.

Error writing data: Bad file number
```

버그 ID 4816009 FIPS 모드 활성화

보안 관리자가 소유자이고 이 보안 관리자가 FIPS 모드를 활성화한 경우 암호화 작업에 비소유 보드를 사용하면 보드가 중지될 수 있습니다.

해결책: FIPS 모드일 때 보드를 원상 복구하지 말고, 보드에 암호화 요청 전송 중에 FIPS 모드의 카드를 초기화하지 마십시오.

버그 ID 4825721 Sun Fire 15K 시스템 테스트

MMF 및 UTP 보드에서 지점간(PTP) 구성으로 Sun Fire 15K 테스트를 수행하는 경우, 콘솔에 다음 오류 메시지가 표시됩니다.

```
Feb 27 11:39:04 xc15p13-b3 vca: [ID 732820 kern.warning] WARNING:
vca1: vce_link_stats_set: cant determine params
Feb 27 11:40:29 xc15p13-b3 vca: [ID 214153 kern.warning] WARNING:
vca1: Can't determine link paramaters!
Feb 27 11:40:29 xc15p13-b3 vca: [ID 702911 kern.notice] NOTICE:
vca1: link up 0 Mbps half duplex
Feb 27 11:40:29 xc15p13-b3 vca: [ID 732820 kern.warning] WARNING:
vca1: vce_link_stats_set: cant determine params
Feb 27 11:41:08 xc15p13-b3 vca: [ID 702911 kern.notice] NOTICE:
vca0: link down
Feb 27 12:01:07 xc15p13-b3 vca: [ID 702911 kern.notice] NOTICE:
vca0: link up 1000 Mbps full duplex
```

이 메시지가 표시되어도 몇 분 후 연결이 재개되므로 통신에는 영향을 미치지 않습니다.

RFE ID 4753295

기본적으로 Apache 웹 서버 소프트웨어는 대용량 암호화 기능이 활성화되어 있으며 비활성화할 수 없습니다. Sun ONE 서버 소프트웨어는 기본적으로 대용량 암호화 기능이 비활성화되어 있으며 이 기능을 사용하려면 빈 파일 (`/etc/opt/SUNWconn/cryptov2/sslreg`)을 생성한 후 Sun ONE 서버 소프트웨어를 재시작하여 수동으로 활성화해야 합니다. Sun ONE 서버 소프트웨어에서 대용량 암호화 기능을 활성화하면 대용량 파일의 전송 속도는 크게 증가하지만 소용량 파일의 전송 속도는 약간 감소될 수 있습니다.

해결책: 대용량 파일을 전송할 경우에만 Sun ONE 서버의 대용량 암호화 기능을 활성화하십시오.

버그 ID 4822356 vcaadm을 통한 마스터 키 재생성

rekey master 명령 수행 시, vcaadm에서 "Cannot get new modulus from firmware" (펌웨어에서 새로운 모듈을 찾을 수 없음)이라는 메시지를 표시합니다. 이 메시지가 마스터 키가 재생성되지 않았음을 의미하지는 않습니다. 실제로는 명령이 성공적으로 완료되었으므로 이 오류 메시지는 잘못 표시된 것입니다.

```
vcaadm{vca0@localhost, sec_officer}> rekey master
WARNING: Rekeying the master key will render all old board backups
         useless with the new keystore file.  If other boards use
this
          keystore, you will need to back up this new key and
initialize
        the other boards to use the keystore, providing the backed
up
          master key in the process.

Rekey board? (Y/Yes/N/No) [No]: y
Rekeying crypto accelerator board.  This may take a few
minutes...Done.
Cannot get new modulus from firmware.
```

버그 ID 4852120 시간 초과 오류

네트워크 트래픽이 극도로 복잡한 시간에 암호화 작업을 수행하는 경우, 다음과 유사한 오류 메시지가 나타날 수 있습니다.

```
Apr 17 23:44:37 xc15p13-b0 vca: WARNING: stale job(s) found in ring 30000978718
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:          request 0x7820aa68
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:          ======================
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:          vr_key_id[0]: 0x00000000
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:          vr_key_id[1]: 0x00000000
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:          vr_cmd: 0x0013
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:          vr_key_flags[0]: 0x0
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:          vr_key_flags[1]: 0x0
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:          vr_in_len: 192
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:          vr_out_len: 192
Apr 17 23:44:37 xc15p13-b0 genunix: WARNING: vca1: fault detected in device;
service unavailable
Apr 17 23:44:37 xc15p13-b0 genunix: WARNING: vca1: crypto job timeout (device
hung?)
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE: vca1: Resetting board...
Apr 18 00:08:47 xc15p13-b0 vca: WARNING: vca1: Device is in failed state!
Apr 18 00:08:47 xc15p13-b0 last message repeated 1 time
```

해결책: Sun Crypto Accelerator 4000 보드를 재설정하십시오.

Sun ONE 웹 서버에 나타난 문제점

버그 ID 4532645 관리 서버 메시지

Sun ONE 4.x 또는 6.x 관리 서버를 실행 중이고 관리 중인 웹 서버가 실행 중이 아닐 경우, 토큰 암호를 묻는 대화 상자가 여러 상황에서 표시됩니다. 너무 큰 글꼴을 사용하거나 토큰이 많아서 암호 입력 행이 여러 줄로 표시되는 경우, 대화 상자의 크기가 고정되어 있으므로 패널 하단의 단추가 표시되지 않습니다. 대화 상자의 크기를 조정할 수 없으므로 패널 하단의 [Accept(동의)] 단추를 선택하고 변경 사항을 전송할 수 없습니다.

이 문제는 다음 두 가지 방법으로 해결할 수 있습니다.

- [GUI Preference(GUI 등록 정보)]를 [On/Off(설정/해제)]로 설정하여 명령행 또는 관리 창에서 웹 서버를 먼저 시작합니다.
- [Apply(적용)] → [Load Configuration Files(구성 파일 로드)]를 차례로 눌러 서버를 시작하지 않고 구성을 적용합니다.

버그 ID 4532941 및 4593111 다수의 키스토어

Sun ONE 웹 서버는 하나 이상의 키스토어가 존재하는 구성에서 제대로 작동하지 않습니다. Sun ONE 웹 서버 6.0 서비스 팩 5 (SP5)에서 이 문제가 해결되었습니다.

해결책: 모든 웹 서버 인스턴스에 대하여 하나 이상의 키스토어를 구성하지 마십시오. 웹 서버 인스턴스 각각에 대하여 각기 다른 키스토어를 구성하여 각각의 웹 서버 인스턴스에 키를 상호 분리하여 저장할 수 있습니다.

버그 ID 4620283 `pk12util` 유틸리티

Sun ONE 제공 유틸리티인 `pk12util`은 내부(소프트웨어) 데이터베이스에서 인증서 및 키를 내보낸 다음 외부(하드웨어) 데이터베이스로 가져옵니다. 그러나 외부 데이터베이스에서는 인증서 또는 키를 내보내지 않습니다.

```
% cd /usr/iplanet/servers/alias
% pk12util -o temp.p12 -n "Our Token:Server-Cert" -d .
Enter Password or Pin for "Our Token":
Enter password for PKCS12 file:
Re-enter password:
pk12util: add cert and key failed: Unable to export.  Private Key
could not be located and exported.
```

버그 ID 4607112 암호 기본값 설정

Sun ONE 웹 서버 6.0을 구성할 때 [Cipher Default(암호 기본값)] 설정을 선택하고, 인증서를 선택하고, [OK(확인)] 단추를 눌러 오른쪽 상단 모서리의 [Apply(적용)] 링크를 선택하여 암호를 적용한 후, *Sun Crypto Accelerator 4000 보드 설치 및 사용 설명서*에 나와 있는 순서대로 정확히 실행하지 않으면 *username:password* 항목이 제거될 수 있습니다. Sun ONE 웹 서버 6.0 서비스 팩 3 (SP3)에서 이 문제가 해결되었습니다.

웹 서버가 Sun Crypto Accelerator 4000 보드와 함께 정확히 시작하려면 이 항목이 필요합니다. 다음 순서에 따라 단계를 실행하면 웹 서버가 시작됩니다.

1. [Cipher Default(암호 기본값)]를 [SSL2] 암호 또는 [SSL3] 암호로 선택합니다.
2. [OK(확인)]를 선택합니다.
3. [Apply(적용)]를 선택합니다.
4. [Load Configuration(구성 로드)]를 선택합니다.

상기 단계를 완료한 후에도 웹 서버가 올바르게 시작되지 않으면 다음 해결책을 사용합니다.

■ 파일을 편집합니다.

```
/usr/iplanet/servers/https-호스트이름.도메인/config/server.xml
```

■ 다음으로 시작되는 행을 찾습니다.

```
<SSLPARAMS servercertnickname="Server-Cert". . .
```

■ 같은 행에서 Server-Cert 텍스트 앞에 *키스토어_이름*: 텍스트를 삽입하여 다음과 같이 변경합니다.

```
<SSLPARAMS servercertnickname="키스토어_이름:Server-Cert". . .
```

■ 웹 서버를 다시 시작합니다.

지원되는 Apache 웹 서버 버전

Sun Crypto Accelerator 4000 소프트웨어는 Apache 1.3.26을 지원합니다.

Apache 웹 서버의 알려진 문제점

버그 ID 4766977 Solaris 8 패치 필요

Solaris 8 운영 환경에서 Apache 웹 서버와 함께 사용하기 위한 Sun Crypto Accelerator 4000 보드를 구성하려면 Sun Crypto Accelerator 4000 소프트웨어를 설치하기 전에 패치 번호 109234-09를 설치해야 합니다. 이 패치는 제품 CD의 patches 하위 디렉토리에 들어 있으며 http://sunsolve.sun.com에서도 다운로드할 수 있습니다.

참고 – 이 패치를 적용한 다음 반드시 시스템을 재부팅한 ***후에*** Sun Crypto Accelerator 4000 소프트웨어를 설치하십시오.

Apache 웹 서버는 *Sun Crypto Accelerator **1000*** 보드와 *Sun Crypto Accelerator **4000*** 보드를 동시에 사용하도록 구성할 수 없습니다. 두 보드 모두가 Apache 웹 서버를 동시에 사용하도록 구성될 경우 Apache가 올바르게 작동되지 않습니다.

보드를 Apache 웹 서버 1.3.26과 함께 사용할 경우에만 Sun Crypto Accelerator 4000 `SUNWkcl2a` 소프트웨어를 설치하십시오. 다른 구성 또는 다른 버전의 Apache 웹 서버를 사용할 경우에는 `SUNWkcl2a` 패키지를 설치하지 마십시오.

시작 파일

Apache (`/etc/rc3.d/S50apache`) 및 `dtlogin` (`/etc/rc2.d/S99dtlogin`)에 대한 시작 파일을 명령하면 시스템 부팅 시에 명령 문제를 발생시킵니다. 이로 인해 시스템 시작 시 Apache 암호 항목을 사용하기 위해 콘솔 액세스가 불가능합니다.

해결책: 루트로 전환한 후 다음 명령을 실행하여 Apache 웹 서버 시작 명령을 다시 실행합니다.

```
# mv /etc/rc3.d/S50apache  /etc/rc2.d/S95apache
```