Sun™ Crypto 加速器 4000 板发布说明

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

部件号 817-2350-10
2003 年 5 月，修订版 A

请将有关本文档的意见发送至：docfeedback@sun.com

版权所有 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 U.S.A. 保留所有权利。

本产品或文档的发行受限制本产品或文档使用、复制、发行和反编译的许可证的制约。未经 Sun 及其许可证发行者 （如果有）事先书面授权，不得以任何形式、任何方式复制本产品或文档的任何部分。第三方软件，包括字体技术，均已从 Sun 供应商获得版权和许可。

产品的某些部件可能源于 Berkeley BSD 系统， Sun 已从 University of California 获得使用许可。 UNIX 是在美国及其它国家/地区的注册商标， Sun 已从 X/Open Company, Ltd. 获得独家使用授权。

Sun、Sun Microsystems、Sun 徽标、SunVTS、AnswerBook2、docs.sun.com、iPlanet、Sun Enterprise、Sun Enterprise Volume Manager 和 Solaris 是 Sun Microsystems, Inc. 在美国以及其它国家/地区的商标、注册商标或服务商标。所有 SPARC 商标都是 SPARC International, Inc. 在美国以及其它国家/地区的商标或注册商标，必须根据许可证条款使用。带有 SPARC 商标的产品以 Sun Microsystems, Inc. 开发的体系结构为基础。Netscape 是 Netscape Communications Corporation 的商标或注册商标。本产品包括由 OpenSSL Project 开发的用于 OpenSSL Toolkit 的软件 (http://www.openssl.org/)。本产品包括由 Eric Young (eay@cryptsoft.com) 编写的加密软件。本产品包括由 Ralf S. Engelschall <rse@engelschall.com> 编写的用于 mod_ssl 项目 (http://www.modssl.org/) 的软件。

OPEN LOOK 和 Sun™ 图形用户界面是 Sun Microsystems, Inc. 专门为其用户和许可证获得者开发的。 Sun 感谢 Xerox 在用户界面形象化和图形化研发方面为计算机行业所做的先导性贡献。 Sun 已从 Xerox 获得对 Xerox 图形用户界面 (GUI) 的非独占使用许可。该许可也涵盖实施 OPEN LOOK GUI 的 Sun 许可证获得者，而其它情况则应符合 Sun 的书面许可协议。

文档以 “原样”提供。除非有关的免责声明在法律上无效，否则 Sun 拒绝承担任何明确或暗示的条件、表示和担保，包括任何对适销性、特定用途的适用性或非侵犯性作出的暗示担保。

请回收

Adobe PostScript

Sun™ Crypto 加速器 4000 板发布说明

本 《发布说明》文档介绍 Sun Crypto 加速器 4000 板的已知问题。

安装 Sun Crypto 加速器 4000 软件时，将会自动安装修补程序 114795-01。要在将来升级时验证此修补程序的版本，请使用 `showrev -p` 命令。

与 Sun Crypto 加速器 4000 软件相关的已知问题

支持的平台

Sun Fire™ 15K 平台当前不支持 Sun Crypto 加速器 4000 板。

FCODE 版本

Sun Crypto 加速器 4000 板的 FCODE 版本为 12.11.13。《*Sun Crypto 加速器 4000 板安装和用户指南*》第 15 页的 `.properties` 输出中没有列出正确的 FCODE 版本。

错误 ID 4757594 vca.conf 变量

此错误的修复方案中提供了一个 vca.conf 变量，在 Solaris 软件解决此错误之前，可以手动添加此变量以解决此错误。请在 kernel/drv/vca.conf 文件中添加以下条目：

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

此解决方法仅适用于低端平台，例如， Sun Blade™ 100 和 150。

错误 ID 4470196 Solaris 8 必需的修补程序

对于 Solaris 8 操作环境，必须在安装 Sun Crypto 加速器 4000 软件之前安装版本号为 112438-01 和 109234-09 的修补程序。这些修补程序位于产品 CD 的 patches 子目录下，也可以从 http://sunsolve.sun.com 网站下载。

注意 – 应用这些修补程序后，您***必须***重新引导系统方可安装 Sun Crypto 加速器 4000 软件。

错误 ID 4621453 密钥抽取

Sun™ ONE Web 服务器 4.x 版本没有附带用于抽取密钥的软件工具，但 Sun ONE Web 服务器 6.x 版本附带了此类工具。

注意 – Sun ONE Web 服务器以前称为 iPlanet™ Web 服务器。

可用两种方法来解决软件 （内部）数据库密钥抽取问题：

- 从 http://www.mozilla.org 网站下载 NSPR 4.12 和 NSS 3.3 （或更高版本）

  安装这些软件产品，然后在数据库上运行 pk12util，以便从软件 （内部）数据库抽取证书和密钥。
- 使用 Netscape Communicator 4.x 或 6.x 从软件 （内部）数据库抽取密钥。

错误 ID 4630250 密钥和证书资料

本文档出版时，还没有办法从 Sun Crypto 加速器 4000 板抽取密钥和证书资料。您可访问 `http://sunsolve.sun.com` 网站的修补程序数据库，看看是否提供了能够解决这一问题的修补程序。

错误 ID 4796664 内部回送测试程序

Sun Crypto 加速器 4000 在 MMF 板上运行 SunVTS™ 测试软件包 `netlbtest` 的内部回送测试程序时，可能会失败，并且会显示以下错误消息：

```
"
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.
```

错误 ID 4826508 单命令模式登录

在单命令模式下无法通过 `vcaadm` 程序登录板，并且该程序会输出以下内容：

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

Error writing data: Bad file number
```

错误 ID 4816009 启用 FIPS 模式

如果一个未分配所有权的板用于加密操作，则在安全主管得到该板的所有权且启用 FIPS 模式时，该板可能会挂起。

解决方法：不要零置 FIPS 模式下的板；并且在将加密请求提交给板时，不要初始化板以用于 FIPS 模式。

错误 ID 4825721 测试 Sun Fire 15K 系统

在点对点配置中，在 MMF 和 UTP 板上执行 Sun Fire 15K 测试时，控制台上会显示以下错误消息：

```
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
```

由于链接会在数分钟后恢复，因此此操作不会引起通信中断。

RFE ID 4753295

默认情况下，系统会为 Apache Web 服务器软件启用批量加密，且不能禁用。对于 Sun ONE 服务器软件，批量加密在默认情况下禁用，并且必须通过以下手动方法才能启用：创建空文件 (`/etc/opt/SUNWconn/cryptov2/sslreg`)，然后重新启动 Sun ONE 服务器软件。为 Sun ONE 服务器软件启用批量加密后，传送较大文件的速率会大大提高，但对于较小文件，速率可能会稍微降低。

解决方法：仅在传送大文件的情况下为 Sun ONE 服务器软件启用批量加密。

错误 ID 4822356 使用 vcaadm 重新设置主密钥

执行 rekey master 命令时，vcaadm 会返回消息：Cannot get new modulus from firmware（无法从固件中获得新的模板）。这并非表示主密钥未被重新生成。此错误消息无效；命令实际上已成功完成。

```
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.
```

错误 ID 4852120 可能出现超时错误

在网络通信极其繁忙时，如果执行加密操作，则可能会显示与以下内容相似的错误信息。

```
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
```

解决方法：重置 Sun Crypto 加速器 4000 板。

与 Sun ONE Web 服务器相关的已知问题

错误 ID 4532645 管理服务器消息

运行 Sun ONE 4.x 或 6.x 管理服务器时，如果没有运行它所管理的 Web 服务器，则在数种情形下，可能会出现要求输入令牌密码的对话框。如果使用很大的字体，或者存在多种令牌 （因此需要输入很多密码：行），则不会显示面板底部的按钮，因为对话框太小，且大小固定。由于对话框的大小无法调整，因此无法从面板底部选择 “接受” 按钮来提交您的更改。

该问题有两种解决方法：

- 首先从命令行或管理窗口启动 Web 服务器，并将 GUI 首选项设为开/关。
- 在不启动 Web 服务器的前提下应用配置：Apply （应用） → Load Configuration Files （加载配置文件）。

错误 ID 4532941 和 4593111 多个密钥库

Sun ONE Web 服务器不便与具有多个密钥库的配置一起工作。此问题会在 Sun ONE Web 服务器 6.0 服务包 5 (SP5) 中得到解决。

解决方法：只为所有 Web 服务器例程配置一个密钥库。然后，您可以为每个 Web 服务器例程配置不同的密钥库用户，从而使每个 Web 服务器例程的密钥相互独立。

错误 ID 4620283 `pk12util` 实用程序

Sun ONE 附带的实用程序 `pk12util` 可从内部 （软件）数据库导出证书和密钥，并将它们导入外部 （硬件）数据库，但是不能从外部数据库导出证书或密钥：

```
% 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.
```

错误 ID 4607112 密码默认设置

配置 Sun ONE Web 服务器 6.0 期间，在选择 “Cipher Default”设置、选择证书、选择 “OK”按钮并选择右上角的 “Apply”链接以应用密码之后，如果不严格按照《*Sun Crypto 加速器 4000 板安装和用户指南*》中介绍的顺序进行操作，则 *user@realm-name* 条目可能会被删除。此问题会在 Sun ONE Web 服务器 6.0 服务包 3 (SP3) 中得到解决。

这是 Web 服务器正确启动 Sun Crypto 加速器 4000 板必不可少的条目。按以下顺序执行这些步骤时会出现此条目：

1. 选择 “Cipher Default”、 SSL2 密码或 SSL3 密码
2. 选择 “OK”
3. 选择 “Apply”
4. 选择 “Load Configuration”

如果您确信按上述顺序执行了这些步骤，但 Web 服务器并未正确启动，请采用以下解决方法：

- 编辑文件：

```
/usr/iplanet/servers/https-hostname.domain/config/server.xml
```

- 找到以下列内容开头的行：

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

- 在此行的文字 `Server-Cert` 之前插入文字 *keystore_name*:，如下所示：

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

- 重新启动 Web 服务器。

Apache Web 服务器的支持版本

本 Sun Crypto 加速器 4000 软件版本支持 Apache 1.3.26。

与 Apache Web 服务器相关的已知问题

错误 ID 4766977 Solaris 8 必需的修补程序

要在 Solaris 8 操作环境下配置 Sun Crypto 加速器 4000 板以便与 Apache Web 服务器配合使用，必须在安装 Sun Crypto 加速器 4000 软件之前安装版本号为 109234-09 的修补程序。此修补程序位于产品 CD 的 `patches` 子目录下，也可以从 `http://sunsolve.sun.com` 网站下载。

注意 – 应用此修补程序后，您***必须***重新引导系统方可安装 Sun Crypto 加速器 4000 软件。

Apache Web 服务器不能同时与 *Sun Crypto 加速器* ***1000*** 板和 *Sun Crypto 加速器* ***4000*** 板配合使用。如果让这两个板同时使用 Apache Web 服务器，Apache 将无法正常工作。

只有您准备将板与 Apache Web 服务器 1.3.26 配合使用时，才有必要安装 Sun Crypto 加速器 4000 `SUNWkcl2a` 软件包。如果使用其它配置或 Apache Web 服务器版本，则不必安装 `SUNWkcl2a` 软件包。

启动文件

Apache 的启动文件 (`/etc/rc3.d/S50apache`) 与 `dtlogin` 的启动文件 (`/etc/rc2.d/S99dtlogin`) 的顺序会导致计算机启动时的顺序问题。这可能会导致启动时无法访问控制台进而无法输入 Apache 密码。

解决方法：以 root 用户身份发出以下命令，重新调整 Apache Web 服务器的启动顺序：

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