



Sun™ Crypto Accelerator 4000 介面卡版本注意事項

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

零件編號 817-2351-10
2003 年 5 月，修訂版 A

請將關於此文件的意見傳送到：docfeedback@sun.com

著作權所有 2003 年 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 U.S.A. 所有權利均予保留。

本產品或文件在限制其使用、複製、發行及反編譯的授權下發行。事先未經 Sun 及其授權人的書面許可，不得使用任何方法以任何形式複製本產品或文件的任何部分。協力廠商軟體，包含字型技術，其著作權歸 Sun 供應商所有，經授權後使用。

本產品的某些部分可能衍生自加州大學授權的 Berkeley BSD 系統的開發成果。UNIX 為美國及其他國家的註冊商標，已獲得 X/Open Company, Ltd. 專屬授權。

Sun、Sun Microsystems、Sun 標誌、SunVTS、AnswerBook2、docs.sun.com、iPlanet、Sun Enterprise、Sun Enterprise Volume Manager 及 Solaris 是 Sun Microsystems, Inc. 在美國及其他國家的商標、註冊商標或服務標誌。所有 SPARC 商標都是 SPARC International, Inc. 在美國及其他國家的商標或註冊商標，經授權後使用。凡帶有 SPARC 商標的產品都是以 Sun Microsystems, Inc. 所開發的架構為基礎。Netscape 是 Netscape Communications Corporation 的商標或註冊商標。本產品包括由 OpenSSL Project 所開發的軟體，供 OpenSSL Toolkit 使用 (<http://www.openssl.org/>)。本產品包含由 Eric Young (eay@cryptsoft.com) 所撰寫的加密軟體。本產品包括由 Ralf S. Engelschall <rse@engelschall.com> 所開發的軟體，供 mod_ssl 計劃使用 (<http://www.modssl.org/>)。

OPEN LOOK 與 Sun™ Graphical User Interface (Sun 圖形使用者介面) 都是由 Sun Microsystems, Inc. 為其使用者與被授權人開發的技術。Sun 公司感謝 Xerox 公司在研究和開發視覺化或圖形化使用者介面概念方面，為電腦工業所作的先驅性努力。Sun 擁有經 Xerox 授權的 Xerox 圖形使用者介面非專屬授權，該授權亦涵蓋使用 OPEN LOOK GUI 並遵守 Sun 書面授權合約的 Sun 公司授權者。

本文件以其「現狀」提供，且在所為免責聲明合法之限度以內，明示不為任何明示或暗示的條件、表示或保固負責，包括但不限於隱含的適銷性保固、特定用途的適用性與非侵權性。



Sun™ Crypto Accelerator 4000 介面卡版本注意事項

本版本注意事項文件將說明 Sun Crypto Accelerator 4000 介面卡的已知問題。

在安裝 Sun Crypto Accelerator 4000 軟體時，系統會自動安裝修正程式 114795-01。要檢查此修正程式的版本以便將來進行更新，請使用 `showrev -p` 指令。

Sun Crypto Accelerator 4000 軟體的已知問題

支援的平台

Sun Fire™ 15K 平台目前不支援 Sun Crypto Accelerator 4000 介面卡。

FCODE 版本

Sun Crypto Accelerator 4000 介面卡的 FCODE 版本為 12.11.13。在 *Sun Crypto Accelerator 4000 介面卡安裝與使用者指南* 的第 15 頁中，`.properties` 執行結果並未列出正確的 FCODE 版本。

錯誤 ID 4757594 vca.conf 變數

此錯誤的解決辦法是在 Solaris 軟體中更正此錯誤前，提供 vca.conf 變數作為手動解決方法。請在 kernel/drv/vca.conf 檔案中新增下列項目：

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

本解決方法只適用於低階平台，例如：Sun Blade™ 100 與 150。

錯誤 ID 4470196 需要 Solaris 8 修正程式

對於 Solaris 8 作業環境，您必須在安裝 Sun Crypto Accelerator 4000 軟體之前，先安裝編號為 112438-01 與 109234-09 的修正程式。這些修正程式可在產品 CD 的 patches 子目錄中找到，也可到 <http://sunsolve.sun.com> 下載。

注意 – 套用這些修正程式後，您必須先重新啟動系統，然後再安裝 Sun Crypto Accelerator 4000 軟體。

錯誤 ID 4621453 金鑰擷取

Sun™ ONE Web Server 4.x 版本未隨附用於金鑰擷取的軟體工具，Sun ONE Web Server 6.x 版本隨附此工具。

注意 – Sun ONE 網站伺服器之前稱為 iPlanet™ 網站伺服器。

目前有兩個解決方法可用於軟體（內部）資料庫的金鑰擷取：

- 請到下列網站下載 NSPR 4.12 與 NSS 3.3（或更新版本）：
<http://www.mozilla.org>

請先安裝這些軟體，然後在資料庫上執行 `pk12util`，以從軟體（內部）資料庫擷取憑證與金鑰。

- 使用 Netscape Communicator 4.x 或 6.x 以便從軟體（內部）資料庫擷取金鑰。

錯誤 ID 4630250 金鑰與憑證資料

在本文件發行時，還沒有可用於從 Sun Crypto Accelerator 4000 介面卡上擷取金鑰與憑證資料的機制。請檢查 <http://sunsolve.sun.com> 中的修正程式資料庫，以確定是否已建立解決此問題的修正程式。

錯誤 ID 4796664 內部迴路測試

Sun Crypto Accelerator 4000 MMF 介面卡可能無法通過 SunVTS™ netlbttest 測試的內部迴路測試。可能會出現的錯誤訊息如下：

```
"
12/19/02 17:20:03 username SunVTS4.5: VTSID 8003 netlbttest.
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.
```

錯誤 ID 4826508 單一指令模式登入

在單一指令模式下使用 vcaadm 且登入失敗時，該程式會顯示下列訊息：

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

Error writing data: Bad file number
```

錯誤 ID 4816009 啓用 FIPS 模式

如果您使用所有權屬於安全管理員的介面卡進行編碼作業，且安全管理員啓用了 FIPS 模式，該介面卡可能會當機。

解決方法：請勿將處於 FIPS 模式下的介面卡化零，也不要對介面卡送出編碼要求時初始化介面卡以使用 FIPS 模式。

錯誤 ID 4825721 測試 Sun Fire 15K 系統

在 MMF 與 UTP 介面卡上執行點對點組態的 Sun Fire 15K 測試時，主控台上會顯示下列錯誤：

```
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
```

這不會導致任何通訊中斷，因為連結在幾分鐘之後即會恢復。

錯誤 ID 4753295

根據預設值，供 Apache 網站伺服器軟體使用的大量加密功能已啟用，您無法停用此功能。對於 Sun ONE 伺服器軟體，大量加密功能預設為停用，您必須建立空白檔案 (/etc/opt/SUNWconn/cryptov2/sslreg) 並重新啟動 Sun ONE 伺服器軟體以手動啟用此功能。在為 Sun ONE 伺服器軟體啟用大量加密功能時，傳輸大檔案的效能將明顯提高，但傳輸小檔案的效能會稍微降低。

解決方法：僅在主要傳輸大檔案時為 Sun ONE 伺服器軟體啟用大量加密功能。

錯誤 ID 4822356 使用 vcaadm 更新主要金鑰

在執行 `rekey master` 指令時，`vcaadm` 將傳回「Cannot get new modulus from firmware.」訊息。這並不表示尚未重新產生主要金鑰。此錯誤訊息無效；該指令實際上已成功完成。

```
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.
```

錯誤 ID 4852120 可能的逾時錯誤

在網路流量非常大時執行編碼作業，系統可能會顯示類似以下所示的錯誤訊息。

```
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
```

解決方法：重設 Sun Crypto Accelerator 4000 介面卡。

Sun ONE 網站伺服器的已知問題

錯誤 ID 4532645 管理伺服器訊息

如果執行的是 Sun ONE 4.x 或 6.x 管理伺服器，且受管理的網站伺服器目前不在執行中，則會出現要求輸入標記密碼的對話方塊的狀況。如果使用相當大的字型，或有許多標記（因此會有許多「Enter password:」指令行），面板下方的按鈕會因為大小固定的對話方塊太小了而無法顯示。由於對話方塊無法重新調整大小，因此無法選擇面板下方的「Accept」按鈕送出變更。

此問題有兩種解決方法：

- 先將 GUI Preference 設定為 On/Off，並從指令行或管理視窗啟動網站伺服器。
- 套用組態但不啟動伺服器：Apply→Load Configuration Files。

錯誤 ID 4532941 與 4593111 多個金鑰庫

在存在多個金鑰庫的組態下工作時，Sun ONE 網站伺服器會發生問題。此問題在 Sun ONE Web Server 6.0 Service Pack 5 (SP5) 中已經解決。

解決方法：為所有網站伺服器例項只設定一個金鑰庫。然後，您可以為每個網站伺服器例項設定不同的金鑰庫使用者。這將使每個網站伺服器例項的金鑰相互獨立。

錯誤 ID 4620283 pk12util 公用程式

Sun ONE 提供的 pk12util 公用程式會從內部（軟體）資料庫匯出憑證與金鑰，並將其匯入外部（硬體）資料庫，但不會從外部資料庫匯出憑證或金鑰：

```
% 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.
```

錯誤 ID 4607112 編碼器預設值

在設定 Sun ONE Web Server 6.0 過程中，如果在依次選擇 Cipher Default 設定、憑證、OK 按鈕及右上角的 Apply 連結以套用編碼器後，未依照 *Sun Crypto Accelerator 4000 介面卡安裝與使用者指南* 中所述的正確順序執行步驟，則可能會移除 *username:password* 項目。此問題在 Sun ONE Web Server 6.0 Service Pack 3 (SP3) 中已經解決。

此項目是正確啟動裝有 Sun Crypto Accelerator 4000 介面卡的網站伺服器所需的項目。按下列順序執行這些步驟即可看到此項目：

1. 選擇 Cipher Default、SSL2 ciphers、或 SSL3 ciphers
2. 選擇 OK
3. 選擇 Apply
4. 選擇 Load Configuration

如果您已執行這些步驟，但網站伺服器仍無法正確啟動，請使用下列解決方法：

- 編輯檔案：

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

- 找到開頭如下的指令行：

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

- 在指令行中的 Server-Cert 之前插入 *keystore_name*，使變更後的指令行如以下所示：

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

- 重新啟動網站伺服器。

支援的 Apache 網站伺服器版本

此版本的 Sun Crypto Accelerator 4000 軟體支援 Apache 1.3.26。

Apache 網站伺服器的已知問題

錯誤 ID 4766977 需要 Solaris 8 修正程式

要設定 Sun Crypto Accelerator 4000 介面卡以在 Solaris 8 作業環境下與 Apache 網站伺服器配合使用，則必須在安裝 Sun Crypto Accelerator 4000 軟體前，先安裝編號為 109234-09 的修正程式。此修正程式可在產品 CD 的 patches 子目錄中找到，也可到 <http://sunsolve.sun.com> 下載。

注意 – 套用此修正程式後，您必須**先**重新啟動系統，然後再安裝 Sun Crypto Accelerator 4000 軟體。

Apache 網站伺服器不能設定為同時與 *Sun Crypto Accelerator 1000* 和 *Sun Crypto Accelerator 4000* 介面卡配合使用。如果將這兩個介面卡設定為同時使用 Apache 網站伺服器，Apache 將無法正常工作。

請僅在計劃將此介面卡與 Apache Web Server 1.3.26 配合使用時，才安裝 Sun Crypto Accelerator 4000 SUNWkcl2a 軟體套件。如果計劃使用任何其他 Apache 網站伺服器組態或版本，請勿安裝 SUNWkcl2a 套件。

啓動檔

對 Apache (/etc/rc3.d/S50apache) 與 dtlogin (/etc/rc2.d/S99dtlogin) 的啓動檔進行排序，可能會在機器啓動時導致排序問題。這可能會導致在啓動時無法存取主控台以輸入 Apache 密碼。

解決方法：以 root 身份登入並發出下列指令，以重新排序 Apache 網站伺服器的啓動檔：

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