Sun™ Crypto Accelerator 4000 介面卡 1.1 版版本說明

Sun Microsystems, Inc.
www.sun.com

文件號碼 817-5933-10
2004 年 1 月，修訂版 A

請在 http://www.sun.com/hwdocs/feedback 上提交有關此文件的意見

請回收

Adobe PostScript

Sun Crypto Accelerator 4000 介面卡 1.1 版版本說明

這些版本說明將說明 Sun Crypto Accelerator 4000 介面卡的已知問題。要獲得此文件的最新版本及最新的已知問題，請參閱：

```
http://www.sun.com/products-n-solutions/hardware/docs/Network_Connectivity/
Crypto_Boards/index.html
```

要獲得最新修正程式、更新及要求，請瀏覽產品網站：

```
http://www.sun.com/products/networking/sslaccel/suncryptoaccel4000/
```

此文件中列出的修正程式可在下列網站取得：`http://sunsolve.sun.com/`。Solaris 更新版包含早期版本的修正程式。使用 `showrev -p` 指令來得知哪些所需的修正程式已經被安裝過了。

請安裝最新版本的修正程式。修正程式每推出一個新的版本，編號尾數 (例如：-01) 也會跟著增加。如果網站上的版本編號比此文件更高，則屬較新版本。

如果在 SunSolve℠ 網站上找不到所需的修正程式，請與當地的業務代表聯絡。

Sun Crypto Accelerator 4000 軟體的已知問題

Sun Fire 15K 支援問題

用於動態重新配置 (DR) 支援的 Sun Fire 15K 平台需要下列修正程式：

- 對於 Solaris 8，請安裝修正程式 110900-10 與修正程式 110824-04
- 對於 Solaris 9，請安裝修正程式 113068-04 與修正程式 112838-08

Sun Fire 15K 平台上的十億位元效能

下列修正程式可加強 Sun Fire 15K 平台上十億位元速度的介面卡效能。

- 對於 Solaris 9，請安裝修正程式 113218-08
- 對於 Solaris 9，請安裝修正程式 112904-08
- 對於 Solaris 9，請安裝修正程式 112233-08

Sun Fire 15K 平台的插槽要求

Sun Crypto Accelerator 4000 介面卡在 Sun Fire 15K 平台上僅支援於 66 MHz 插槽中。

Sun ONE Application Server 7 的評估版本

用於安裝應用程式伺服器軟體的 `iplssl cfg` 指令碼，與 Sun ONE Application Server 7 的評估版本不相容。此指令碼與其他版本皆可配合使用。使用 `modutil` 指令安裝應用程式伺服器的評估版本。

vcaadm 鎖定檔案

vcaadm 鎖定檔案 (.trustlock) 用於防止覆寫兩個 vcaadm 程序間的變更。如果 vcaadm 公用程式沒有正確關閉，此鎖定檔案可能會阻止存取信任資料庫。如果出現此問題，您將接收到下列錯誤訊息：

```
Lock file prevented read access to trust DB: Timer expired
```

解決方法：刪除 ${HOME}/.vcaadm 目錄中的 .trustlock 鎖定檔案。

```
# rm ${HOME}/.vcaadm/.trustlock
```

錯誤 ID 4948204 pcicfg 在成功執行 FCODE 後不得再次測試 BAR

如果在解讀 FCODE 後 pcicfg 公用程式再次測試基底位址暫存器 (BAR)，則可能會配置給 BAR 錯誤數目的位址空間。如果配置的位址空間少於 FCODE 要求的空間，busra 公用程式將偵測到錯誤的自由呼叫並在取消配置程序時無法操作。

- 對於 Solaris 9，請安裝修正程式 112838-08
- 對於 Solaris 8，請安裝修正程式 110900-10

錯誤 ID 4922816 Outbound IPsec 可能無法卸載

如果硬體較安全關聯 (SA) 爲新，Outbound IPsec 將不會卸載。如果 Sun Crypto Accelerator 4000 介面卡使用現有 SA 以配置於嵌入式 IPsec 加速的系統中，安全關聯資料庫 (SADB) 必須重新載入以使用現有 SA。重新啓動系統或使用 ipseckey 公用程式可執行重新載入。請參閱 *IPsec and IKE Administration Guide* 以取得有關如何使用 ipseckey 公用程式的資訊。

錯誤 ID 4979555 vca 初始化失敗

在某些系統中初始化 vca 驅動程式時，下列警告訊息可能會寫入訊息記錄中：

```
WARNING: vca0: Unknown pci device(0x582114e4) found on bus 1, slot 0
vca0: PCI initialization failed, retry ...
```

這些訊息表示在 Sun Crypto Accelerator 4000 介面卡上初始掃描內部 PCI 匯流排失敗，亦表示後續重新掃描 (重新嘗試) 成功。如果重新掃描失敗，這些訊息後將出現其他資訊，但這些初始訊息不表示介面卡上的故障。

錯誤 ID 4721396 vca 記憶體滲漏

Sun Crypto Accelerator 4000 驅動程式 vca 可能會導致核心記憶體滲漏。在 Solaris 軟體中更正此錯誤前，此錯誤的解決辦法是提供 vca.conf 變數作爲手動解決方法。

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。

- 對於 Solaris 9，請安裝修正程式 113218-08

錯誤 ID 4762081 匯流排速度偵測

在電源開啓時匯流排速度偵測可能以不正確順序出現。

- 對於 Solaris 9，請安裝修正程式 113068-04
- 對於 Solaris 8，請安裝修正程式 110842-11

錯誤 ID 4698278 動態重新配置

Sun Fire™ V880 伺服器上的 Sun Crypto Accelerator 4000 介面卡 DR 可能會偶然導致系統故障。

此問題會在 DR 的連接位相時出現。此外，有時介面卡可能會標識爲 unknown(ㄔㄋㄓ)。33 MHz 與 66 MHz 插槽都會受到影響。

- 對於 Solaris 9，請安裝修正程式 113068-04
- 對於 Solaris 8，請安裝修正程式 110842-11

錯誤 ID 4718370 使用熱插入設定 PCI 卡時的故障

I/O 空間、記憶體空間及主要匯流排均啓用，即使 PCI 配置空間中的所有暫存器均未初始化。此外，某 PCI 記憶體位址指派至兩個資源而導致故障。

基底位址暫存器 (BAR) 將在重新啓動插槽後保留其值，而系統軟體在開啓 I/O 與記憶體存取前，需要初始化 BAR。

- 對於 Solaris 9，請安裝修正程式 112838-08
- 對於 Solaris 8，請安裝修正程式 110824-04 與修正程式 110900-10

錯誤 ID 4847585 次要節點名稱發生衝突

透過建立兩個次要節點，一個名爲 `fred` 支援 Style 2，另一個名爲 `fred0` 支援 Style 1，網路驅動程式實例 (例如：`fred`) 可支援 DLPI Style 1 與 Style 2 介面。

`ip_rcm` 模組不支援此次要節點命名慣例，並且可能嘗試兩次設定或取消設定 `fred0`，雖然 IP 僅需要套用 Style 1 或 Style 2 介面之一而非兩者皆套用。

解決方法：請勿建立衝突的次要節點—例如：`fred` 與 `fred0`，其中驅動程式 `fred` 的實例號碼爲零。

- 對於 Solaris 9，請安裝修正程式 114758-01
- 對於 Solaris 8，請安裝修正程式 110839-04

錯誤 ID 4836686 DLPI 供應器名稱

爲 Style 1 DLPI 供應器建構「exported」名稱時，`network_rcm.c` 模組可能會使用「name」OBP 屬性。這使得匯出名稱的形式爲 `network0` 而非 `vca0`。

- 對於 Solaris 9，請安裝修正程式 114758-01
- 對於 Solaris 8，請安裝修正程式 110839-04

錯誤 ID 4470196 需要 Solaris 8 修正程式

對於 Solaris 8，您必須在安裝 Sun Crypto Accelerator 4000 軟體之前，先安裝修正程式 112438-01 與修正程式 109234-09。這些修正程式可在產品 CD 的 `patches` 子目錄中找到，也可自 `http://sunsolve.sun.com` 下載。

注意 – 套用這些修正程式後，您必須***先***重新啓動系統，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 版本則隨附此工具。

注意 – Sun ONE Web 伺服器之前稱爲 iPlanet™ Web 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 4836099 無回返纜線的 SunVTS `netlbtest` 內部故障

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

```
"
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.
```

可以忽略這些訊息。

解決方法：使用附加的回返纜線進行 SunVTS 內部迴路測試。

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，該程式會顯示下列應忽略的不相關訊息：

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

Error writing data: Bad file number
```

錯誤 ID 4816009 啓用 FIPS 模式

在介面卡積極執行操作時，如果安全管理員自主地於未初始化的介面卡上啓用 FIPS 模式，介面卡可能會當機。

解決方法：請勿將處於 FIPS 模式下的介面卡歸零，也不要在對介面卡送出加密要求時爲 FIPS 模式初始化介面卡。

RFE ID 4753295

根據預設值，供 Apache Web 伺服器軟體使用的大量加密功能已啓用，您無法停用此功能。對於 Sun ONE 伺服器軟體，大量加密功能預設爲停用，您必須建立空白檔案 (/etc/opt/SUNWconn/cryptov2/sslreg) 並重新啓動 Sun ONE 伺服器軟體以手動啓用此功能。在爲 Sun ONE 伺服器軟體啓用大量加密功能時，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爲 Sun ONE 伺服器軟體啓用大量加密功能。

錯誤 ID 4822356 使用 vcaadm 更新主金鑰

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加密作業，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。

錯誤 ID 4757594 vca.conf 變數

在 Solaris 軟體中更正此錯誤前，此錯誤的解決辦法是提供 vca.conf 變數作爲手動解決方法。該錯誤在 Solaris 9 4/03 中已經解決。

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。

- 對於 Solaris 9 4/03 之前的 Solaris 版本，請安裝修正程式 112233-08
- 對於 Solaris 8，請安裝修正程式 108528-23

Sun ONE Web 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 Web 伺服器目前不在執行中，則會出現許多要求輸入記號密碼的對話方塊之狀況。如果使用相當大的字型，或有許多記號 (因此會有許多「Enter password:」指令行)，面板下方的按鈕會因爲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」(接受) 按鈕提交變更。

此問題有兩種解決方法：

- 先從指令行啓動 Web 伺服器，或先將 GUI Preference 設定爲 On/Off，再從管理視窗啓動 Web 伺服器。
- 套用配置但不啓動伺服器：套用 → 載入配置檔案。

錯誤 ID 4532941 與 4593111 多個金鑰庫

在存在多個金鑰庫的配置下工作時，Sun ONE Web 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：爲所有 Web 伺服器實例只設定一個金鑰庫。然後，您可以爲每個 Web 伺服器實例設定不同的金鑰庫使用者。這將使每個 Web 伺服器實例的金鑰相互獨立。

錯誤 ID 4620283 pk12util 公用程式

Sun ONE 提供 pk12util 公用程式從內部軟體資料庫匯出認證與金鑰，並自外部硬體資料庫匯入。但是，pk12util 公用程式無法從外部硬體資料庫匯出認證或金鑰，例如：Sun Crypto Accelerator 介面卡：

```
% 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.
```

解決方法：使用 pk11export 公用程式從介面卡擷取金鑰。請參閱 *Sun Crypto Accelerator 4000 介面卡 1.1 版安裝及使用者指南*以取得詳細資料。

錯誤 ID 4607112 密碼預設值

在設定 Sun ONE Web Server 6.0 過程中，如果在依次選擇 Chiper Default (密碼預設值) 設定、憑證、OK (確定) 按鈕及右上角的 Apply (套用) 連結以套用密碼後，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。

此爲正確啓動裝有 Sun Crypto Accelerator 4000 介面卡的 Web 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 cipher 或 SSL3 cipher
2. 選擇 OK (確定)
3. 選擇 Apply (套用)
4. 選擇 Load Configuration (載入配置)

如果您已執行這些步驟，但 Web 伺服器仍無法正確啓動，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". . .
```

- 重新啓動 Web 伺服器。

支援的 Apache Web 伺服器版本

此 Sun Crypto Accelerator 4000 軟體版本支援 Apache 1.3.26。

Apache Web 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 下與 Apache Web 伺服器配合使用，則必須在安裝 Sun Crypto Accelerator 4000 軟體前，先安裝修正程式 109234-09。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***重新啓動系統，然後再安裝 Sun Crypto Accelerator 4000 軟體。

Apache Web 伺服器不能設定爲同時與 *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同時設定爲使用 Apache Web 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 Web 伺服器配置或版本，請勿安裝 SUNWkcl2a 套件。

啓動檔

Apache (`/etc/rc3.d/S50apache`) 與 `dtlogin` (`/etc/rc2.d/S99dtlogin`) 的啓動檔順序可能會在機器啓動時導致順序問題。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 Web 伺服器的啓動檔：

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