Guide de l'utilisateur et d'installation de la carte Crypto Accelerator 1000 de Sun™

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

Référence n° 816-4566-10
mars 2002, révision A

Envoyez vos commentaires concernant ce document à l'adresse : docfeedback@sun.com

Produit
recyclable

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.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

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

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

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

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。

Table des matières

Tableaux

Préface

Le *Guide de l'utilisateur et d'installation de la carte Crypto Accelerator 1000 de Sun* décrit les caractéristiques de la carte Crypto Accelerator 1000 de Sun™ ainsi que son installation et utilisation sur votre système.

Ce guide est conçu pour les administrateurs système familiarisés avec l'environnement d'exploitation Solaris.

Utilisation des commandes UNIX

Ce document ne contient pas d'informations sur les commandes et procédures de base UNIX®, telles que l'arrêt du système, l'amorçage du système ou la configuration des périphériques.

Pour plus d'informations, consultez la documentation suivante :

- *Guide de la plate-forme matérielle Solaris*
- Documentation en ligne AnswerBook2™ pour l'environnement d'exploitation Solaris™
- Toute autre documentation sur les logiciels livrée avec votre système

Conventions typographiques

Police	Signification	Exemples
`AaBbCc123`	Noms de commandes, fichiers et répertoires. Messages apparaissant à l'écran.	Modifiez votre fichier `.login`. Utilisez `ls -a` pour afficher la liste de tous les fichiers. `% Vous avez reçu du courrier.`
`AaBbCc123`	Ce que l'utilisateur tape par opposition aux messages apparaissant à l'écran.	`% su` `Password:`
AaBbCc123	Titres de guide, nouveaux mots ou termes, mots à mettre en valeur.	Consultez le chapitre 6 du *Guide de l'utilisateur.* Il s'agit d'options de *catégorie*. Vous *devez* être superutilisateur pour effectuer cette opération.
	Variable de ligne de commande, à remplacer par une valeur ou un nom réel.	Pour supprimer un fichier, entrez `rm` *nomfichier.*

Invites Shell

Shell	Invite
C shell	*nom_machine*%
C shell superutilisateur	*nom_machine*#
Bourne shell et Korn shell	$
Bourne shell et Korn shell superutilisateur	#

Accès à la documentation de Sun en ligne

Vous trouverez un grand choix de documentation sur les systèmes Sun à l'adresse suivante :

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

Vous trouverez une documentation exhaustive sur Solaris, ainsi que d'autres ouvrages, à l'adresse :

`http://docs.sun.com`

Vos commentaires sont les bienvenus chez Sun

Dans le souci d’améliorer notre documentation, tous vos commentaires et suggestions sont les bienvenus. N’hésitez pas à nous les faire parvenir à l’adresse suivante :

`docfeedback@sun.com`

Mentionnez le numéro de référence (816-4566-10) de votre documentation dans l’objet de votre message électronique.

CHAPITRE 1

Présentation du produit

Ce chapitre décrit la carte Crypto Accelerator 1000 de Sun.

Ce chapitre comprend les sections suivantes :

Présentation du matériel

La carte Crypto Accelerator 1000 de Sun est une petite carte PCI qui fonctionne de la même manière qu'un co-processeur cryptographique, pour accélérer la cryptographie symétrique et de clés publiques. Ce produit ne comporte aucune interface externe. La carte communique avec l'hôte par l'interface du bus PCI interne. Cette carte a été conçue dans le but d'accélérer tout un ensemble d'algorithmes cryptographiques sollicitant des calculs à très hautes vitesses, pour des protocoles de sécurité, destinés aux applications eCommerce.

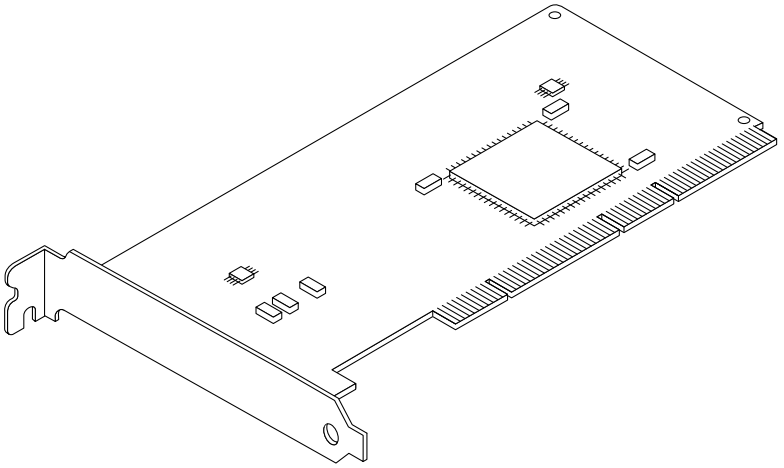


FIGURE 1-1 Carte Crypto Accelerator 1000 de Sun

Caractéristiques du produit

La carte Crypto Accelerator 1000 de Sun est une carte d'accélération cryptographique permettant d'optimiser les performances de SSL sur les plates-formes Sun. Elle permet d'accélérer les algorithmes cryptographiques du matériel aussi bien que du logiciel. Des coûts d'accélération des algorithmes cryptographiques différents pour chaque algorithme expliquent la complexité de leurs caractéristiques. Certains algorithmes cryptographiques ont été spécialement conçus pour être implémentés sur du matériel, d'autres sur du logiciel. De plus, une accélération matérielle implique un coût élevé pour le déplacement de données, de l'espace d'application de l'utilisateur vers le périphérique d'accélération matérielle, puis le ré-acheminement des résultats vers l'application de l'utilisateur.

Notez que quelques algorithmes cryptographiques (par exemple, ARCFOUR) peuvent être traités par un logiciel hautement optimisé, aussi rapidement que par du matériel dédié. La carte Crypto Accelerator 1000 de Sun examine chaque requête cryptographique et détermine le meilleur emplacement pour l'accélérateur (processeur hôte ou carte Crypto Accelerator 1000 de Sun), afin de parvenir à un débit maximum. La distribution des charges est basée sur un algorithme cryptographique, sur le chargement en cours et sur la taille des données.

Le TABLEAU 1-1 indique quels algorithmes accélérés peuvent être délégués au matériel et quels algorithmes logiciels sont fournis pour les serveurs Web iPlanet et Apache.

TABLEAU 1-1 Algorithmes SSL pris en charge

	Serveurs Web IPlanet		Serveurs Web Apache	
Algorithme	**Matériel**	**Logiciel**	**Matériel**	**Logiciel**
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

Prise en compte de la fonctionnalité Dynamic Reconfiguration et de la caractéristique High Availability

Le matériel Crypto Accelerator 1000 de Sun et le logiciel associé fournissent une capacité de fonctionnement efficace sur les plates-formes Sun et permettent une prise en charge de la fonctionnalité Dynamic Reconfiguration (DR) et des connexions à chaud. Dans le cas où une opération de DR ou de connexion à chaud est réalisée, la couche logicielle de Crypto Accelerator 1000 de Sun détecte automatiquement l'ajout ou la suppression d'une carte et règle les algorithmes de programmation en fonction des ressources matérielles.

Pour les configurations High Availability (HA), plusieurs cartes Crypto Accelerator 1000 de Sun peuvent être installées dans un système ou un domaine, afin de garantir la disponibilité constante de l'accélération matérielle. Dans le cas peu probable d'une panne du matériel Crypto Accelerator 1000 de Sun, la couche logicielle détecte la panne et supprime la carte concernée de la liste des accélérateurs cryptographiques matériels disponibles. Le logiciel Crypto Accelerator 1000 de Sun règle les algorithmes de programmation en fonction de la réduction des ressources matérielles. Les requêtes cryptographiques suivantes seront programmées sur les cartes restantes.

De plus, les bibliothèques du logiciel Crypto Accelerator 1000 de Sun permettent d'effectuer toutes les opérations cryptographiques dans le logiciel, comme la suppression des DR et des connexions à chaud de toutes les cartes Crypto Accelerator 1000 de Sun, au sein d'un domaine de système, sans provoquer de

dysfonctionnement. Cependant, il faudra prévoir une perte de performance significative, jusqu'à ce que la configuration du matériel Crypto Accelerator 1000 de Sun soit restaurée.

Notez que le matériel Crypto Accelerator 1000 de Sun fournit une source d'entropie de haute qualité pour la création de clés de longue durée. Si toutes les cartes Crypto Accelerator 1000 de Sun au sein d'un même domaine ou système sont supprimées, les clés de longue durée sont créées avec une entropie de qualité plus faible.

Partage de charges

Le logiciel Crypto Accelerator 1000 de Sun répartie les charges sur toutes les cartes installées sur le domaine ou le système Solaris. Les requêtes cryptographiques entrantes sont réparties sur les cartes, sur la base de files d'attente de longueurs fixes. Les requêtes sont mises en attente sur la première carte disponible pouvant accepter le type de requête en question. Le mécanisme de mise en attente a été conçu pour optimiser le débit en simplifiant le regroupement des requêtes sur une carte.

Conditions logicielles et matérielles requises

Le TABLEAU 1-2 résume les conditions logicielles et matérielles requises pour la carte Crypto Accelerator 1000 de Sun.

TABLEAU 1-2 Conditions logicielles et matérielles requises

Matériel et logiciel	Conditions requises
Matériel	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

TABLEAU 1-2 Conditions logicielles et matérielles requises

Matériel et logiciel	Conditions requises
Environnement d'exploitation	Solaris 8 7/01 ou une version ultérieure compatible
Emplacements PCI	32 ou 64 bits 33 ou 66 MHz
Logiciel	Serveur Web iPlanet™ 4.1 SP9, 6.0 SP1 ou Serveur Web Apache 1.3.12 Tout correctif requis pour le démarrage des serveurs Web iPlanet ou Apache

Remarque – Les numéros du service pack (SP9 ou SP1) sont indiqués toutes les fois que le serveur Web iPlanet 4.1 ou 6.0 est mentionné.

Correctifs requis

Les correctifs suivants sont requis pour le démarrage du logiciel Crypto Accelerator 1000 de Sun sur votre système. Les mises à jour de Solaris comportent les correctifs des versions précédentes. Utilisez la commande `showrev -p` pour déterminer si les correctifs énumérés ont déjà été installés.

Vous pouvez, le cas échéant, télécharger les correctifs à partir du site Web suivant : `http://sunsolve.sun.com`.

Installez la dernière version des correctifs. Le numéro comportant un tiret (-01, par exemple) augmente à chaque nouvelle version du correctif. Si le numéro de version sur le site Web est supérieur à celui indiqué dans les tableaux suivants, il s'agit tout simplement d'une version ultérieure.

Si le correctif dont vous avez besoin n'est pas disponible sur SunSolve℠, contactez votre vendeur ou votre service d'assistance local.

Les tableaux suivants répertorient les correctifs requis et recommandés pour l'utilisation avec ce produit. Le TABLEAU 1-3 répertorie et décrit les correctifs requis.

TABLEAU 1-3 Correctifs requis pour le logiciel Crypto Accelerator 1000 de Sun

Numéro de correctif	Description
110383-01	`libnvpair`
108528-05	`KU-05` (prise en charge `nvpair`)
112438-01	`/dev/random`

Remarque – Si vous envisagez d'utiliser le serveur Web Apache 1.3.12, vous devez également installer le correctif 109234-02.

Le TABLEAU 1-4 répertorie et décrit les correctifs recommandés.

TABLEAU 1-4 Correctifs recommandés pour le logiciel Crypto Accelerator 1000 de Sun

Numéro de correctif	Description
108528-13	`KU-13` (corrections relatives à la sécurité `nvpair`)

CHAPITRE **2**

Installation et suppression de la carte Crypto Accelerator 1000 de Sun

Ce chapitre décrit les procédures d'installation logicielle et matérielle de la carte Crypto Accelerator 1000 de Sun.

Ce chapitre comporte les sections suivantes :

Manipulation de la carte

Chaque carte est emballée dans un sachet antistatique spécial par soucis de protection lors de l'expédition et du stockage. Pour éviter d'endommager les composants de la carte sensibles à l'électricité statique, réduisez l'électricité statique présente sur vous avant de toucher la carte. Vous pouvez utiliser l'une de ces méthodes :

- Touchez la partie métallique de l'ordinateur.
- Fixez un bracelet antistatique à votre poignet et à une surface métallique mise à la terre.

Attention – Pour éviter d'endommager les composants de la carte sensibles à l'électricité statique, portez un bracelet antistatique pendant la manipulation de la carte, tenez-la par les bords uniquement et placez-la toujours sur une surface antistatique (comme le sachet en plastique qui la contenait).

Installation de la carte

L'installation de la carte Crypto Accelerator 1000 de Sun implique son insertion dans le système et le chargement des outils logiciels. Les instructions d'installation matérielle comportent uniquement des étapes générales à suivre pour l'installation de la carte. Reportez-vous à la documentation fournie avec votre système pour connaître les instructions d'installation spécifiques.

▼ Pour installer le matériel

1. **En tant que superutilisateur, suivez les instructions fournies avec votre système pour éteindre et mettre votre ordinateur hors tension, déconnecter le cordon d'alimentation et retirer le couvercle de l'ordinateur.**
2. **Recherchez un emplacement PCI disponible (de préférence un emplacement de 64 bits, 66 MHz).**
3. **Fixez un bracelet antistatique à votre poignet et à une surface métallique mise à la terre.**
4. **A l'aide d'un tournevis Phillips, retirez la vis du couvercle de l'emplacement PCI.**

   Mettez-la de côté pour tenir le support à l'étape 5.
5. **En tenant la carte Crypto Accelerator 1000 de Sun par le bord uniquement, retirez-la de son emballage et insérez-la dans l'emplacement PCI. Fixez ensuite la vis à l'arrière du support.**
6. **Replacez le couvercle de l'ordinateur, reconnectez le cordon d'alimentation et mettez le système sous tension.**
7. **Assurez-vous que la carte est correctement installée en exécutant la commande `show-devs` à partir de l'invite `ok` :**

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

Les lignes `/pci@1f,2000/pci108e,5455@`*n* indiquent que la carte est installée et reconnue par le système.

Installation du logiciel Crypto Accelerator 1000 de Sun

Le logiciel Crypto Accelerator 1000 de Sun est compris dans le CD *Crypto Accelerator 1000 de Sun*. Vous devrez peut-être télécharger des correctifs à partir du site Web SunSolve. Voir la section « Correctifs requis », page 5 pour plus d'informations.

▼ Pour installer le logiciel

1. **Insérez le CD** *Crypto Accelerator 1000 de Sun* **dans le lecteur de CD-ROM connecté à votre système.**
   - Si votre système exécute Sun Enterprise Volume Manager™, il mettra le CD-ROM automatiquement en place dans le répertoire `/cdrom/cdrom0`.
   - S'il ne l'exécute pas, mettez le CD-ROM en place de cette manière :

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

Les fichiers et répertoires suivants seront alors affichés dans le répertoire `/cdrom/cdrom0`.

Fichier ou répertoire	Contenu	
`Copyright`	Fichier de copyright américain	
`FR_Copyright`	Fichier de copyright français	
`Docs`	Guide de l'utilisateur et d'installation de la carte Crypto Accelerator 1000 de Sun	
`Packages`	Comporte les progiciels Crypto Accelerator 1000 de Sun :	
	`SUNWcrypr`	composants du noyau de cryptographie
	`SUNWcrypu`	bibliothèques et utilitaire d'administration cryptographique
	`SUNWcrysu`	prise en charge SSL pour Apache (facultatif)
	`SUNWcrypm`	pages manuel d'administration cryptographique
	`SUNWdcar`	accélérateur cryptographique DCA (racine)
	`SUNWdcamn`	page manuel de l'accélérateur cryptographique DCA
	`SUNWdcav`	test SunVTS de l'accélérateur cryptographique DCA (facultatif)
	`SUNWcrysl`	outils et bibliothèques de développement SSL pour Apache (facultatif)

Installez le progiciel `SUNWcrysu` uniquement si vous envisagez d'utiliser Apache comme votre serveur Web.

Installez le progiciel `SUNWcrysl` uniquement si vous envisagez de vous relier à une autre version (non prise en charge) du serveur Web Apache.

Installez le progiciel `SUNWdcav` uniquement si vous envisagez d'effectuer les tests SunVTS™. Pour installer le progiciel `SUNWdcav`, vous devez d'abord installer SunVTS 4.4, 4.5 ou 4.6

2. **Installez les progiciels en saisissant :**

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

3. **Pour vous assurer que le logiciel a été installé correctement, exécutez la commande** `pkginfo`.

```
# 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. **(Facultatif) Pour vous assurer que le pilote est relié, exécutez la commande** `prtconf`.

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

5. **(Facultatif) Exécutez la commande** `modinfo` **pour vérifier que les modules sont chargés.**

```
# 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)
```

Cependant, il se peut que `kcl` et `cryptio` ne soient pas chargés ou n'apparaissent pas, jusqu'à ce que vous utilisiez la carte Crypto Accelerator 1000 de Sun, pour effectuer des cryptographies.

Répertoires et fichiers

Le TABLEAU 2-1 indique les répertoires créés après l'installation par défaut du logiciel Crypto Accelerator 1000 de Sun.

TABLEAU 2-1 Répertoires Crypto Accelerator 1000 de Sun

Répertoire	Contenu
`/etc/opt/SUNWconn/crypto/realms`	Domaine et données de l'utilisateur
`/opt/SUNWconn/crypto/bin`	Exécutables d'application
`/opt/SUNWconn/crypto/lib`	Bibliothèques d'application
`/opt/SUNWconn/crypto/sbin`	Exécutables liés statiquement

La FIGURE 2-1 indique l'ordre hiérarchique des répertoires et fichiers.

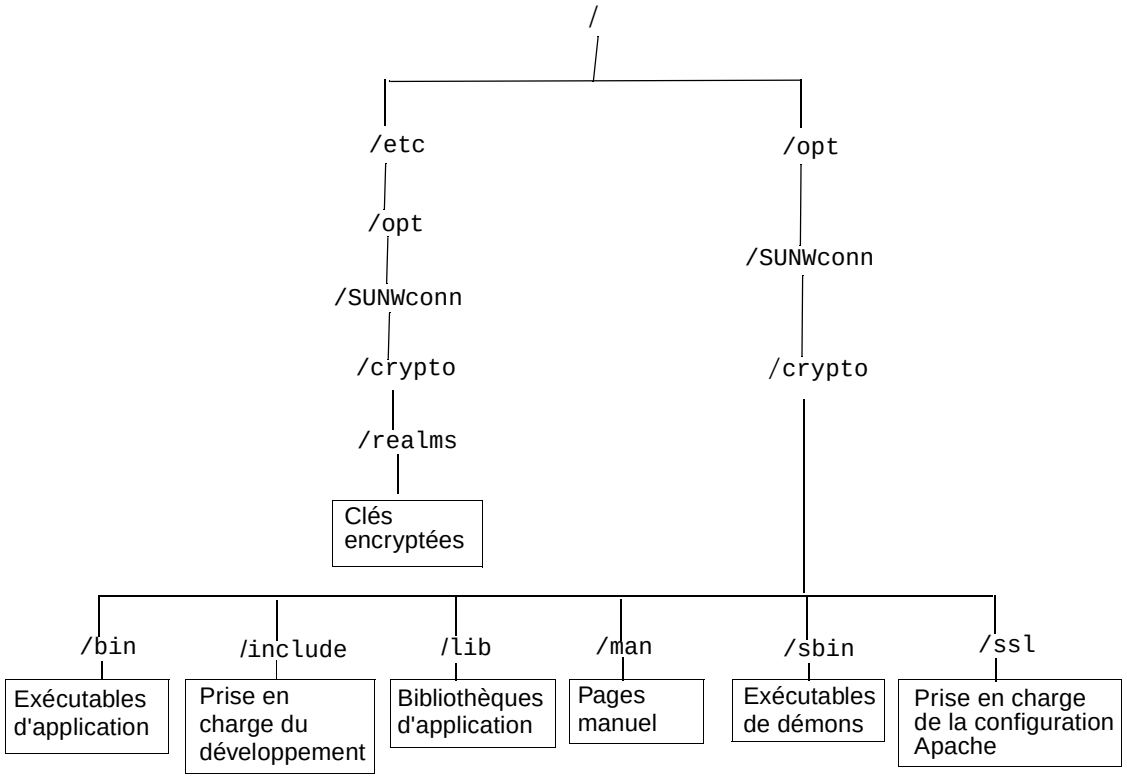


FIGURE 2-1 Répertoires et fichiers du logiciel Crypto Accelerator 1000 de Sun

Désinstallation du logiciel

Si vous avez créé des domaines, vous devez les supprimer avant de désinstaller le logiciel. Si vous n'avez créé aucun domaine, vous pouvez ignorer les procédures suivantes. Vous ne pouvez pas supprimer un domaine qui est en cours d'utilisation. Pour supprimer des références dans les domaines, vous devrez peut-être arrêter le serveur Web et/ou le serveur d'administration.

Attention – Avant de désinstaller le logiciel Crypto Accelerator 1000 de Sun, vous devez désactiver tous les serveurs Web activés pour l'utilisation de la carte Crypto Accelerator 1000 de Sun. Si vous ne prenez pas cette précaution, les serveurs Web concernés ne fonctionneront plus.

▼ Pour supprimer les domaines

1. **Accédez à l'utilitaire `secadm` en tant que superutilisateur :**

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

2. **Utilisez l'utilitaire `secadm` pour supprimer chaque domaine.**

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

Toutes les données de domaine spécifiques à tous les sites sont alors supprimées, y compris les clés matérielles.

▼ Pour désinstaller le logiciel

- **En tant que superutilisateur, utilisez la commande `pkgrm` pour désinstaller uniquement les progiciels que vous avez installés.**

  Les progiciels installés doivent être désinstallés dans l'ordre indiqué ci-dessous. Si vous omettez de les désinstaller dans cet ordre, il se peut que vous fassiez l'objet de mises en garde relatives à l'interdépendance des éléments et que les modules du noyau soient toujours chargés.

  Si vous avez installé tous les progiciels, désinstallez-les comme suit :

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

Remarque – Après l'installation ou la désinstallation du test SunVTS pour le logiciel Crypto Accelerator 1000 de Sun (`SUNWdcav`), si SunVTS est déjà en cours d'exécution, il se peut que SunVTS doive re-tester le système pour mettre à jour les tests disponibles. Pour plus d'informations, consultez votre documentation SunVTS.

CHAPITRE 3

Activation de la carte pour les serveurs Web iPlanet

Ce chapitre indique comment activer la carte Crypto Accelerator 1000 de Sun pour l'utiliser avec les serveurs Web iPlanet.

Ce chapitre comporte les sections suivantes :

Mots de passe

Vous devrez entrer plusieurs mots de passe au cours de l'activation d'un serveur Web iPlanet (iWS). Le TABLEAU 3-1 décrit chaque mot de passe. Il sera fait référence à ces mots de passe au cours de ce chapitre. Si vous ne savez pas quel mot de passe utiliser, reportez-vous au TABLEAU 3-1.

TABLEAU 3-1 Mots de passe requis pour les serveurs Web iPlanet

Type de mot de passe	Description
Serveur d'administration iWS	Requis pour démarrer le serveur d'administration iPlanet. Ce mot de passe a été affecté lors de la configuration de iPlanet.
Base de données de certification de serveur Web	Requis pour démarrer les modules cryptographiques internes lors de l'exécution en mode sécurisé, lorsqu'un certificat est requis et lorsque le certificat est installé. Dans le serveur Web iPlanet ce mot de passe est également appelé mot de passe de fichier de paires de clés et mot de passe interne du module.
Administrateur système	Requis lors de l'exécution d'opérations privilégiées `secadm`. Il s'agit du mot de passe de l'hôte UNIX.
user@realm-name (utilisateur@nom-domaine)	Requis pour le démarrage du module Crypto Accelator 1000 de Sun lors de l'exécution en mode sécurisé. Ce mot de passe a été affecté lors de la création d'un utilisateur pour un domaine avec `secadm.`

Création et remplissage d'un domaine

Avant de pouvoir activer la carte pour une utilisation avec les serveurs Web iPlanet, vous devez tout d'abord configurer et remplir les domaines. Si ce n'est pas déjà fait, vous devez configurer au minimum un domaine et un utilisateur. Voir l'annexe A pour plus d'informations sur les domaines.

▼ Pour créer et remplir un domaine

1. **Placez le répertoire des outils Crypto Accelerator 1000 de Sun dans votre chemin de recherche, si vous ne l'avez pas déjà fait. Par exemple :**

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

2. **Accédez à l'utilitaire `secadm` :**

```
$ secadm
```

3. **Utilisez l'utilitaire `secadm` pour créer un nouveau domaine :**

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

4. **Remplissez les domaines avec les utilisateurs.**

   Ces noms d'utilisateurs sont connus uniquement dans le domaine du logiciel Crypto Accelerator 1000 de Sun et ne doivent pas obligatoirement être identiques au nom d'utilisateur UNIX sous lequel le serveur Web s'exécute. Avant la création de l'utilisateur, rappelez-vous que vous devez tout d'abord configurer le domaine actuellement en cours d'utilisation et vous connecter en tant qu'administrateur système.

   Avant de créer les utilisateurs, vous devez configurer le domaine qui les accueillera.

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

   a. **S'il vous faut uniquement un utilisateur de domaine, vous pouvez éviter de configurer un fichier de jetons en utilisant le nom d'utilisateur « nobody ». (Voir la section « Fichiers de jetons », page 59 pour plus d'informations.)**

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

      Vous devez utiliser ce mot de passe lors de l'authentification au cours du démarrage d'un serveur Web. Il s'agit du mot de passe *user@realm-name*.

Attention – Vous devez vous souvenir du mot de passe que vous avez entré. Sans ce mot de passe, vous ne pourrez pas accéder à vos clés. Il est impossible de récupérer un mot de passe oublié.

5. **Quittez secadm.**

```
secadm> exit
```

Présentation de l'activation des serveurs Web iPlanet

Pour activer les serveurs Web iPlanet vous devez effectuer les procédures suivantes, qui sont expliquées en détails dans les deux chapitres suivants.

1. Installez le serveur Web iPlanet.
2. Créez une base de données de certification.
3. Demandez un certificat.
4. Installez le certificat.
5. Configurez le serveur Web iPlanet.

Attention – Vous devez exécuter ces procédures dans l'ordre indiqué. Vous risquez sans cela d'obtenir une configuration incorrecte.

- Si vous utilisez le serveur Web iPlanet 4.1, allez au chapitre 4.
- Si vous utilisez le serveur Web iPlanet 6.0, allez au chapitre 5.

CHAPITRE 4

Installation et configuration d'un serveur Web iPlanet 4.1

Ce chapitre décrit l'installation et la configuration d'un serveur Web iPlanet 4.1

Ce chapitre comprend les sections suivantes :

Installation d'un serveur Web iPlanet 4.1

Les sections suivantes décrivent l'installation d'un serveur Web iPlanet 4.1. Vous devez suivre les procédures dans l'ordre indiqué. Reportez-vous à la documentation du serveur Web iPlanet pour plus d'informations sur les serveurs Web iPlanet.

▼ Pour installer un serveur Web iPlanet 4.1

1. **Installez le logiciel du serveur Web iPlanet 4.1.**

   Ce logiciel est disponible à l'adresse URL suivante :

   `http://www.iplanet.com`

2. **Installez le serveur Web.**

   Vous trouverez un exemple d'instructions mais vous pouvez choisir de configurer votre serveur Web différemment. Le nom du chemin par défaut du serveur est : `/usr/netscape/server4`

   Acceptez le chemin par défaut pendant l'installation du serveur Web iPlanet. Ce guide fait référence à ces chemins par défaut. Si vous décidez de l'installer à un emplacement différent, assurez-vous de noter l'emplacement.

3. **Lancez le programme de configuration.**

4. **Répondez aux invites du script d'installation.**

   Pour simplifier l'utilisation, vous pouvez accepter les paramètres par défaut, excepté pour les invites suivantes :

   a. **Acceptez les termes de la licence en saisissant** `oui`**.**

   b. **Entrez un** *hostname.domain* **(nomhôte.domaine) entièrement valide.**

   c. **Entrez le mot de passe du serveur d'administration iWS deux fois.**

   d. **A l'invite, appuyez sur Entrée.**

▼ Pour créer une base de données de certification

1. **Démarrez le serveur d'administration.**

   - Pour démarrer un serveur Web iPlanet 4.1, utilisez la commande suivante (au lieu d'exécuter `startconsole` comme requis lors de la configuration) :

```
# /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
```

   Un message de réponse vous indique l'URL auquel vous devez vous connecter pour administrer vos serveurs.

2. **Démarrez le serveur d'administration iPlanet en ouvrant un navigateur Web et en entrant :**

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

   Une fenêtre indépendante vous invite à entrer l'identificateur d'utilisateur et le mot de passe. Entrez le nom d'utilisateur du serveur d'administration iWS et le mot de passe choisis au cours de l'exécution de la configuration.

Remarque – Entrez le mot `admin` pour l'identificateur d'utilisateur ou le nom d'utilisateur du serveur d'administration iWS, si vous avez utilisé les paramètres par défaut lors de la configuration du serveur Web iPlanet.

3. **Cliquez sur OK.**

4. **Créez la base de données de certification pour les instances du serveur Web.**

   Vous voulez peut-être activer la sécurité sur plus d'une instance du serveur Web. Répétez cette opération pour chaque instance de serveur Web.

   Remarque – Si vous voulez exécuter SSL également sur le serveur d'administration, la configuration d'une base de données de certification est identique. Reportez-vous à la documentation iPlanet pour plus d'informations.

   a. **Cliquez sur l'onglet Servers (Serveurs) dans le serveur d'administration.**

   b. **Sélectionnez un serveur et cliquez sur le bouton Manage (Gestion).**

   c. **Cliquez sur l'onglet Security (Sécurité) sur la partie supérieure de la page et sélectionnez l'option Create database (Créer une base de données).**

   d. **Entrez un mot de passe (base de données de certification du serveur Web) dans les deux boîtes de dialogue et cliquez sur OK.**

      Choisissez un mot de passe de 8 caractères au minimum. Il s'agit du mot de passe utilisé pour lancer les modules cryptographiques internes lorsque le serveur Web iPlanet est exécuté en mode sécurisé.

5. **Exécutez le script suivant pour activer la carte Crypto Accelerator 1000 de Sun :**

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

   Ce script vous invite à choisir le serveur Web. Il permet d'installer les modules cryptographiques de la carte Crypto Accelerator 1000 de Sun pour les serveur Web iPlanet ou Apache. Puis, le script met à jour les fichiers de configuration pour activer la carte Crypto Accelerator 1000 de Sun.

6. **Entrez `1` pour configurer votre serveur Web iPlanet afin utiliser SSL, puis appuyez sur Entrée.**

```
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. **A l'invite, entrez le chemin du répertoire racine du serveur Web, puis appuyez sur Entrée.**

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

8. **A l'invite, entrez `y` et appuyez sur Entrée, si vous désirez poursuivre.**

```
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. **Entrez `0` pour quitter.**

▼ Pour créer un certificat de serveur

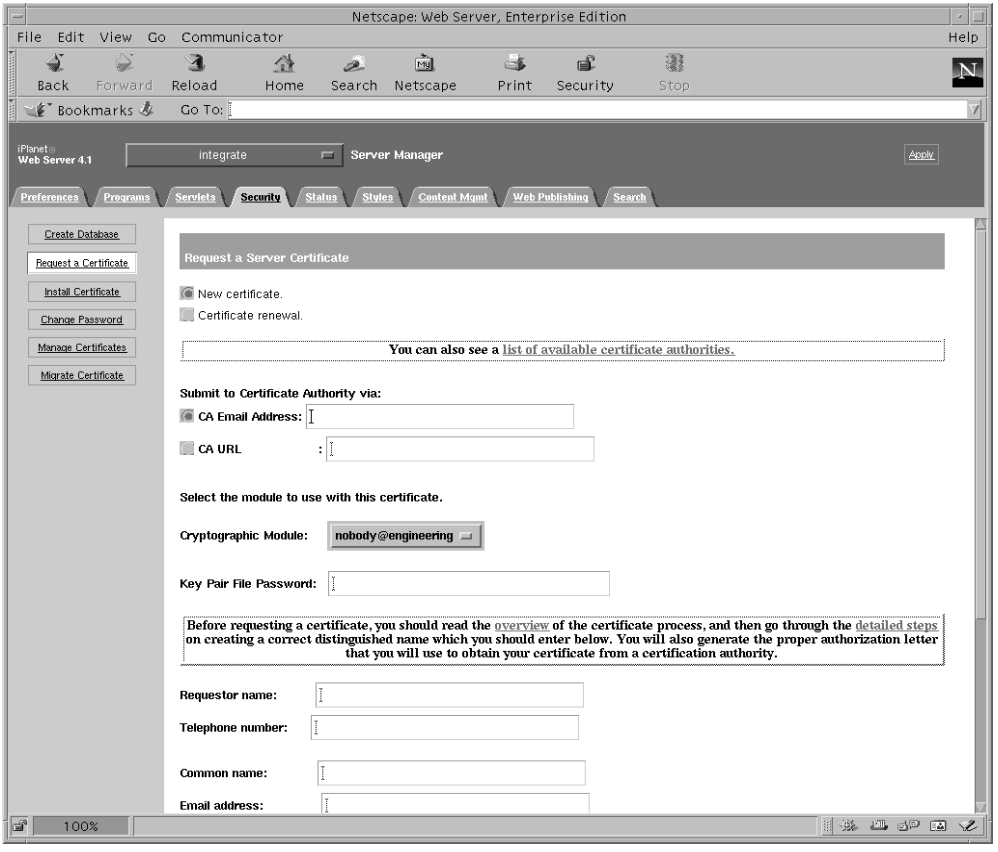
1. **Redémarrez le serveur Web d'administration en entrant les commandes suivantes :**

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

2. **Pour effectuer une demande de certificat de serveur, cliquez sur l'onglet Security (Sécurité) sur la partie supérieure de la page.**

   Le fenêtre Create Trust Database (Création de base de données de certification) s'affiche.

3. **Cliquez sur le lien Request Certificate (Demande de certificat) sur la partie gauche de la page.**



4. **Remplissez le formulaire pour créer une demande de certificat, à l'aide des informations suivantes :**

   a. **Sélectionner un nouveau certificat**

      Si vous pouvez envoyer directement votre demande de certificat à une autorité de certification ou d'enregistrement sur le Web, sélectionnez l'option CA URL (URL de l'autorité de certification). Dans le cas contraire, sélectionnez CA Email Address (Adresse e-mail de l'autorité de certification) et choisissez une adresse e-mail à laquelle vous voulez envoyer votre demande de certificat.

   b. **Sélectionnez le module cryptographique que vous voulez utiliser.**

      Chaque domaine dispose de sa propre entrée dans ce menu déroulant. Assurez-vous de sélectionner le domaine correct. Pour utiliser le Crypto Accelerator 1000 de Sun, vous devez sélectionner un module sous la forme de *user@realm-name*.

   c. **Dans la boîte de dialogue Key Pair File password (Mot de passe de fichier de paire de clés), entrez le mot de passe pour le *user@realm-name* qui sera en possession de la clé.**

   d. **Indiquez les informations appropriées pour les champs suivants :**

      - Requestor Name (Nom du demandeur) : Coordonnées du demandeur.
      - Telephone Number (Numéro de téléphone) : Coordonnées du demandeur.
      - Common Name (Nom commun) : domaine du site Web entré dans le navigateur d'un visiteur *hostname.domaine.*
      - Email Address (Adresse e-mail) : Coordonnées du demandeur.
      - Organization (Organisme) : valeur pour l'organisme à déclarer sur le certificat.
      - Organizational Unit (Unité de l'organisme) : (facultatif) valeur pour l'unité de l'organisme qui sera déclarée sur le certificat.
      - Locality (Localité) : (facultatif) ville, département, principauté ou pays, également déclaré sur le certificat, si fourni.
      - State (Département) : (facultatif) nom complet du département.
      - Country (Pays) : les deux lettres du code ISO désignent le pays qui est déclaré sur le certificat. Ce champ est obligatoire.

   e. **Une fois ces informations entrées, cliquez sur le bouton OK pour les soumettre.**

5. **Faites appel à une autorité de certification pour créer le certificat.**

   - Si vous choisissez d'envoyer votre demande de certificat à un URL d'autorité de certification, elle sera automatiquement envoyée à cette adresse.
   - Si vous choisissez une adresse e-mail d'autorité de certification, copiez la demande de certificat qui vous a été envoyée par courrier électronique avec les en-têtes et déposez-la auprès de l'autorité de certification.

6. **Une fois le certificat créé, copiez-le avec les en-têtes sur le presse-papier.**

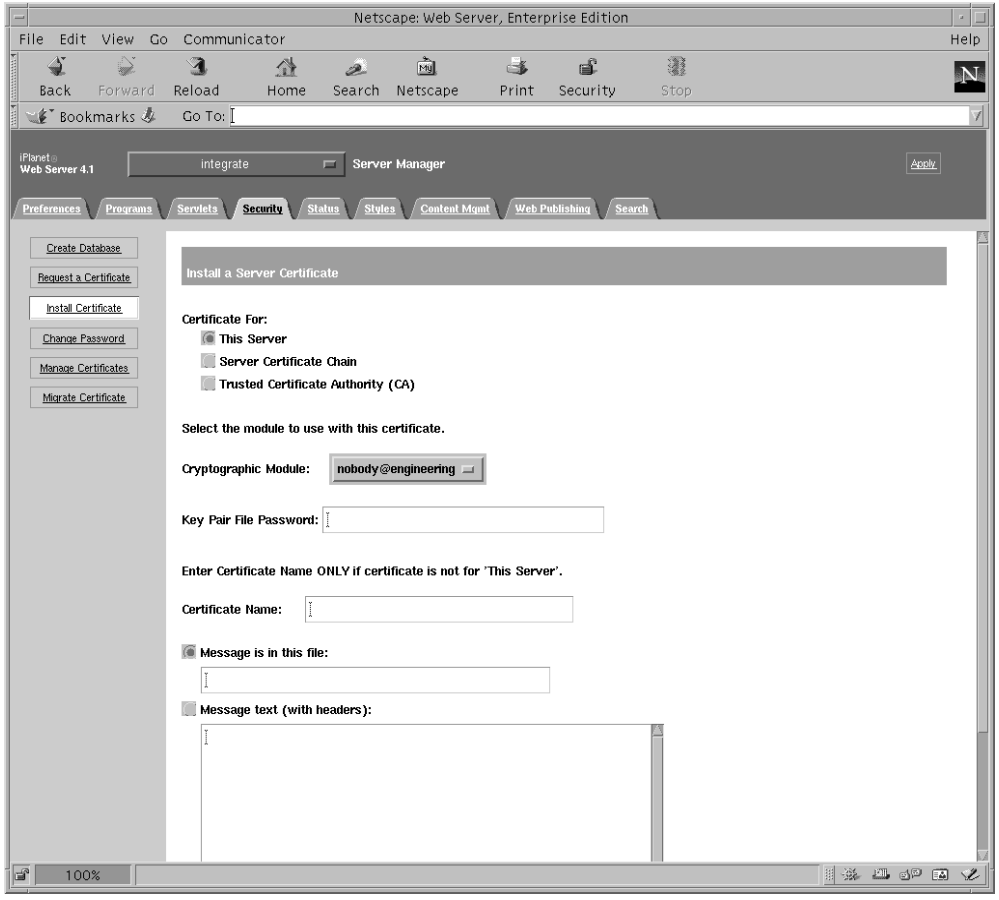
   Notez que le certificat est différent de la demande de certificat et qu'il vous est généralement présenté sous forme de texte.

▼ Pour installer le certificat de serveur

1. **Sélectionnez le lien Install Certificat (Installer le Certificat) sur la partie gauche de la page.**

   Lorsque votre demande a été approuvée par une autorité de certification, et qu'un certificat vous a été délivré, vous devez l'installer sur le serveur Web iPlanet.

2. **Sélectionnez l'onglet Security (Sécurité) à gauche puis l'option Install Certificat (Installer le certificat).**



3. **Remplissez le formulaire pour installer votre certificat :**
   - Certificat For (Certificat pour) : ce serveur
   - Cryptographic Module (Module cryptographique) : sélectionnez le nom *user@realm-name* approprié.

- Key Pair File Password (Mot de passe du fichier de paire de clés) : entrez le mot de passe pour le *user@realm-name* qui possède la clé créée précédemment.
- Certificat Name (Nom du certificat) : dans la plupart des cas, vous pouvez laisser ce champ vide. Si vous choisissez d'entrer un nom, celui-ci modifiera le nom utilisé par le serveur Web pour accéder au certificat et à la clé lors de l'exécution avec la prise en charge SSL.

4. **Choisissez Message Text (with headers) (Texte des messages (avec en-têtes)) et collez le certificat copié précédemment.**
5. **Cliquez sur le bouton OK sur la partie inférieure de la page, en copiant le certificat copié à partir de l'autorité de certification dans la boîte Message.**

   Des informations de base sur le certificat s'affichent alors.
6. **Si tout vous semble correct, cliquez sur le bouton Add Server Certificate (Ajouter un certificat de serveur).**

   Des messages à l'écran vous indiquent de redémarrer le serveur. Cela n'est pas nécessaire car l'instance du serveur Web a été arrêtée pendant toute la durée des opérations. Vous serez également notifié que le serveur Web doit être configuré de manière à pouvoir utiliser SSL. Utilisez les procédures suivantes pour configurer le serveur Web.

Configuration d'un serveur Web iPlanet 4.1

A présent que le serveur Web et le certificat du serveur sont installés, vous devez configurer le serveur Web pour SSL.

▼ Pour configurer le serveur Web iPlanet 4.1

1. **A partir de la page principale d'administration, choisissez l'instance du serveur Web avec laquelle vous désirez travailler et cliquez sur le bouton Gestion.**

   Par défaut, vous êtes sur l'onglet Preferences (Préférences) sur la partie supérieure de la page. Si ce n'est pas le cas, cliquez sur cet onglet.
2. **Cliquez sur l'onglet Preferences (Préférences) sur la partie supérieure de la page. Cliquez sur le lien Encryption On/Off sur la partie gauche de la page. Configurez l'encryption sur On.**

   Le champ port dans la boîte de dialogue doit être mise à jour au numéro de port SSL par défaut : 443. Modifiez le numéro de port si nécessaire.

3. **Cliquez sur le bouton OK.**

4. **Appliquez ces modifications en cliquant sur le bouton Save (Enregistrer).**

   Le serveur Web est à présent configuré pour une exécution en mode sécurisé.

5. **Modifiez le fichier `/usr/netscape/server4/https-`*hostname*`/config/magnus.conf` en ajoutant la ligne suivante :**

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

   où *hostname* est le nom du serveur Web.

   Par défaut, le certificat créé à l'étape 2 et 3 est nommé `Server-Cert`. Si votre certificat a un nom différent, remplacez-le par `Server-Cert`.

6. **Sélectionnez le serveur que vous voulez administrer et cliquez sur le bouton Apply (Appliquer) dans le coin supérieur droit de la page.**

   Cette action applique les modifications dans le serveur d'administration.

7. **Cliquez sur le bouton Load Configuration Files (Charger les fichiers de configuration) pour appliquer les modifications que vous venez d'effectuer sur le fichier `magnus.conf`.**

   En cliquant sur le bouton Apply Changes (Appliquer les modifications) alors que le serveur est arrêté, une fenêtre indépendante dans laquelle vous êtes invité à entrer un mot de passe s'affiche. Il est impossible de redimensionner la fenêtre et il se peut que vous ne puissiez pas soumettre les modifications. Il existe deux solutions à ce problème.

   - Cliquez sur le bouton Load Configuration Files (Charger les fichiers de configuration) à la place.
   - Démarrez le serveur Web d'abord puis cliquez sur le bouton Apply Changes (Appliquer les modifications).

8. **Sur la page du serveur Web, cliquez sur le lien On/Off sur la partie gauche de la page. Entrez les mots de passe des serveurs et cliquez sur le bouton OK.**

   Vous êtes invité à entrer un ou plusieurs mots de passe. A l'invite du module interne, entrez le mot de passe pour la base de données de certification du serveur Web.

   A l'invite du module *user@realm-name*, entrez le mot de passe que vous avez créé lorsque vous avez créé l'*utilisateur* dans *nom-domaine* à l'aide de `secadm`.

9. **Vérifiez que SSL est activé sur le nouveau serveur Web, avec un navigateur, à l'adresse URL suivante :**

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

   Notez que le *server_port* par défaut est 443.

CHAPITRE 5

Installation et configuration d'un serveur Web iPlanet 6.0

Ce chapitre décrit l'activation de la carte Crypto Accelerator 1000 de Sun pour l'utilisation avec le serveur Web iPlanet 6.0.

Ce chapitre comprend les sections suivantes :

Installation du serveur Web iPlanet 6.0

Les sections suivantes décrivent l'installation et la configuration du serveur Web iPlanet. Vous devez suivre les procédures dans l'ordre indiqué. Reportez-vous à la documentation du serveur Web iPlanet pour plus d'informations sur les serveurs Web iPlanet.

▼ Pour installer le serveur Web iPlanet 6.0

1. **Installez le logiciel du serveur Web iPlanet 6.0.**

   Ce logiciel est disponible à l'adresse URL suivante :

   `http://www.iplanet.com`

2. **Installez le serveur Web.**

   Vous trouverez un exemple d'instructions mais vous pouvez choisir de configurer votre serveur Web différemment. Le nom du chemin par défaut est : `/usr/iplanet/servers`

   Acceptez le chemin par défaut pendant l'installation du serveur Web iPlanet. Ce guide fait référence à ces chemins par défaut. Si vous décidez de l'installer à un emplacement différent, assurez-vous de noter l'emplacement.

3. **Lancez le programme de configuration.**

4. **Répondez aux invites du script d'installation.**

   Pour simplifier l'utilisation, vous pouvez accepter les paramètres par défaut, excepté pour les invites suivantes :

   a. **Acceptez les termes de la licence en saisissant** `oui`**.**

   b. **Entrez un** *hostname.domain* **(nomhôte.domaine) entièrement valide.**

   c. **Entrez le mot de passe du serveur d'administration iWS deux fois.**

   d. **A l'invite, appuyez sur Entrée.**

▼ Pour créer une base de données de certification

1. **Démarrez le serveur d'administration.**

   Pour démarrer un serveur Web, utilisez la commande suivante (au lieu d'exécuter `startconsole` comme requis lors de la `configuration`) :

```
# /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
```

   Un message de réponse vous indique l'URL auquel vous devez vous connecter pour administrer vos serveurs.

2. **Démarrez le serveur d'administration iPlanet en ouvrant un navigateur Web et en entrant :**

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

Une fenêtre indépendante vous invite à entrer l'identificateur d'utilisateur et le mot de passe. Entrez le nom d'utilisateur du serveur d'administration iWS et le mot de passe choisis au cours de l'exécution de la configuration.

Remarque – Entrez le mot `admin` pour l'identificateur d'utilisateur ou le nom d'utilisateur du serveur d'administration iWS, si vous avez utilisé les paramètres par défaut lors de la configuration du serveur Web iPlanet.

---

3. **Cliquez sur OK.**

4. **Créez la base de données de certification pour les instances du serveur Web.**

Vous voulez peut-être activer la sécurité sur plus d'une instance du serveur Web. Répétez cette opération pour chaque instance de serveur Web.

Remarque – Si vous voulez exécuter SSL également sur le serveur d'administration, la configuration d'une base de données de certification est identique. Reportez-vous à la documentation iPlanet pour plus d'informations.

---

   a. **Cliquez sur l'onglet Servers (Serveurs) dans le serveur d'administration.**

   b. **Sélectionnez un serveur et cliquez sur le bouton Manage (Gestion).**

   c. **Cliquez sur l'onglet Security (Sécurité) sur la partie supérieure de la page et sélectionnez l'option Create Database (Créer une base de données).**

   d. **Entrez un mot de passe (base de données de certification du serveur Web) dans les deux boîtes de dialogue et cliquez sur OK.**

      Choisissez un mot de passe de 8 caractères au minimum. Il s'agit du mot de passe utilisé pour lancer les modules cryptographiques internes lorsque le serveur Web iPlanet est exécuté en mode sécurisé.

5. **Exécutez le script suivant pour activer la carte Crypto Accelerator 1000 de Sun :**

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

Ce script vous invite à choisir le serveur Web. Il permet d'installer les modules cryptographiques de la carte Crypto Accelerator 1000 de Sun pour le serveur Web iPlanet ou Apache. Puis, le script met à jour les fichiers de configuration pour activer la carte Crypto Accelerator 1000 de Sun.

6. **Entrez `1` pour configurer votre serveur Web iPlanet afin d'utiliser SSL, puis appuyez sur Entrée.**

```
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. **A l'invite, entrez le chemin du répertoire racine du serveur Web, puis appuyez sur Entrée.**

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

8. **A l'invite, entrez `y` et appuyez sur Entrée, si vous désirez poursuivre.**

```
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. **Entrez `0` pour quitter.**

▼ Pour créer un certificat de serveur

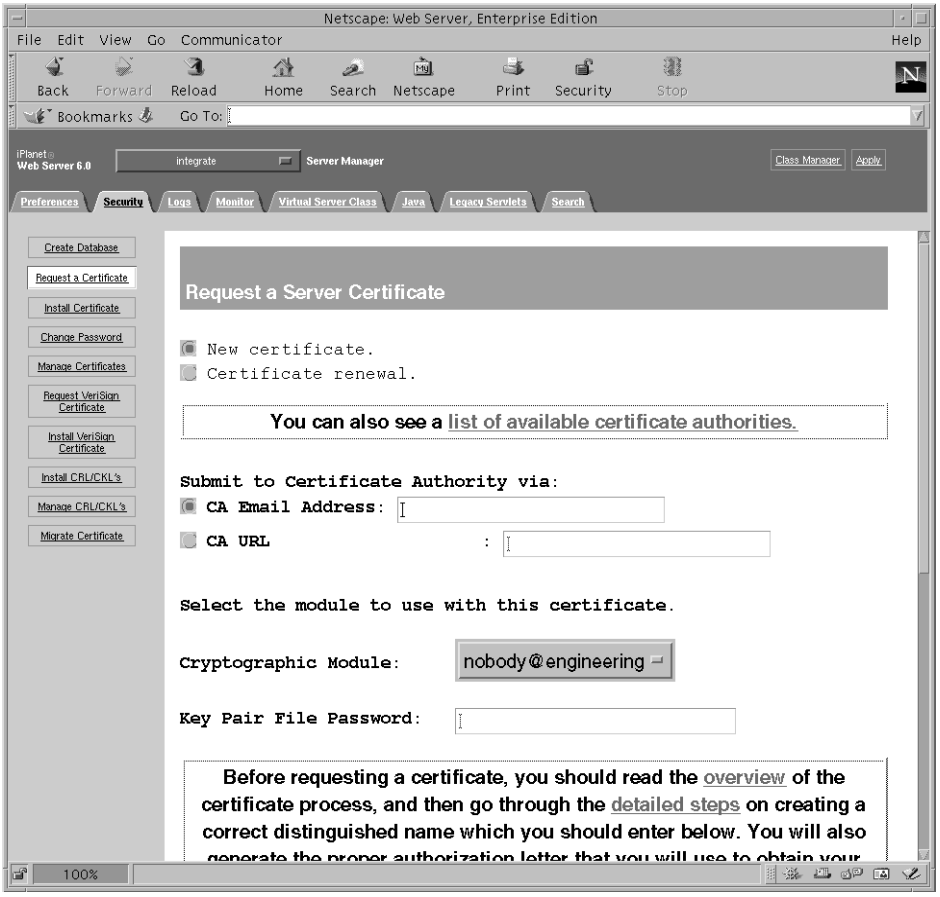
1. **Redémarrez le serveur Web d'administration en entrant les commandes suivantes :**

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

2. **Pour effectuer une demande de certificat de serveur, cliquez sur l'onglet Security (Sécurité) sur la partie supérieure de la page.**

   Le fenêtre Create Trust Database (Création de base de données de certification) s'affiche.

3. **Cliquez sur le lien Request Certificate (Demande de certificat) sur la partie gauche de la page.**



4. **Remplissez le formulaire pour créer une demande de certificat, à l'aide des informations suivantes :**

   a. **Sélectionnez un nouveau certificat**

   Si vous pouvez envoyer directement votre demande de certificat à une autorité de certification ou d'enregistrement sur le Web, sélectionnez l'option CA URL (URL de l'autorité de certification). Dans le cas contraire, sélectionnez CA Email Address (Adresse e-mail de l'autorité de certification) et choisissez une adresse e-mail à laquelle vous voulez envoyer votre demande de certificat.

b. Sélectionnez le module cryptographique que vous voulez utiliser.

Chaque domaine dispose de sa propre entrée dans ce menu déroulant. Assurez-vous de sélectionner le domaine correct. Pour utiliser le Crypto Accelerator 1000 de Sun, vous devez sélectionner un module sous la forme de *user@realm-name*.

c. Dans la boîte de dialogue Key Pair File Password (Mot de passe de fichier de paire de clés), entrez le mot de passe pour le *user@realm-name* qui sera en possession de la clé.

d. Indiquez les informations appropriées pour les champs suivants :

- Requestor Name (Nom du demandeur) : coordonnées du demandeur.
- Telephone Number (Numéro de téléphone) : coordonnées du demandeur.
- Common name (Nom commun) : domaine du site Web entré dans le navigateur d'un visiteur *hostname.domaine*
- Email Address (Adresse e-mail) : coordonnées du demandeur.
- Organization (Organisme) : valeur pour l'organisme à déclarer sur le certificat.
- Organizational Unit (Unité de l'organisme) : (facultatif) valeur pour l'unité de l'organisme qui sera déclarée sur le certificat.
- Locality (Localité) : (facultatif) ville, département, principauté ou pays, également déclaré sur le certificat, si fourni.
- State (Département) : (facultatif) nom complet du département.
- Country (Pays) : les deux lettres du code ISO désignent le pays qui est déclaré sur le certificat. Ce champ est obligatoire.

e. Une fois ces informations entrées, cliquez sur le bouton OK pour les soumettre.

5. Faites appel à une autorité de certification pour créer le certificat.

- Si vous choisissez d'envoyer votre demande de certificat à un URL d'autorité de certification, elle sera automatiquement envoyée à cette adresse.
- Si vous choisissez une adresse e-mail d'autorité de certification, copiez la demande de certificat qui vous a été envoyée par courrier électronique avec les en-têtes et déposez-la auprès de l'autorité de certification.

6. Une fois le certificat créé, copiez-le avec les en-têtes sur le presse-papier.

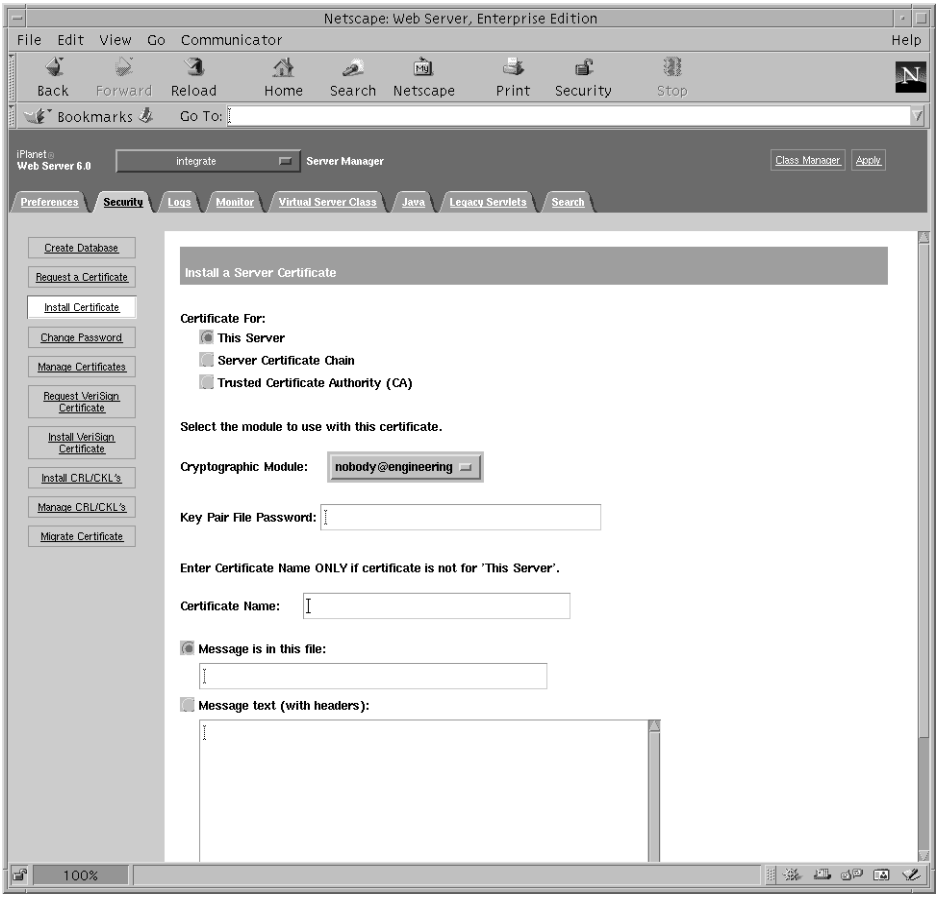
Notez que le certificat est différent de la demande de certificat et qu'il vous est généralement présenté sous forme de texte.

▼ Pour installer le certificat de serveur

1. Sélectionnez le lien Install Certificate (Installer le Certificat) sur la partie gauche de la page.

Lorsque votre demande a été approuvée par une autorité de certification, et qu'un certificat vous a été délivré, vous devez l'installer sur le serveur Web iPlanet.

2. **Sélectionnez l'onglet Security (Sécurité) à gauche puis l'option Install Certificate (Installer le certificat).**



3. **Remplissez le formulaire pour installer votre certificat :**
   - Certificate For (Certificat pour) : ce serveur
   - Cryptographic Module (Module cryptographique) : sélectionnez le nom *user@realm-name* approprié.
   - Key Pair File Password (Mot de passe du fichier de paire de clés) : entrez le mot de passe pour le *user@realm-name* qui possède la clé créée précédemment.
   - Certificate Name (Nom du certificat) : dans la plupart des cas, vous pouvez laisser ce champ vide. Si vous choisissez d'entrer un nom, celui-ci modifiera le nom utilisé par le serveur Web pour accéder au certificat et à la clé lors de l'exécution avec la prise en charge SSL.

4. **Choisissez Message Text (with headers) (Texte des messages (avec en-têtes)) et collez le certificat copié précédemment.**

5. **Cliquez sur le bouton OK sur la partie inférieure de la page, en copiant le certificat copié à partir de l'autorité de certification dans la boîte Message.**

   Des informations de base sur le certificat s'affichent alors.

6. **Si tout vous semble correct, cliquez sur le bouton Add Server Certificate (Ajouter un certificat de serveur).**

   Des messages à l'écran vous indiquent de redémarrer le serveur. Cela n'est pas nécessaire car l'instance du serveur Web a été arrêtée pendant toute la durée des opérations. Vous serez également notifié que le serveur Web doit être configuré de manière à pouvoir utiliser SSL. Utilisez les procédures suivantes pour configurer le serveur Web.

Configuration du serveur Web iPlanet 6.0

A présent que le serveur Web et le certificat du serveur sont installés, vous devez configurer le serveur Web pour SSL.

▼ Pour configurer le serveur Web iPlanet 6.0

1. **Cliquez sur l'onglet Preferences (Préférences) sur la partie supérieure de la page. Sélectionnez l'option Edit Listen Sockets (Modifier les sockets de réception) dans le cadre situé sur la partie gauche.**

   Le cadre principal répertorie toutes les sockets de réception définies pour l'instance du serveur Web.

   a. **Modifiez les champs suivants :**

      - Port : défini sur le port sur lequel vous allez exécuter votre serveur Web avec SSL activé (il s'agit généralement du port 443).
      - Security (Sécurité) : défini sur On.

   b. **Cliquez sur le bouton OK pour appliquer ces changements.**

      Dans le champ Security (Sécurité) de la page Edit Listen Sockets (Modifier les sockets de réception), il devrait y avoir maintenant le lien Attributes (Attributs).

2. **Cliquez sur le lien Attributes (Attributs).**

3. **Entrez le mot de passe** *user@realm-name* **pour certifier votre identité sur** *user@realm-name,* **sur le système.**

4. **Sélectionnez SSL settings (Paramètres SSL) à partir de la fenêtre indépendante.**

   Vous pouvez choisir Cipher Default settings, SSL2, or SSL3/TLS (Paramètres de chiffrement par défaut, SSL2 ou SSL3/TLS). L'option par défaut n'affiche pas les paramètres par défaut. Les deux autres options nécessitent la sélection des algorithmes que vous voulez activer.

5. **Sélectionnez le certificat pour le** *user@realm-name* **suivi de** `:Server-Cert` **(ou le nom que vous avez choisi s'il est différent).**

   Uniquement les clés appartenant au *user@realm-name* approprié sont affichées dans le champ Certificate name (Nom de certificat).

6. **Lorsque vous avez choisi un certificat et confirmé tous les paramètres de sécurité, cliquez sur le bouton OK.**

7. **Cliquez que le lien Apply (Appliquer) dans le coin supérieur droit pour appliquer ces changements avant de démarrer le serveur.**

8. **Cliquez sur le lien Charger les fichiers de configuration pour appliquer ces modifications.**

   Ce lien vous dirige vers une page vous permettant de démarrer l'instance du serveur Web.

   En cliquant sur le bouton Apply Changes (Appliquer les modifications) alors que le serveur est arrêté, une fenêtre indépendante dans laquelle vous êtes invité à entrer un mot de passe s'affiche. Il est impossible de redimensionner la fenêtre et il se peut que vous ne puissiez pas soumettre les modifications.

   Il existe deux solutions à ce problème :

   - Cliquez sur le bouton Load Configuration Files (Charger les fichiers de configuration) à la place.
   - Démarrez le serveur Web d'abord puis cliquez sur le bouton Apply Changes (Appliquer les modifications).

9. **Entrez les mots de passe requis dans les boîtes de dialogue pour démarrer le serveur.**

   Vous êtes invité à entrer un ou plusieurs mots de passe. A l'invite du module interne, entrez le mot de passe pour la base de données de certification du serveur Web.

   A l'invite du module *user@realm-name*, entrez le mot de passe que vous avez créé lorsque vous avez créé l'*utilisateur* dans *nom-domaine* à l'aide de `secadm`.

10. **Vérifiez que SSL est activé sur le nouveau serveur Web, avec un navigateur, à l'adresse URL suivante :**

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

    Notez que le *server_port* par défaut est 443.

CHAPITRE 6

Activation du serveur Web Apache

Ce chapitre décrit l'activation de la carte Crypto Accelerator 1000 de Sun pour une utilisation avec un serveur Web Apache.

Ce chapitre comprend les sections suivantes :

Activation du serveur Web Apache

Le serveur Web Apache 1.3.12 est fourni avec l'environnement d'exploitation Solaris 8 7/01. Les instructions suivantes sont spécifiquement applicables à cette version du serveur Web Apache. Pour de plus amples informations sur l'utilisation d'un serveur Web Apache, veuillez consulter la documentation qui s'y rapporte.

▼ Pour activer le serveur Web Apache

1. **Créez un fichier de configuration `httpd`.**

   Pour les systèmes Solaris, le fichier `httpd.conf-example` se trouve généralement dans `/etc/apache`. Vous pouvez utiliser ce fichier comme modèle et le copier comme suit :

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

   Remplacez `ServerName` dans le fichier, par le nom de votre serveur.

2. **Démarrez** `sslconfig`.

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

3. **Sélectionnez 2 pour configurer votre serveur Web Apache pour l'utilisation de SSL :**

```
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. **Indiquez le répertoire où se trouvent les binaires Apache.**

   Sur les systèmes Solaris, il s'agit généralement de `/usr/apache`.

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

5. **Indiquez l'emplacement des fichiers de configuration de Apache.**

   Sur les systèmes Solaris, il s'agit généralement de `/etc/apache`.

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

6. **Créez une paire de clés RSA pour votre système.**

   Si vous décidez de ne pas en créer une, vous devrez le faire ultérieurement et utiliser `sslconfig` pour créer les clés.

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

   Si vous répondez non, allez directement à la section « Pour créer un certificat », page 46.

7. **Indiquez le répertoire pour le stockage des clés.**

   Si ce répertoire n'existe pas, il sera créé.

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

8. **Choisissez un nom de base pour la clé matérielle.**

   Ce nom comportent plusieurs suffixes pour vous permettre de distinguer les fichiers de clés, les fichiers de demande de certificat et, ultérieurement, les fichiers de certificats.

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

9. **Fournissez une clé dont la longueur se situe entre 512 et 2048 bits.**

   Pour la plupart des applications de serveur Web, une longueur de 1024 bits est suffisamment solide, mais vous pouvez opter pour des clés plus solides si vous le désirez.

```
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. **Créez votre phrase-clé PEM.**

    Cette phrase-clé est utilisée pour protéger la clé matérielle. Assurez-vous de choisir une phrase-clé solide dont vous pourrez vous souvenir. Si vous oubliez le mot de passe, vous ne pourrez pas accéder à vos clés.

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

Attention – Vous devez vous souvenir de la phrase-clé que vous avez entrée. Sans elle, vous ne pourrez pas accéder à vos clés. Il est impossible de récupérer une phrase-clé oubliée.

Création d'un certificat

La procédure suivante décrit la création du certificat requis pour activer un serveur Web Apache afin d'utiliser la carte Crypto Accelerator 1000 de Sun.

▼ Pour créer un certificat

1. **Vous pouvez créer une demande de certificat en utilisant les clés que vous venez de créer.**

   Vous devez d'abord entrer le mot de passe pour accéder à vos clés. Indiquez ensuite les informations appropriées dans les champs suivants :

   - Country Name (Pays) : les deux lettres du code ISO désignent le pays qui est déclaré sur le certificat. Ce champ est obligatoire.
   - State or Province Name (Département) : (facultatif) nom complet du département (ou entrez . et appuyez sur Entrée)
   - Locality (Localité) : (facultatif) ville, département, principauté ou pays, également déclaré sur le certificat, si fourni
   - Organizational Name (Organisme) : valeur pour l'organisme à déclarer sur le certificat
   - Organizational Unit Name (Unité de l'organisme) : (facultatif) valeur pour l'unité de l'organisme qui sera déclarée sur le certificat
   - SSL Server Name (Nom du serveur SSL) : domaine du site Web qui est tapé dans le navigateur d'un visiteur.
   - Email Address (Adresse email) : coordonnées du demandeur

```
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. **Modifiez le fichier** `/etc/apache/httpd.conf` **comme indiqué.**

   Des informations concernant vos fichiers de clés et de certificats s'affichent. Vous verrez également des instructions pour la modification du fichier `/etc/apache/httpd.conf` pour l'utiliser avec le logiciel Crypto Accelerator 1000 de Sun.

```
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. **Si vous choisissez de configurer un** `VirtualHost`**, les directives** `SSLEngine`**,** `SSLCertificateFile` **et** `SSLCertificateKeyFile` **doivent être placées dans le fichier** `httpd.conf`**, juste au-dessus de la directive** `SSLPassPhraseDialog`**.**

```
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>
```

Si vous avez répondu non à la question de l'étape 6, vous obtiendrez également des informations supplémentaires sur la création ultérieure de clés matérielles :

```
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. **Sélectionnez** `0` **pour quitter, une fois les opérations terminées avec l'utilitaire** `sslconfig`**.**

5. **Copiez votre demande de certificat avec les en-têtes à partir de** `/etc/apache/keys/`*base_name*`-certreq.pem` **(où base_name a été configuré à l'étape 8) et déposez-la auprès de votre autorité de certification.**

6. **Une fois le certificat créé, vous pouvez créer le fichier de certificat `/etc/apache/keys/`*base_name*`-cert.pem` et y copier votre certificat.**

7. **Démarrez le serveur Web Appache.**

   Il est entendu que votre répertoire de binaires Apache est `/usr/apache/bin`. S'il ne s'agit pas de votre répertoire de binaires, entrez le répertoire approprié.

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

8. **A l'invite, entrez votre phrase-clé PEM.**

9. **Vérifiez que SSL est activé sur le nouveau serveur Web, avec un navigateur, à l'adresse URL suivante :**

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

   Notez que le *server_port* par défaut est 443.

CHAPITRE 7

Diagnostics et dépannage

Ce chapitre décrit les tests de diagnostics et le dépannage pour le logiciel Crypto Accelerator 1000 de Sun. Il comprend les sections suivantes :

Logiciel de diagnostics SunVTS

Le test SunVTS `dcatest`, fourni dans le progiciel `SUNWdcav` sur le CD *Crypto Accelerator 1000 de Sun*, fonctionne avec l'interface utilisateur et de contrôle de tests SunVTS fourni dans les progiciels `SUNWvts` et `SUNWvtsx` sur le CD Supplement de Solaris. Ce test effectue des diagnostics pour la carte Crypto Accelerator 1000 de Sun.

Reportez-vous à la documentation SunVTS pour obtenir plus d'instructions sur le démarrage et le contrôle de ces tests de diagnostics. Ces documents sont disponibles dans le Solaris on Sun Hardware AnswerBook, fourni avec le CD Supplement de Solaris pour la version Solaris de votre système.

Remarque – SunVTS ne peut être utilisé qui si vous avez installé les progiciels SunVTS à partir du CD Supplement de Solaris.

▼ Pour lancer `dcatest`

1. **Lancez SunVTS en tant que superutilisateur.**

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

   Reportez-vous au *SunVTS User's Guide* pour obtenir des instructions détaillées sur le lancement de SunVTS.

   Les instructions suivantes supposent que vous avez lancé SunVTS avec l'interface utilisateur CDE.

2. **Dans la fenêtre principale de diagnostics SunVTS, configurez la carte du système sur le mode Logical (logique).**

3. **Désactivez tous les tests en désélectionnant les cases.**

4. **Sélectionnez la case OtherDevices (Autres périphériques), puis la case plus de OtherDevices pour afficher tous les tests dans le groupe OtherDevices.**

5. **Désélectionnez les cases du groupe OtherDevices qui ne sont pas nommées `dcatest`.**

   - Si un `dcatest` est affiché, allez à l'étape 6.
   - Si un `dcatest` n'est pas affiché, cherchez-le en sondant le système et en sélectionnant Reprobe system (Re-sonder le système) dans le menu déroulant Commands (Commandes).

   Reportez-vous à la documentation SunVTS pour connaître la procédure exacte. Lorsque la recherche est terminée et qu'un `dcatest` est affiché, poursuivez avec l'étape 6.

6. **Sélectionnez l'une des instances de `dcatest`, puis cliquez dessus avec le bouton droit de la souris et déplacez-la pour afficher les options de paramètres de test.**

   Ces options, qui se rapportent à `dcatest`, sont décrites dans la section « Options de paramètres de test pour `dcatest` », page 53.

7. **Après avoir effectué toutes les sélections, cliquez sur Within Instance Apply (Appliquer sur l'instance) pour modifier l'instance sélectionnée de `dcatest` ou cliquez sur Accross All instances Apply (Appliquer sur l'ensemble des instances) pour modifier toutes les instances cochées de `dcatest`.**

   Cette action supprime la fenêtre indépendante et vous retournez alors à la fenêtre principale de diagnostics Sun.

8. **Sélectionnez l'une des instances de `dcatest`, puis cliquez dessus avec le bouton droit de la souris et déplacez-la pour afficher les options d'exécution de tests.**

   Une autre méthode pour l'affichage des options d'exécution de tests consiste à cliquer sur la fenêtre indépendante Options puis sur Test Executions (Exécution de tests). Ces options sont des commandes générales de SunVTS qui touchent tous les tests. Reportez-vous à la documentation SunVTS pour obtenir des informations détaillées.

9. **Une fois toutes les sélections effectuées, cliquez sur Apply (Appliquer) pour supprimer la fenêtre indépendante et retourner à la fenêtre principale de diagnostics de Sun.**

10. **Cliquez sur le bouton Start (Lancer) pour lancer les tests sélectionnés.**

11. **Cliquez sur Stop (Arrêter) pour arrêter tous les tests.**

Options de paramètres de test pour `dcatest`

Le TABLEAU 7-1 répertorie les options de paramètres de test pour `dcatest` comme indiqué à l'étape 6 de la section « Pour lancer `dcatest` », page 52. Le type de carte étant testé s'affiche dans la zone Configuration de la fenêtre indépendante.

TABLEAU 7-1 Options de paramètres de test pour `dcatest`

Nom de l'option	Description
`Test_Sel`	Une valeur décimale qui spécifie la combinaison des sous-tests à lancer. La valeur 0 (zéro) sélectionne tous les tests. A chaque sous-test est affecté un nombre en puissance de deux. Un sous-test individuel peut être sélectionné en entrant le nombre affecté au sous-test. Plusieurs sous-test peuvent être sélectionnés en entrant la somme des nombres affectés aux sous-tests choisis. Le paramètre par défaut est zéro.
`Info_Print`	Active ou désactive l'impression des messages d'informations (type INFO. Le paramètre par défaut est Enable (Activer).

Le TABLEAU 7-2 décrit les sous-tests `dcatest`.

TABLEAU 7-2 Sous-tests `dcatest`

Nom du test	Nombre	Description
`ALL`	0	Tous les tests sont exécutés.
`SHOWINFO`	1	Imprime un message de type INFO montrant le fournisseur et le périphérique sous un test d'informations.
`3DES`	2	Teste l'encryption de masse 3DES.
`RSA`	4	Teste les clés publiques et privées RSA.
`DSA`	32	Teste la vérification de la signature DSA.
`Random`	64	Teste la génération de nombres aléatoires et pseudo-aléatoires. Imprime un message de type INFO montrant les nombres générés.

Les messages générés par sous-tests sont affichés dans la zone Test Messages (Messages de tests) de la fenêtre principale de diagnostiques SunVTS. Les messages générés par les sous-tests sont groupés par type :

- Les messages de type INFO sont affichés dans la zone de test de messages et enregistrés dans le journal d'informations, si Info_Print est activé dans la fenêtre indépendante de paramètres de tests. Les messages de type INFO fournissent des informations non critiques.
- Messages de type erreur FATALE qui sont toujours affichés et enregistrés dans le journal des erreurs de tests et dans le journal d'informations.
- Messages de type VERBOSE qui suivent la progression effectuée au travers des sous-tests sont affichées uniquement si l'option VERBOSE est activée dans la fenêtre indépendante Test Execution (Exécution de tests). Les messages VERBOSE ne sont enregistrés dans aucun journal.

  Vous pouvez sélectionner un mode silencieux de test affichant et journalisant les messages d'erreur FATALE `dcatest` en désactivant les options VERBOSE et `Info_Print`.

Syntaxe de la ligne de commande `dcatest`

Si vous choisissez de lancer `dcatest` à partir de la ligne de commande à la place de l'environnement CDE, vous devez alors spécifier tous les arguments dans la chaîne de la ligne de commande.

En mode 32 bits, le chemin vers `dcatest` est `/opt/SUNWvts/bin/`. En mode 64 bits, le chemin vers `dcatest` est `/opt/SUNWvts/bin/sparcv9/`.

L'exemple suivant indique la syntaxe pour la commande en mode 32 bits :

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

Reportez-vous au manuel *SunVTS Test Reference Manual* pour obtenir une définition des arguments de ligne de commande standard. Comme `dcatest` est un test en mode Fonctionnel, `-f` doit être inclus. Incluez `-u` pour afficher un message d'utilisation ou `-v` pour des messages VERBOSE. Les éléments entre crochets ci-dessus indiquent les entrées facultatives. L'omission d'une option produit le comportement par défaut pour cette option, comme indiqué dans le TABLEAU 7-3.

TABLEAU 7-3 Syntaxe de la ligne de commande `dcatest`

Argument	Description
`dev=dca`*n*	Spécifie l'instance du périphérique à tester, telle que dca0 ou dca2. A la valeur dca0 par défaut, si aucune valeur n'est incluse.
`testsel=`*n*	Spécifie les sous-tests à exécuter où n peut être un nombre de 0 à 127. A la valeur 0 si aucune valeur n'est incluse.
`infodis`	Inclus si les messages de type INFO doivent être désactivés. A la valeur Info_Print Enabled (Activé) par défaut, si aucune valeur n'est incluse.

Dépannage du périphérique Crypto Accelerator 1000 de Sun

Pour déterminer si le périphérique Crypto Accelerator 1000 de Sun est répertorié dans le système, entrez, à partir de l'invite OpenBoot PROM (OBP), `show-devs`, pour afficher la liste des périphériques. Dans la liste des périphériques, s'affichent des lignes semblables aux exemples ci-dessous, spécifiques à la carte Crypto Accelerator 1000 Sun :

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

Dans l'exemple ci-dessus, `pci108e,5455` identifie le chemin du périphérique à la carte Crypto Accelerator 1000 de Sun. Il n'y a aucun microprogramme sur cette carte. C'est pourquoi les diagnostics de niveau de OBP ne sont pas disponibles.

La carte Crypto Accelerator 1000 ne comporte aucun voyant ou autre indicateur reflétant l'activité cryptographique de la carte. Afin de déterminer si les demandes de fonctionnalités cryptographiques sont effectuées sur la carte, utilisez la commande `kstat`(1M) pour afficher l'utilisation du périphérique :

```
# 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
```

L'affichage des informations `kstat` indique si les demandes relatives à la cryptographie ou les « jobs » sont envoyées à la carte Crypto Accelerator 1000 de Sun. Une modification de la valeur « jobs » au cours du temps indique que la carte Crypto Accelerator de Sun accélère les demandes de fonctionnalités cryptographiques qui lui sont envoyées. Si les demandes ne sont pas envoyées à la carte, vérifiez votre configuration du serveur Web via la configuration spécifique du serveur Web.

Il n'est pas toujours possible de déterminer l'emplacement où une demande cryptographique a été effectuée. Ces demandes peuvent être effectuées à des emplacements différents, selon le chargement du sous-système au moment de la soumission de la demande.

N'essayez pas d'interpréter les valeurs statistiques du noyau/pilote renvoyées par `kstat`(1M). Ces valeurs sont maintenues au sein du pilote afin de faciliter la prise en charge de champ. Le sens et les noms peuvent varier au cours du temps.

ANNEXE **A**

Administration de la carte Crypto Accelerator 1000 de Sun avec un serveur Web iPlanet

Cette annexe présente les fonctionnalités de la carte Crypto Accelerator 1000 de Sun administrée avec un serveur Web iPlanet.

Remarque – Pour pouvoir gérer des domaines, vous devez avoir accès au compte de l'administrateur système pour votre machine.

Cette annexe comprend les sections suivantes :

Concepts et terminologie

Des domaines et utilisateurs doivent être créés pour des applications communiquant avec la carte Crypto Accelerator 1000 de Sun par une interface PKCS#11, telle que le serveur Web iPlanet.

Les utilisateurs de la carte Crypto Accelerator 1000 de Sun sont les uniques propriétaires des clés matérielles cryptographiques. Chaque utilisateur peut détenir plusieurs clés. Un utilisateur peut décider de détenir plusieurs clés afin de prendre en charge différentes configurations ; par exemple une clé de « production » et une clé de « développement » (marquant les différents organismes de l'utilisateur). Il peut également nécessiter plusieurs clés pour faciliter un configuration High Availability (HA). Notez que les termes « utilisateur » ou « compte utilisateur » se

rapportent aux utilisateurs de la carte Sun Crypto Accelerator 1000, non pas aux comptes utilisateur UNIX traditionnels. Il n'y a pas de mappage fixe entre les noms d'utilisateurs UNIX et ceux de la carte Crypto Accelerator 1000 de Sun.

Les domaines représentent des partitionnements logiques d'utilisateurs et de leurs clés matérielles. Ils permettent de réunir plusieurs utilisateurs dans un même ensemble. Le maintien d'un espace de nom unique pour chaque domaine constitue l'un des avantages du partitionnement des utilisateurs par domaine. Le contenu des domaines peut ainsi être géré séparément.

Une installation type comprend un domaine unique et un utilisateur unique. Par exemple, une telle configuration peut être composée d'un domaine unique « webserver » et d'un utilisateur dans ce domaine « nobody ». Ce qui autorise l'utilisateur « nobody » à obtenir et maintenir le contrôle d'accès des clés du serveur au sein d'un domaine unique.

Il est possible de créer des domaines supplémentaires pour partitionner les utilisateurs et les clés matérielles. Une configuration plus complexe consisterait en plusieurs domaines, par exemple « finance », « legal » et « engineering ». Chaque domaine conserve un nom d'espace unique. Par exemple, l'utilisateur « webserv » dans le domaine « finance » représente un compte utilisateur différent de « webserv » dans le domaine « engineering ».

Un outil d'administration, `secadm`, est utilisé pour gérer des domaines et des utilisateurs de la carte Crypto Accelerator 1000 de Sun.

Domaines, utilisateurs et serveur Web iPlanet

Lorsqu'un serveur Web iPlanet doit référencer une clé gérée par la carte Crypto Accelerator 1000 de Sun, il utilise un « nom de jeton » pour indiquer que la clé est gérée par le matériel et non par sa base de données logicielle interne.

La carte Crypto Accelerator 1000 de Sun crée ses noms de jetons en combinant un compte utilisateur et nom de domaine avec le symbole « @ ». Dans l'exemple d'installation type indiqué ci-dessus, un domaine unique « webserver » a été créé avec un utilisateur unique « nobody ». Le nom de jeton que le serveur Web iPlanet utiliserait pour référencer les clés détenues par l'utilisateur « nobody » dans le domaine « webserver » serait « nobody@webserver ». Le mot de passe pour l'utilisateur « nobody » (créé lorsque l'utilisateur est créé à l'aide de `secadm`) doit être utilisé lorsque vous effectuez une demande de certificat, installez ce dernier ou procédez à une authentification pour démarrer le serveur Web iPlanet.

Jetons et fichiers de jetons

Le serveur Web iPlanet peut accéder à la clé matérielle via les jetons. Les fichiers de jetons constituent, pour les administrateurs de la carte Crypto Accelerator 1000 de Sun, une technique de présentation, selon leurs choix, de jetons spécifiques à une application donnée.

Si aucun fichier de jetons n'existe, le logiciel Crypto Accelerator 1000 de Sun présente un ensemble de jetons par défaut au serveur Web iPlanet. Dans ce cas, un jeton est présenté par domaine, avec le nom de domaine `nobody@`*realm-name*.

Exemple

Il existe trois domaines : « engineering », « finance » et « legal ». Les jetons suivants sont présentés au serveur Web iPlanet :

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

Cependant, pour que ces noms puissent être utilisables, un utilisateur « nobody » doit exister dans chacun de ces domaines.

Fichiers de jetons

Pour ignorer la case par défaut, un fichier de jetons doit exister. Les fichiers de jetons sont des fichiers de texte qui contiennent un ou plusieurs noms de jetons, un par ligne. Un serveur Web iPlanet présente uniquement les jetons répertoriés dans ce fichier. Les méthodes de spécification des fichiers de jetons sont les suivantes (par ordre de précédence) :

1. Le fichier `$HOME/.SUNWconn_crypto_slots`

   Ce fichier doit exister dans le répertoire d'accueil de l'utilisateur UNIX sous lequel s'exécute le serveur Web iPlanet. Le serveur Web iPlanet peut s'exécuter sous le nom d'utilisateur UNIX ne disposant d'aucun répertoire d'accueil, dans quel cas cette approche peut être irréalisable.

2. Le fichier `/etc/opt/SUNWconn/crypto/slots`

   Le fichier `/etc/opt/SUNWconn/crypto/slots` est un fichier général par défaut, utilisé dans le cas où un fichier `.SUNWconn_crypto_slots` n'existe pas dans le répertoire d'accueil de l'utilisateur.

Voici un exemple du contenu d'un fichier de jetons :

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

Si aucun des fichiers ci-dessus n'est trouvé, alors la méthode par défaut décrite dans la section « Jetons et fichiers de jetons », page 59 est utilisée.

Voir le chapitre 3 pour plus d'informations sur les noms de jetons se rapportant à la configuration du serveur Web iPlanet.

Utilisation de `secadm`

Le programme `secadm` fournit une interface de ligne de commande au Crypto Accelerator 1000 de Sun.

Pour accéder facilement au programme `secadm`, placez le répertoire outils Crypto Accelerator 1000 de Sun dans votre chemin de recherche, par exemple :

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

La syntaxe de la commande `secadm` est :

`secadm` [`-h`]

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

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

La commande est placée dans le répertoire `/opt/SUNWconn/crypto/bin/`.

Le TABLEAU A-1 indique les options de l'outil `secadm`.

TABLEAU A-1 Options `secadm`

Option	Description
`-h`	Afficher la commande aide pour `secadm` et quitter.
`-f` *filename*	Lire une ou plusieurs commandes à partir de *filename* et quitter.
`-r` *realm-name*	Utilisé seulement en mode de commande simple. L'option `-r` indique à `secadm` d'exécuter la commande communiquée dans la domaine *realm-name*.
`-s` *admin-name*	Utilisé seulement en mode de commande simple. L'option `-s` indique à `secadm` de se connecter en tant qu'administrateur système en utilisant *admin-name* comme nom d'utilisateur. *admin-name* doit être un utilisateur UNIX UID 0 (zéro), par exemple un `superutilisateur`. La connexion aura lieu avant que la commande communiquée soit exécutée.
`-u` *username*	Utilisé seulement en mode de commande simple. L'option `-u` indique à `secadm` de se connecter en tant que *username*. La connexion aura lieu avant que la commande communiquée soit exécutée.
`-y`	Impose une réponse « oui » à toutes les commandes qui invitent généralement à une confirmation.

Modes de fonctionnement

`secadm` peut fonctionner dans un de ces trois modes. Ces modes diffèrent principalement selon la manière dont les commandes sont communiquées à `secadm`. Les trois modes sont : mode commande simple, mode fichier, mode interactif. Chaque mode nécessite un mot de passe différent.

Mode commande simple

En mode commande simple, l'utilisateur spécifie la commande à exécuter par `secadm` après que toutes les options de ligne de commande sont spécifiées. Par exemple, la commande suivante indiquerait tous les domaines existant et retournerait l'utilisateur vers l'invite du shell de la commande.

```
$ secadm show realm
```

La commande suivante effectue une connexion en tant qu'administrateur système et crée l'utilisateur « webserv » dans le domaine « engineering ».

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

Notez que le mot de passe entré à l'invite « Password: » nécessite le mot de passe de l'administrateur système tandis que le mot de passe entré à l'invite « Initial password: » et « Confirm password: » nécessite le mot de passe de l'utilisateur récemment créé.

Toutes les sorties du mode commande simple sont dirigées vers le flux de sortie standard. Cette sortie peut être redirigée à l'aide de méthodes UNIX basées sur le shell.

Mode fichier

En mode fichier, l'utilisateur spécifie un fichier à partir duquel `secadm` lit une ou plusieurs commandes. Le fichier doit être du texte ASCII comportant une commande par ligne. Commencez chaque commentaire par un dièse « # ». Si l'option en mode fichier est définie, `secadm` ignore tous les arguments de la ligne de commande après la dernière option. L'exemple suivant démarre les commandes dans `deluser.scr` et répond à toutes les invites par l'affirmative.

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

Mode interactif

Le mode interactif fournit à l'utilisateur une interface similaire à `ftp`(1), où les commandes peuvent être entrées l'une après l'autre. L'option `-y` n'est pas prise en charge en mode interactif.

Entrée de commandes avec secadm

Le programme secadm dispose d'un langage de commande qui doit être utilisé pour interagir avec la carte Crypto Accelerator 1000 de Sun. Les commandes sont entrées en utilisant tout ou partie d'un mot (partie suffisamment longue pour pouvoir identifier le mot de manière unique). Utiliser « sh » à la place de « show » conviendrait parfaitement mais utiliser « lo » est ambigu parce que cela peut signifier « login » ou « logout ».

L'exemple suivant indique l'entrée de commandes à l'aide de mots entiers :

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

La même information peut être obtenue en utilisant des parties de mots en tant que commandes, telles que sh us.

Une commande ambiguë produit une réponse de demande d'explication :

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

Authentification à l'aide de secadm

De nombreuses commandes et tout spécialement celles liées aux comptes utilisateur et aux clés, nécessitent une authentification de votre part, en tant qu'administrateur système ou utilisateur. Les administrateurs système doivent effectuer une authentification sur la carte Crypto Accelerator 1000 de Sun pour exécuter des opérations telles que la création de domaines, de comptes utilisateur, l'activation et la désactivation de comptes utilisateur et la suppression de domaines et de comptes utilisateur. L'authentification en tant qu'utilisateur est nécessaire afin de modifier le mot de passe d'un utilisateur ou répertorier les objets clés détenus par l'utilisateur.

Le TABLEAU A-2 indique les commandes pouvant être utilisées par l'administrateur système et celles pouvant être utilisées par l'utilisateur.

TABLEAU A-2 Matrice des commandes

Commande	Authentifier	Informations d'authentification maintenues	Utilisateur authentifié
`create user=`*username*	Non	Oui	Administrateur système
`create realm=`*realm-name*	Oui	Non	Administrateur système
`delete user=`*username*	Non	Oui	Administrateur système
`delete realm=`*realm-name*	Oui	Non	Administrateur système
`disable user=`*username*	Non	Oui	Administrateur système
`enable user=`*username*	Non	Oui	Administrateur système
`exit`	Non	Non	Tous
`login`	Oui	Non	Utilisateur
`logout`	Non	Non	Tous
`passwd`	Oui	Oui	Utilisateur
`set realm=`*realm-name*	Non	Non	Tous
`show class`	Non	Non	Tous
`show key`	Non	Oui	Utilisateur
`show realm`	Non	Non	Tous
`show user`	Non	Oui	Administrateur système
`su`	Oui	Non	Administrateur système
`quit`	Non	Non	Tous
`unset realm`	Non	Non	Tous

Pour vous identifier en tant qu'administrateur système, vous devez fournir, à l'invite, un nom d'utilisateur UNIX UID 0 (par exemple superutilisateur) ainsi que le mot de passe. Les utilisateurs nécessitent le mot de passe créé à leur intention lorsque l'utilisateur a été créé. Lorsque vous vous connectez en tant qu'administrateur système ou en tant qu'utilisateur, vous devez tout d'abord sélectionner un domaine.

Pour vous connecter en tant qu'utilisateur, entrez :

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

Pour vous connecter en tant qu'administrateur système, entrez :

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

Lorsque vous vous connectez en tant qu'utilisateur ou administrateur système, l'invite `secadm` vous indique l'utilisateur actuellement connecté. Une connexion utilisateur se différencie d'une connexion administrateur système par le dernier caractère dans l'invite. Les utilisateurs sont définis par un crochet pointu (>) tandis que les administrateurs système le sont par un dièse (#). Si vous êtes actuellement connecté en tant qu'utilisateur ou administrateur système, et que vous essayez de vous connecter en tant qu'un autre utilisateur ou administrateur système, les informations d'authentification vous concernant seront perdues lorsque la nouvelle connexion sera réussie. Par exemple :

```
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}>
```

Obtention d'aide pour les commandes

`secadm` comporte des fonctions d'aide intégrées. Pour obtenir de l'aide, vous devez entrer un caractère « ? » suivi de la commande pour laquelle vous désirez obtenir de l'aide. Si une commande dans son ensemble est entrée et qu'un « ? » existe quelque part sur une ligne, vous obtiendrez la syntaxe de la commande, par exemple :

```
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
```

En entrant un « ? », vous obtiendrez la liste des mots des commandes valides, par exemple :

```
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
```

Si vous désirez obtenir de l'aide en mode ligne de commande, rappelez-vous que dans certains cas, le caractère « ? » est interprété par le shell dans lequel vous travaillez. Assurez-vous d'utiliser le caractère d'échappement du shell de commande avant le point d'interrogation.

Fermeture d'un programme `secadm`

Deux commandes vous permettent de quitter `secadm` : `quit` et `exit`. La séquence de clé CTRL-D existe également à partir de `secadm`.

Configuration et gestion des domaines

Un domaine est un référentiel pour clé matérielle. Les administrateurs et utilisateurs sont également associés au domaine. Les domaines fournissent non seulement un espace de stockage mais permettent également aux objets clés d'être détenus par les comptes utilisateur. Cela permet de dissimuler les clés des applications qui ne sont pas authentifiées comme les détenteurs. Les domaines sont composés de deux éléments :

- Les objets clés : il s'agit de clés de longue durée stockées pour des applications telles que le serveur Web iPlanet.

- Comptes utilisateur : ces comptes permettent aux applications d'authentifier des clés spécifiques et d'y accéder.

Il peut arriver que plusieurs domaines soient présents et que chaque domaine possède ses propres comptes utilisateur, alors qu'un seul domaine est nécessaire. Par exemple, si une application est authentifiée en tant qu'utilisateur `webserv` et qu'il est nécessaire d'accéder à des clés dans un domaine, alors, le compte utilisateur `webserv` doit exister dans ce domaine.

Création d'un domaine

La création d'un domaine entraînera la création des répertoires, des fichiers et d'autres ressources nécessaires au stockage des objets clés de longue durée. Pour créer un domaine, l'administrateur doit utiliser la commande `create realm` et entrer le nom du domaine qui doit être créé. Que les informations d'authentification actuelles soient maintenues ou non, l'administrateur système doit être authentifié pour que la réalisation de cette commande réussisse. A l'invite, entrez le mot de passe UNIX de l'administrateur système. Par exemple :

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

Vous pouvez nommer les domaines selon vos besoins. Par exemple, vous choisirez peut-être de configurer des domaines pour différents départements, tels que « finance » et « engineering ». Dans ce cas, vous nommerez les domaines `finance` et `engineering`. Par exemple :

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

Configuration du domaine actuellement en fonctionnement

`secadm` peut uniquement gérer des clés et des comptes utilisateur dans un domaine à la fois. La majorité des commandes relatives aux domaines et comptes utilisateur nécessite que vous sélectionniez d'abord un domaine. Pour sélectionner un domaine, exécutez la commande `set realm,` comme indiqué dans l'exemple suivant :

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

Lorsque vous avez sélectionné le domaine, l'invite `secadm` indique le nom de domaine entre des accolades.

Si vous ne désirez plus travailler dans le domaine en cours d'opération, vous pouvez soit configurer ce domaine sur une nouvelle valeur ou bien annuler la configuration. La modification ou l'annulation de la configuration du domaine en cours d'opération déconnectera automatiquement tout utilisateur ou administrateur système actuellement authentifié, dans ce domaine. Par exemple :

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

Remplissage du domaine avec les utilisateurs

Ces noms d'utilisateurs sont uniquement connus avec la carte Crypto Accelerator 1000 de Sun et il n'est pas nécessaire qu'ils soient identiques au nom d'utilisateur UNIX sous lequel le serveur Web s'exécute. Avant d'essayer de créer l'utilisateur, n'oubliez pas que vous devez tout d'abord sélectionner le domaine correct et vous connecter en tant qu'administrateur système. Par exemple :

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

Si vous avez uniquement besoin d'un nom de domaine, vous pouvez éviter de configurer un fichier de jetons en utilisant le nom de domaine « nobody ». L'exemple suivant crée l'utilisateur « nobody » dans le domaine « engineering » et configure le mot de passe comme « nobody@engineering », défini comme *user@realm-name* dans le TABLEAU 3-1.

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

Vous devez utiliser ce mot de passe lors de l'authentification effectuée au cours du démarrage d'un serveur Web.

Attention – Vous devez vous souvenir du mot de passe que vous avez entré. Sans ce mot de passe, vous ne pourrez pas accéder à vos clés. Il est impossible de récupérer un mot de passe oublié.

Création d'une liste des domaines

Vous pouvez créer une liste des informations contenues dans un domaine en exécutant la commande `show realm=`*realm-name*.

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

Création de listes de classes de domaines

Les classes de domaines sont des modules de gestion de clés contrôlant la gestion des objets de clés, des comptes utilisateur et des données d'authentification par les domaines. L'unique classe de domaine actuellement gérée par la carte Crypto Accelerator 1000 de Sun est `SUNW_filesys`. Pour créer une liste de toutes les classes de domaines actuellement gérées, utilisez la commande `show class`.

```
secadm> show class
Classe de données
-----------------------------------------------------
SUNW_filesys
-----------------------------------------------------
```

Suppression d'un domaine

Vous pouvez supprimer un domaine en exécutant la commande `delete realm` et en fournissant le nom du domaine qui doit être supprimé. Lorsque vous exécutez la commande, `secadm` vous invite à confirmer ou infirmer la suppression du domaine par oui ou par non. De même que pour la création d'un domaine, l'administrateur système doit d'abord être authentifié avant que la commande ne soit exécutée. De plus, vous ne pouvez pas supprimer un domaine en cours d'utilisation. Pour supprimer des références dans les domaines, vous devrez peut-être fermer le serveur Web et/ou le serveur d'administration.

Configuration et gestion des comptes utilisateur

Les comptes utilisateur permettent aux applications d'être authentifiées sur la carte Crypto Accelerator 1000 de Sun et aux clés d'être séparées au sein d'un domaine. Les clés détenues par un compte utilisateur ne sont pas accessibles aux applications qui ne sont pas authentifiées ou bien elles sont authentifiées sur ce domaines comme un autre utilisateur. Pour toutes ces commandes, vous devez sélectionner un domaine et l'administrateur système doit être connecté à ce domaine à l'aide de la commande `secadm su`.

Création d'utilisateurs

- **Exécutez la commande** `create user` **pour créer un utilisateur.**

  Cette commande nécessite un nom d'utilisateur sous la forme `create user=`*username*.

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

Attention – Vous devez vous souvenir du mot de passe que vous avez entré. Sans ce mot de passe, vous ne pourrez pas accéder à vos clés. Il est impossible de récupérer un mot de passe oublié.

Création d'une liste d'utilisateurs

Seul l'administrateur système peut créer une liste des utilisateurs dans un domaine. L'administrateur système doit exécuter la commande `show user`. Cette commande crée uniquement une liste des utilisateurs dans le domaine que vous avez sélectionné.

- **Exécutez la commande** `show user`**.**

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

Modification des mots de passe utilisateur

Seul l'utilisateur connecté individuellement et utilisant la commande `secadm login` peut modifier le mot de passe utilisateur. Vous devez connaître votre mot de passe actuel avant de pouvoir en définir un nouveau.

- **Exécutez la commande** `passwd`**.**

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

Attention – Vous devez vous souvenir du mot de passe que vous avez entré. Sans ce mot de passe, vous ne pourrez pas accéder à vos clés. Il est impossible de récupérer un mot de passe oublié.

Activation ou désactivation des utilisateurs

Seuls les administrateurs système peuvent activer ou désactiver des utilisateurs. Par défaut, chaque utilisateur est créé avec le statut activé.

- **Pour désactiver un compte utilisateur entrez la commande** `disable user=`*username***.**

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

Toutes les tentatives d'authentification d'un utilisateur désactivé échoueront. Aucune clé n'est, de toutes les manières, modifiée de quelque façon que ce soit. Lorsqu'un compte est ré-activé, toutes les clés qui sont détenues par cet utilisateur sont une fois de plus accessibles par l'application authentifiée.

- **Pour activer un compte, entrez la commande** `enable user=`*username***.**

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

Suppression des utilisateurs

- **Exécutez la commande** `delete user` **en spécifiant l'utilisateur qui doit être supprimé.**

  L'administrateur système doit fournir le nom du compte utilisateur qui doit être supprimé.

  Les clés associées aux utilisateurs sont supprimées lorsque la commande est exécutée. `secadm` invite l'administrateur système à confirmer ou infirmer la suppression de l'utilisateur, par oui ou par non.

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

ANNEXE **B**

Pages manuel

Cette annexe décrit les pages `man` fournies avec le logiciel Crypto Accelerator 1000 de Sun.

Vous pouvez consulter les pages man à l'aides de la commande :

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

Le TABLEAU B-1 répertorie et décrit les pages `man`.

TABLEAU B-1 Pages `man` du logiciel Crypto Accelerator 1000 de Sun

Page `man`	Description
`cryptio(7d)`	Le pilote de périphérique `cryptio` offre un contrôle d'accès à l'accélérateur cryptographique matériel sous-jacent. Le pilote `cryptio` nécessite un logiciel en couches pour que les applications et les clients du noyau puissent accéder aux services fournis.
`dca(7d)`	Le pilote de périphérique `dca` est un pilote feuille qui offre un contrôle d'accès à l'accélérateur cryptographique matériel sous-jacent. Le pilote `dca` nécessite un logiciel en couches pour que les applications et les clients du noyau puissent accéder aux services fournis.
`kcl(7d)`	Le pilote de périphérique `kcl` est un module de noyau chargeable multithread offrant une prise en charge des pilotes de fournisseurs cryptographiques de Sun. Le pilote `kcl` nécessite un logiciel en couches pour que les applications et les clients du noyau puissent accéder aux services fournis.

TABLEAU B-1 Pages `man` du logiciel Crypto Accelerator 1000 de Sun

Page `man`	Description
`kcpi(7d)`	Le pilote de périphérique `kcpi` est un module de noyau chargeable multithread offrant une prise en charge des pilotes de fournisseurs cryptographiques de Sun. Le pilote `kcpi` nécessite un logiciel en couches pour que les applications et les clients du noyau puissent accéder aux services fournis.
`secadm(1m)`	`secadm` est l'utilitaire d'administration du logiciel Crypto Accelerator 1000 de Sun. La commande `secadm` est utilisée pour la manipulation de la configuration, du compte et des bases de données des clés liées au logiciel Crypto Accelerator de Sun. `secadm` manipule des informations de clés cryptographiques sensibles.
`secd(1m)`	Le démon `secd` offre des services d'accès administratifs à l'application `secadm`.
`sslconfig(1m)`	`sslconfig` est l'utilitaire de configuration du logiciel Crypto Accelerator 1000 de Sun.

ANNEXE **C**

Directives de Configuration SSL pour le serveur Web Apache

Cette annexe répertorie les directives de configuration d'une prise en charge SSL pour le serveur Web Apache avec le logiciel Crypto Accelerator 1000 de Sun. Ces directives de configuration se trouvent dans votre fichier `http.conf`. Pour plus d'informations reportez-vous à la documentation Apache.

1. `SSLPassPhraseDialog exec:`*program*

   Contexte : global

   Cette directive informe le serveur Web Apache que le *programme* spécifié doit être exécuté pour que vous puissiez obtenir le mot de passe pour le fichier de clés. *program* doit imprimer le mot de passe obtenu sur la sortie standard.

   Si plusieurs fichiers de clés sont présents et qu'ils ont le même mot de passe, alors *program* ne sera exécuté qu'une fois (chaque mot de passe obtenu est vérifié avant de relancer *program*).

   program est exécuté avec deux arguments ; le premier est le nom du serveur, sous la forme *servername*:*port*, par exemple : `www.fictional-company.com:443`. (Le port 443 est le port type pour les serveurs Web basés sur SSL). Le second est le type de clé dans le fichier de clés (*keytype*). *keytype* peut être soit RSA ou DSA.

Remarque – Comme ce programme peut être exécuté au moment du démarrage du système, assurez-vous qu'il est conçu de manière à s'adapter à un périphérique non `tty` (c'est-à-dire que la commande `tty`(3c) renverra faux).

   Le programme fourni `/opt/SUNWconn/crypto/bin/sslpassword` peut être utilisé pour l'exécutable *program*. Ce programme vous invite automatiquement à entrer le mot de passe en supprimant l'affichage de ce dernier à mesure qu'il est entré.

Le programme `sslpassword` fourni recherche également automatiquement des mots de passe dans les fichiers. Ainsi vous évitez l'interaction des utilisateurs au démarrage du serveur Web. Les mots de passe pour les fichiers de clés sont recherchés dans les fichiers nommés `/etc/apache/`*servername*`:`*port*`.`*keytype*`.pass`. Si ce fichier n'est pas présent, alors le fichier `/etc/apache/default.pass` sera utilisé. Ces fichiers de mot de passe ne contiennent que le mot de passe non encrypté sur une ligne.

Remarque – Les fichiers de mot de passe doivent être protégés par une autorisation afin que seul l'utilisateur UNIX, sous lequel le serveur Web s'exécute, puisse lire le fichier. Cet utilisateur doit être le même que celui configuré avec la directive standard de `l'utilisateur` Apache.

S'il n'y a aucune précision, le comportement par défaut consiste à utiliser un mécanisme d'invite interne. Il est conseillé aux clients Sun d'éviter le comportement par défaut et d'utiliser le programme `sslpassword` à la place, afin d'éviter les problèmes d'interaction au démarrage du système.

2. `SSLEngine` (`on|off`)

   Contexte : global, hôte virtuel

   Cette directive est utilisée pour permettre le protocole SSL. Elle est généralement utilisée avec un hôte virtuel pour activer SSL sur un sous-système de serveurs. L'une des formes communément utilisées est :

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

qui configure l'utilisation de SSL pour tout serveur récepteur sur le port 443 (le port HTTPS standard). Si elle n'est pas présente, elle est désactivée par défaut.

3. `SSLProtocol [+-]`*protocol*

   Contexte : global, hôte virtuel

   Cette directive configure le(s) protocole(s) que le serveur doit utiliser pour les transactions SSL.

Les protocoles disponibles sont répertoriés et décrits dans le TABLEAU C-1 :

TABLEAU C-1 Protocoles SSL

Protocole	Description
`SSLv2`	protocole SSL standard de facto original de Netscape
`SSLv3`	version mise à jour du protocole SSL, prise en charge par la plupart des navigateurs Web
`TLSv1`	mise à jour de `SSLv3` en cours de standardisation IETF, avec une prise en charge de navigateur minimale à la date où nous publions.
`all`	active tous les protocoles

L'utilisation des signes plus (+) ou moins (-), permet d'ajouter ou de supprimer des protocoles. Par exemple, pour désactiver la prise en charge de SSLv2, la directive suivante pourrait être utilisée :

```
SSLProtocol all -SSLv2
```

qui équivaut à

```
SSLProtocol +SSLv3 +TLSv1
```

4. `SSLCipherSuite` *cipher-spec*

   Contexte : global, hôte virtuel, répertoire, `.htaccess`

   La directive SSLCipherSuite est utilisée pour configurer les chiffrements SSL qui sont disponibles pour l'utilisation et leur préférence. Dans un contexte global et un contexte d'hôte virtuel, elle est utilisée lors du protocole SSL handshake initial. Dans un contexte par répertoire, elle oblige une re-négociation SSL à utiliser les chiffrements nommés. La re-négociation a lieu après la lecture de la requête, mais avant l'envoi de la réponse.

cipher-spec est une liste de chiffrements délimités par des deux-points, décrite dans le TABLEAU C-2.

TABLEAU C-2 Chiffrements SSL disponibles

Label du chiffrement	Protocole	Echange de clés	Authent.	Encryption	MAC	Type
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES (168 bits)	SHA1	
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES (168 bits)	MD5	
RC4-SHA	SSLv3	RSA	RSA	ARCFOUR (128 bits)	SHA1	
RC4-MD5	SSLv3	RSA	RSA	ARCFOUR (128 bits)	MD5	
RC4-MD5	SSLv2	RSA	RSA	ARCFOUR (128 bits)	MD5	
RC2-CBC-MD5	SSLv2	RSA	RSA	ARCTWO (128 bits)		
DES-CBC-SHA	SSLv3	RSA	RSA	DES (56 bits)	SHA1	
RC4-64-MD5	SSLv2	RSA	RSA	ARCFOUR (64 bits)	MD5	
DES-CBC-MD5	SSLv2	RSA	RSA	DES (56 bits)	MD5	
EXP-DES-CBC-SHA	SSLv3	RSA (512 bits)	RSA	DES (40 bits)	SHA1	export
EXP-RC2-CBC-MD5	SSLv2	RSA (512 bits)	RSA	ARCTWO (40 bits)	SHA1	export
EXP-RC2-CBC-MD5	SSLv3	RSA (512 bits)	RSA	ARCTWO (40 bits)	SHA1	export
EXP-RC4-MD5	SSLv3	RSA (512 bits)	RSA	ARCFOUR (40 bits)	MD5	export
EXP-RC4-MD5	SSLv2	RSA (512 bits)	RSA	ARCFOUR (40 bits)	MD5	export
NULL-SHA	SSLv3	RSA	RSA	Aucune	SHA1	
NULL-MD5	SSLv3	RSA	RSA	Aucune	MD5	
ADH-DES-CBC3-SHA	SSLv3	DH	Aucune	3DES (168 bits)	SHA1	
ADH-DES-CBC-SHA	SSLv3	DH	Aucune	DES (56 bits)	SHA1	
ADH-RC4-MD5	SSLv3	DH	Aucune	ARCFOUR (128 bits)	MD5	
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES (168 bits)	SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES (168 bits)	SHA1	
EDH-RSA-DES-CBC-SHA	SSLv3	DH	RSA	DES (56 bits)	SHA1	
EDH-DSS-DES-CBC-SHA	SSLv3	DH	DSS	DES (56 bits)	SHA1	
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH (512 bits)	RSA	DES (40 bits)	SHA1	export

TABLEAU C-2 Chiffrements SSL disponibles

Label du chiffrement	Protocole	Echange de clés	Authent.	Encryption	MAC	Type
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	DH (512 bits)	DSS	DES (40 bits)	SHA1	export
EXP-ADH-DES-CBC-SHA	SSLv3	DH (512 bits)	Aucune	DES (40 bits)	SHA1	export
EXP-ADH-RC4-MD5	SSLv3	DH (512 bits)	Aucune	ARCFOUR (40 bits)	MD5	export

Dans le TABLEAU C-2, DH se rapporte à Diffie-Hellman et DSS à Digital Signature Standard.

Le TABLEAU C-3 répertorie et décrit les alias fournissant des groupements de type macro.

TABLEAU C-3 Alias SSL

Alias	Description
SSLv2	tous les chiffrements SSL version 2.0
SSLv3	tous les chiffrements SSL version 3.0
EXP	tous les chiffrements de niveau exportation
EXPORT40	tous les chiffrements d'exportation de 40 bits
EXPORT56	tous les chiffrements d'exportation de 56 bits
LOW	chiffrements de puissance faible (DES, RC4 de 40 bits)
MEDIUM	tous les chiffrements de 128 bits
HIGH	tous les chiffrements utilisant Triple DES
RSA	tous les chiffrements utilisant l'échange de clés RSA
DH	tous les chiffrements utilisant l'échange de clés Diffie-Hellman
EDH	tous les chiffrements utilisant l'échange de clés Diffie-Hellman éphémère
ADH	tous les chiffrements utilisant l'échange de clés Diffie-Hellman anonyme
DSS	tous les chiffrements utilisant une authentification DSS
NULL	tous les chiffrements n'utilisant aucune encryption

Les préférences des chiffrements peuvent être configurées à l'aide des caractères spéciaux répertoriés et décrits dans le TABLEAU C-4.

TABLEAU C-4 Caractères spéciaux pour la configuration des préférences de chiffrement

Caractère	Description
<none>	ajouter un chiffrement à la liste.
!	supprimer entièrement un chiffrement de la liste ; il est impossible de le rajouter ultérieurement.
+	ajouter un chiffrement à la liste et le situer à son emplacement actuel (ou l'abaisser).
-	supprimer un chiffrement de la liste (il est possible de le rajouter à la liste ultérieurement)

La valeur par défaut de *cipher-spec* est :

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

La valeur par défaut configure tous les chiffrements à l'exception des codes Diffie-Hellman anonymes (non authentifiés), de préférence ARCFOUR et RSA, et privilégiant les degrés d'encryption élevés à ceux plus faibles.

5. `SSLCertificateFile` *file*

   Contexte : global, hôte virtuel

   Cette directive précise l'emplacement du fichier de certificat X.509 encodé au format PEM pour le serveur.

6. `SSLCertificateKeyFile` *file*

   Contexte : global, hôte virtuel

   Cette directive précise l'emplacement du fichier de clés privé encodé au format PEM pour le serveur, correspondant au certificat configuré avec la directive `SSLCertificateFile`.

7. `SSLCertificateChainFile` *file*

   Contexte : global, hôte virtuel

   Cette directive précise l'emplacement d'un fichier contenant les certificats encodés au format PEM constituant le chemin de certification du serveur. Elle peut être utilisée pour assister des clients dans la vérification du certificat du serveur, lorsque le certificat du serveur n'est pas directement signé par une autorité que le client reconnaît.

   Les certificats dans les chaînes sont supposés être valides également pour une authentification des clients, lorsque cette pratique (`SSLVerifyClient`) est utilisée.

8. `SSLCACertificateFile` *file*

   Contexte : global, hôte virtuel

   Cette directive précise l'emplacement d'un fichier contenant la concaténation des certificats pour les autorités de certification utilisée pour l'authentification des clients.

9. `SSLCARevocationFile` *file*

   Contexte : global, hôte virtuel

   Cette directive précise l'emplacement d'un fichier contenant la concaténation des listes de révocation des certificats des autorités de certifications utilisée pour l'authentification des clients.

10. `SSLVerifyClient` *level*

    Contexte : global, hôte virtuel, répertoire, `.htaccess`

    Cette directive configure l'authentification des clients du serveur. (Notez qu'elle n'est pas généralement nécessaire pour les applications d'eCommerce, mais elle est utilisée pour d'autres applications.)

    Les valeurs de *niveau* sont répertoriées et décrites dans le TABLEAU C-5.

TABLEAU C-5 Niveaux SSL de vérification des clients

Niveau	Description
`none`	aucun certificat client n'est requis.
`optional`	le client peut présenter un certificat valide.
`require`	le client *doit* présenter un certificat valide.
`optional_no_ca`	le client peut présenter un certificat, mais celui-ci ne doit pas obligatoirement être valide.

Généralement soit `none` soit `require` sera utilisé. La niveau par défaut est `none`.

11. `SSLVerifyDepth` *depth*

    Contexte : global, hôte virtuel, répertoire, `.htaccess`

    Cette directive précise la profondeur maximale de chaîne du certificat que le serveur autorisera pour les certificats de clients. Une valeur de 0 signifie que seuls les certificats auto-signés sont valides, tandis qu'une valeur de 1 signifie que les certificats de clients doivent être signés par une autorité de certification directement connue par le serveur (via `SSLCACertificateFile`). Des valeurs élevées permettent une délégation de l'autorité de certification.

12. `SSLLog` *filename*

    Contexte : global, hôte virtuel

Cette directive précise l'existence d'un fichier journal où des informations spécifiques à SSL seront enregistrées. Si elle n'est pas précisée (valeur par défaut), aucune information spécifique à SSL ne sera enregistrée.

13. `SSLLogLevel` *level*

Contexte : global, hôte virtuel

Cette directive précise la verbosité des informations enregistrées dans le fichier journal SSL. Les valeurs de *niveau* sont répertoriées et décrites dans le TABLEAU C-6.

TABLEAU C-6 Valeurs de niveau des fichiers journaux SSL

Valeur	Description
`none`	aucun enregistrement mais des messages d'erreur sont encore envoyés au fichier journal Apache standard
`warn`	comporte des messages d'avertissement
`info`	comporte des messages d'informations
`trace`	comporte des messages de trace
`debug`	comporte de messages de débogage

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

Contexte : global, hôte virtuel, répertoire, `.htaccess`

La directive configure les options spécifiques à SSL. Des options peuvent être ajoutées à la configuration actuelle en les préfixant avec un signe (+) ou supprimées avec un signe moins (-). S'il n'y a pas de signes moins ou plus, alors l'éventail d'options les plus proches sont utilisées.

Les options sont répertoriées et décrites dans le TABLEAU C-7.

TABLEAU C-7 Options SSL disponibles

Options	Description
`StdEnvVars`	un ensemble de variables standard d'environnement CGI/SSI lié à SSL est créé. Les performances en seront affectées.
`ExportCertData`	provoque l'exportation des variables d'environnement `SSL_SERVER_CERT`, `SSL_CLIENT_CERT` et `SSL_CLIENT_CERT_CHAIN`*n* (*n* = 0, 1, ...). Ces variables comportent des certificats encodés au format PEM pour le client et le serveur.
`FakeBasicAuth`	Le DN (Distinguished Name) du certificat de client est traduit en un nom d'utilisateur d'authentification basic HTTP et son authentification est simulée. Ce qui permet l'utilisation de mécanismes standard de contrôle d'accès à Apache avec l'authentification de client SSL, sans inviter l'utilisateur à entrer un mot de passe. Les entrées pour ces utilisateurs dans les fichiers de mot de passe Apache doivent utiliser le mot de passe encrypté `xxj31ZMTZzkVA`, qui n'est que la forme encryptée (`crypt`(3c)) du mot « mot de passe ».
`StrictRequire`	oblige le refus d'un accès interdit dû à `SSLRequireSSL`, et ce même en présence d'autres directives, telles que `Satisfy Any`, qui pourraient l'écraser.

15. `SSLRequireSSL`

Contexte : répertoire, `.htaccess`

Cette directive interdit l'accès à un répertoire donné à moins d'utiliser HTTPS. Elle peut être utilisée pour prévenir les erreurs de configuration qui pourraient mettre les données d'un répertoire à la disposition d'utilisateurs non authentifiés et non encryptés.

ANNEXE **D**

Création d'applications pour une utilisation avec la Carte Crypto Accelerator 1000 de Sun

Cette annexe traite du logiciel fourni avec la carte Crypto Accelerator 1000 de Sun, qui peut être utilisé pour construire des applications compatibles avec OpenSSL afin de bénéficier des fonctions d'accélération cryptographiques de la carte Crypto Accelerator de Sun.

Remarque – Ces informations sur la création d'applications pour l'utilisation du logiciel et du matériel Crypto Accelerator 1000 de Sun sont fournies en l'état et ne constituent pas une partie officiellement prise en charge du produit. Ces informations sont fournies à titre indicatif, sans aucune garantie. Si vous désirez obtenir une solution prise en charge par Sun, veuillez contacter les services professionnels de Sun pour en savoir plus.

Vous devez tout d'abord installer la progiciel `SUNWcrysl` qui contient les en-têtes de fichiers et les bibliothèques requis.

Votre application doit être configurée de manière à inclure les en-têtes OpenSSL à partir de `/opt/SUNWconn/crypto/include`, comme avec le drapeau de compilation :

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

De plus, le linker doit être dirigé de manière à inclure des références vers les bibliothèques appropriées. La plupart des applications compatibles avec OpenSSL référenceront soit l'une des bibliothèques `libcrypto.a` et `libssl.a` soit les deux. Les bibliothèques cryptographiques de Sun doivent être également incluses. Les drapeaux de linker suivants effectueront ceci :

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

Notez que certaines applications OpenSSL ne tireront aucun avantage à être compilées de la sorte (contrairement à une construction avec une bibliothèque OpenSSL, qui peut être téléchargée à partir de `www.openssl.org`).

ANNEXE **E**

Spécifications de la Carte Crypto Accelerator 1000 de Sun

Ce chapitre décrit les diverses spécifications de la carte Carte Crypto Accelerator 1000 de Sun.

Cette annexe comporte les sections suivantes :

Dimensions physiques

TABLEAU E-1 Dimensions physiques

Dimension	Mesure
Longueur	174,625 mm
Largeur	106,680 mm

Spécifications de l'interface

TABLEAU E-2 Spécifications de l'interface

Fonctionnalités	Spécification
Horloge PCI	33 ou 66 MHz
Interface hôte	PCI 2,1 avec une prise en charge d'une fréquence d'horloge de 33 ou 66 MHz et d'une tolérance à 3,3 ou 5 V.
Largeur de bus PCI	32 ou 64 bits

Alimentation requise

TABLEAU E-3 Alimentation requise

Spécification	Mesure
Consommation électrique maximale	10 W à 5 V 700 MW à 3,3 V
Tolérance	5 V +/- 5 % 3,3 V +/- 5 %
Courant	2 A à 1,8 V 150 mA à 3,3 V

Caractéristiques environnementales

TABLEAU E-4 Caractéristiques environnementales

Condition	Spécification de fonctionnement	Spécification de stockage
Température	0° à 70° C	-65° à +150° C
Taux d'humidité	5 à 85 % sans condensation	0 à 95 % sans condensation

ANNEXE **F**

Third-Party Licenses (Licences détenues par des tiers)

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.

Index

S

T

U

V