



Encryption Kit Installation Guide

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 817-0523
December 2004

Copyright 2004 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, SunOS, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2004 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Certaines parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, SunOS, et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REPOUDRE A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



041202@10536



Contents

Installing the Solaris Encryption Kit	5
About Encryption	5
Before You Begin	6
Local Installation	6
▼ To Install on a Local System Using the pkgadd Command	6
Remote Installation	7
▼ To Install From a Remote System	7
How to Get Help	8

Installing the Solaris™ Encryption Kit

This document includes the following sections:

- “About Encryption” on page 5
- “Before You Begin” on page 6
- “Local Installation” on page 6
- “Remote Installation” on page 7
- “How to Get Help” on page 8

About Encryption

The Solaris Encryption Kit contains encryption algorithms. The Encryption Kit contains kernel modules that implement various forms of encryption for IPsec and Kerberos. The Encryption Kit contains utilities that encrypt files from the command line. The Encryption Kit contains libraries with functions that application programs call in order to perform encryption.

The Encryption Kit includes the unrestricted implementation of the following algorithms:

- AES (128, 192, and 256-bit key sizes)
- Blowfish (32 to 448-bit key sizes, in 8-bit increments)
- ARCFOUR, also called RC4 (8 to 2048-bit key sizes)

The Encryption Kit replaces the default cryptographic libraries and kernel modules in the Solaris operating system, which are restricted to a maximum key size of 128 bits. After you install the Encryption Kit, commands that use encryption access the encryption libraries that the Encryption Kit installs.

Regulations on the export of encryption software are subject to change. For current information, please follow the links to Export Information at <http://www.sun.com/solaris/binaries>.

Before You Begin

The Encryption Kit installs on two types of hardware, or platforms: SPARC™ and x86. The information in this document applies to both platforms unless a direction is specifically called out for a particular platform.

The Encryption Kit installation requires a Solaris system with a CD-ROM device. In all cases, you must insert the Encryption Kit disc into the CD-ROM drive before you begin the install procedure.

This document describes the following tasks:

- Installing the Encryption Kit CD on a local system
- Installing the Encryption Kit CD from a remote system that has a CD-ROM drive

Local Installation

This procedure describes how to install the Encryption Kit on a Solaris system with a local CD-ROM drive.

▼ To Install on a Local System Using the pkgadd Command

1. Insert the CD into the CD-ROM drive.

2. Become superuser or assume an equivalent role:

```
% su
Password: Type superuser password
#
```

3. As superuser or in an equivalent role, add the packages in the Encryption Kit.

- SPARC: Use the following pkgadd command:

```
# pkgadd -d /cdrom/solaris_10_crypt/Encryption_10/sparc/Packages
The following packages are available:
 1  SUNWcrman      Encryption Kit On-Line Manual Pages
                        (sparc) 8.0,REV=1
 2  SUNWcry        Crypt Utilities
                        (sparc) 11.10.0,REV=2004.02.06.14.04
 3  SUNWcryr       Solaris Root Crypto
```

```
(sparc) 11.10.0,REV=2004.02.06.14.04
```

```
Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,?,q]: all
```

- x86: Use the following pkgadd command:

```
# pkgadd -d /cdrom/solaris_10_crypt/Encryption_10/i386/Packages
The following packages are available:
1  SUNWcrman      Encryption Kit On-Line Manual Pages
                        7.0,REV=1
2  SUNWcry        utilities for software encryption and decryption
                        (i386) 11.9.0,REV=2002.04.06.13.11
3  SUNWcryr       Solaris kernel root software encryption and decryption
                        (i386) 11.9.0,REV=2002.04.06.13.11

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,?,q]: all
```

Remote Installation

If the system on which you want to install the Encryption Kit does not have a CD-ROM drive, you can mount the CD-ROM drive of a remote system.

The remote system must be running the Solaris operating environment.

▼ To Install From a Remote System

1. On the remote system, insert the CD into the CD-ROM drive.
2. Become superuser or assume an equivalent role:

```
% su
Password:  Type superuser password
#
```

3. Determine whether the `nfsd` and `mountd` daemons are running:

```
# ps -ef | grep mountd
root  2426   497  0 10:26:30 pts/4      0:00 grep mountd
```

```
# ps -ef | grep nfsd
root  2428   497  0 10:27:50 pts/4      0:00 grep nfsd
```

If the daemons are running, the system returns more lines than the `grep` command:

```
root  2426   497  0 10:26:30 pts/4      0:00 grep mountd
root  1810     1  0  Apr 30  ?        0:14 /usr/lib/nfs/mountd
root  2427   497  0 10:27:50 pts/4      0:00 grep nfsd
```

```
root 1812      1  0   Apr 30 ?           6:19 /usr/lib/nfs/nfsd
```

- If the daemons are not running, start the daemons by typing:

```
# /usr/lib/nfs/nfsd -a 8
# /usr/lib/nfs/mountd
```

Repeat the `ps -ef | grep daemon` commands to confirm that the daemons are running.

- If the mount daemons are running, go to [Step 4](#).

4. Share the CD-ROM:

```
# share -F nfs -o ro cdpath
```

- SPARC: Use
/cdrom/solaris_10_crypt/Encryption_10/sparc/Packages for
cdpath
- x86: Use /cdrom/solaris_10_crypt/Encryption_10/i386/Packages
for cdp~~ath~~

5. On the system where you plan to install the Encryption Kit, become superuser or assume an equivalent role:

```
% su
Password: Type superuser password
#
```

6. Mount the remote CD-ROM drive:

```
# mkdir -p cdpath
# mount -F nfs cd-host:cdpath cdpath
```

- SPARC: Use
/cdrom/solaris_10_crypt/Encryption_10/sparc/Packages for
cdpath
- x86: Use /cdrom/solaris_10_crypt/Encryption_10/i386/Packages
for cdp~~ath~~

7. Install the Encryption Kit as described in [Step 3](#) of “Local Installation” on page 6.

How to Get Help

If you have problems when you install the Solaris Encryption Kit, call your service representative.

Be prepared to give the dispatcher the following information about your system:

- Model number
- Serial number
- Encryption Kit release number
- SunOS™ release number
- To find the SunOS release number, use the `uname` command with the `-r` option:

```
% uname -r  
5.9
```

