Encryption Kit Installation Guide

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

Part No: 817–0523
December 2004

041202@10536

Contents

Installing the Solaris™ Encryption Kit

This document includes the following sections:

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 *cdpath*

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 *cdpath*

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
```