ProtectToolkit C

Installation Guide

SafeNet
THE DATA PROTECTION COMPANY

Part Number 007-002861-009
Version 5.0

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. Send your comments, together with your personal and/or company details to the address below:

SafeNet, Inc.
4690 Millennium Drive
Belcamp, Maryland USA 21017

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support. SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact method	Contact information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	(800) 545-6608, (410) 931-7520
	Australia and New Zealand	+1 410-931-7520
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	+1 410-931-7520
	United Kingdom	0870 7529200, +1 410 931-7520
Web	www.safenet-inc.com	
Support and Downloads	www.safenet-inc.com/Support Provides access to the SafeNet Knowledge Base and quick downloads for various products.	

Customer Connection Center	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.

Revision History

Revision	Date	Reason
A	27 October 2014	Release 5.0

Table of Contents

Chapter 1
Introduction

Product Overview

ProtectToolkit C is a cryptographic service provider that implements the PKCS #11 application programming interface (API) standard as specified by RSA labs. It also includes a lightweight, proprietary Java API to access these PKCS #11 functions from Java.

The PKCS #11 API, also known as Cryptoki, includes a suite of cryptographic services for encryption, decryption, signature generation and verification as well as permanent key storage. The software found on the installation DVD is compliant with PKCS #11 V 2.10.

To provide the highest level of security, ProtectToolkit C interfaces to and is used in conjunction with SafeNet access provider software and the SafeNet range of hardware security modules (HSMs) such as the:

- ProtectServer Internal Express 2 (PSI-E2) intelligent cryptographic services PCIe adapter card
- ProtectServer External 2 appliance (PSE2)

HSMs may be located locally, on the same host system as ProtectToolkit C or they may be located remotely across a network.

Two product packages are available. These are:

- Runtime for operational use and
- SDK (software development kit) for use by developers

With ProtectToolkit C SDK installed the product may be configured to operate in Software Only mode for testing and development purposes. In this mode access to a HSM is not required.

About This Guide

This guide is intended for use by administrators who will install or uninstall the product on host computer systems. It covers those issues and concepts that must be understood to complete installation and uninstallation successfully.

Since ProtectToolkit C may be installed on systems running various operating systems, the installation chapters of this guide are organized accordingly. Thus, reference need only be made to operating system information that is relevant to you.

Before installing ProtectToolkit C some preparation may first be required. Additionally, once ProtectToolkit C is installed, further configuration will also be necessary. Please refer to Installation Overview for further information.

System Requirements

- A PC with a Pentium class processor or better and, where an adapter card is to be used, a PCI bus interface spare slot.

- A SafeNet hardware security module (not required when using software only operating mode for development and testing purposes).

- Java runtime (required for graphical user interface utilities only). The product has been tested using Java runtime version 1.6.x and 1.7.x. It may also operate correctly using other versions of the runtime however SafeNet does not warrant this.

- .NET versions 3.5 and 4.5 (Windows only). All required .NET versions are available for download from Microsoft.

- MSVC 2005, MSVC 2008, and MSVC 2010 (Windows only). All required MSVC versions are available for download from Microsoft.

Note: The Java runtime, .NET and MSCV must be installed *before* you install ProtectToolkit C.

Supported Platforms

The supported platforms are listed in the following table.

C=PTK-C component, PKCS #11 v2.10/2.20
M=PTK-M component, MS CSP 2.0 with CNG
J=PTK-J, Java runtime 1.6.x/1.7.x

Operating system	**32-bit binary 32-bit O/S**		**32-bit binary 64-bit O/S**		**64-bit binary 64-bit O/S**	
	PSE2	**PSI-E2**	**PSE2**	**PSI-E2**	**PSE2**	**PSI-E2**
Windows Server 2012 R2 x86			-	-	C/M/J	C/M/J
Windows Server 2008 R2 x86	–	–	–	–	C/M/J	C/M/J
Windows 7	C/J	C/J			C/M/J	C/M/J
RedHat Enterprise Linux 6 x86	C/J	C/J			C/J	C/J

Chapter 2
Installation Overview

Operating Modes

ProtectToolkit C can be used in any one of three operating modes. These are:

- **PCI mode** in conjunction with a compatible SafeNet cryptographic services adapter such as the *ProtectServer* installed locally
- **network mode** over a TCP/IP network, in conjunction with a compatible SafeNet cryptographic services hardware product such as the *ProtectServer External*
- **software only mode**, on a local machine without access to a hardware security module, for development and testing purposes

The following figures show these operating mode scenarios and the associated software required in each case.

Figure 1: PCI Mode

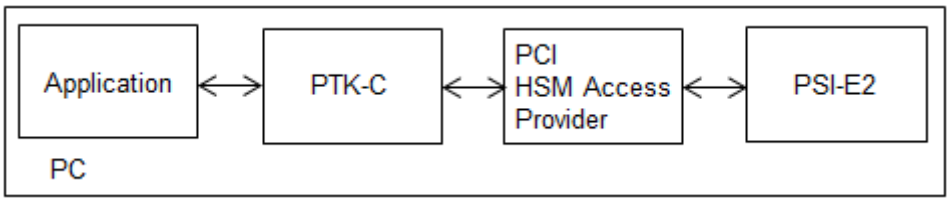


Figure 2: Network Mode using a SafeNet standalone HSM

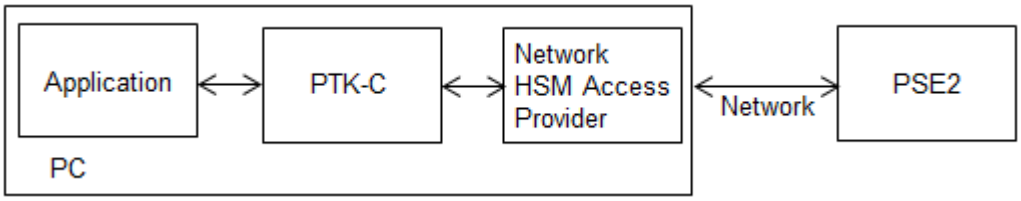
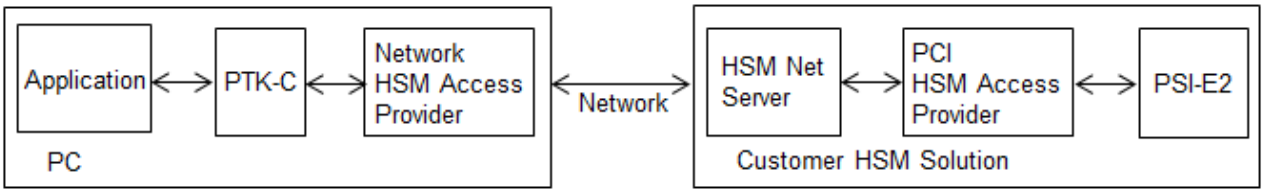


Figure 3: Network Mode using a SafeNet ProtectServer adapter



Operating Mode Setup

Installation of ProtectToolkit C is part of an operating mode setup, as summarized in the following steps.

PCI and Network Operating Modes

1. Install hardware

See the installation Guides provided with the hardware, such as the *ProtectServer Installation Manual.*

2. Install third-party software

Install the Java runtime, .NET (Windows only) and MSCV (Windows only) software.

3. Install and configure access provider software

Access provider software must be installed and configured to support the operating mode required, as detailed in the *Hardware Security Module: Access Provider Install and Configuration* section of this document

Note: It is not necessary to install access provider software when ProtectToolkit C is used in software-only mode for development and testing purposes.

4. Install ProtectToolkit C

Read the ProtectToolkit C Packages section (page 5), then install ProtectToolkit C on your computer system as detailed in this Guide.

5. Configure the secure messaging system (SMS)

Refer to the *Secure Messaging Overview, Messaging Mode Configuration,* and *Configuring Session Protection* sections in the *ProtectToolkit C Administration Manual*.

6. Establish network communication (network operating mode only)

To establish network communication the client must be configured to use one or more servers that are available on the same network. Refer to the *Specifying the Network Server(s)* section in the *ProtectToolkit C Administration Manual* for further information.

Software-Only Mode

1. Install ProtectToolkit C SDK

Read the ProtectToolkit C Packages section (page 5), then install the ProtectToolkit C SDK (Software Development Kit) on your computer system as detailed in this Guide.

2. Make configuration changes if required

Further changes may be made to customize the installation and optimize its performance. Refer to the *Software Only Mode Configuration* section in the *ProtectToolkit C Administration Manual* for further information if required.

ProtectToolkit C Packages

Two product packages are available for all supported Windows and Unix/Linux platforms. These are:

- **Runtime** for operational use. Package name: *PTKcprt*
- **SDK** (software development kit) for use by developers. Package name: *PTKcpsdk*

Runtime Package *(PTKcprt)*

The Runtime package provides all the necessary tools and interfaces needed to implement a ProtectToolkit C based Cryptoki service provider.

For Runtime package installation instructions please refer to Basic Installation on Windows for installation on Windows host operating systems and for Unix/Linux.

SDK Package *(PTKcpsdk)*

The SDK package is provided as a software development platform. Header files are included in addition to all the necessary tools and interfaces needed to implement a ProtectToolkit C based Cryptoki service provider.

Developers may work using a HSM, installed locally (PCI mode) or accessible across a network (network mode), to most closely approximate the operating environment. Alternatively, software only mode can be used.

Testing can easily be performed on any machine using software only mode without the need for a HSM. This may be of use in situations such as when it is not feasible to make HSMs available to multiple developers. Note that software-only mode is not a secure implementation, since key files are located on the hard drive of the host computer system.

Different ProtectToolkit C Cryptoki provider files are required depending upon whether a HSM is being used or not. During installation the developer must specify the required Cryptoki provider. Both Cryptoki provider files are installed and the one specified is made active. Subsequently, if the developer wishes to change operating modes this Cryptoki provider selection can be changed. See Changing the Cryptoki Provider for details

For SDK package installation instructions please refer to Basic Installation on Windows for installation on Windows host operating systems and Basic Installation on Unix/Linux for Unix/Linux.

Chapter 3
Basic Installation on Windows

This chapter covers installation of the Runtime and SDK packages on a Windows based operating system. Windows uninstallation instructions can also be found at the end of this chapter.

Review

The Runtime Package

The Runtime package provides all the necessary tools and interfaces needed to implement a ProtectToolkit C based Cryptoki service provider.

The SDK Package

The SDK package is provided as a software development platform. Header files are included in addition to all the necessary tools and interfaces needed to implement a ProtectToolkit C based Cryptoki service provider.

Developers may work using a HSM, installed locally (PCI mode) or accessible across a network (network mode), to most closely approximate the operating environment. Alternatively, software only mode can be used.

Preparation

1. Ensure that you have completed any preparatory steps required for the particular operating mode to be used. See Operating Mode Setup for further information.

2. Ensure that you have "Administrator" privileges. To add or remove software you must have "Administrator" privileges.

3. Install the Java runtime required by the GUI utilities. The Java runtime must be installed before you install ProtectToolkit C. See System Requirements for the supported versions.

4. Download and install MSVC 2005, MSVC 2008, and MSVC 2010 before you install ProtectToolkit C. All required MSVC versions are available for download from Microsoft.

5. Download and install .NET 3.5 and .NET 4.5 before you install ProtectToolkit C. All required .NET versions are available for download from Microsoft.

Note: The Runtime and SDK packages cannot be installed concurrently. To move from one package to the other, uninstall the package that is no longer required (see the *Uninstallation Procedure* section below) and then install the new one using the instructions that follow.

When Upgrading

To upgrade the software from a prior version, first remove any prior versions and then follow the instructions for installation below. See the *Uninstallation* section at the end of this chapter for further information about uninstallation.

Runtime Installation Procedure

Note: You must install the access provider software before you can install the PTK-C runtime. Otherwise the installation will fail. See the *HSM Access Provider Installation Guide* for details.

1. Locate the installation DVD and execute the file *PTKcprt.msi*. This is the ProtectToolkit C Runtime package.

2. Work through the installation wizard to complete the installation.

SDK Installation Procedure

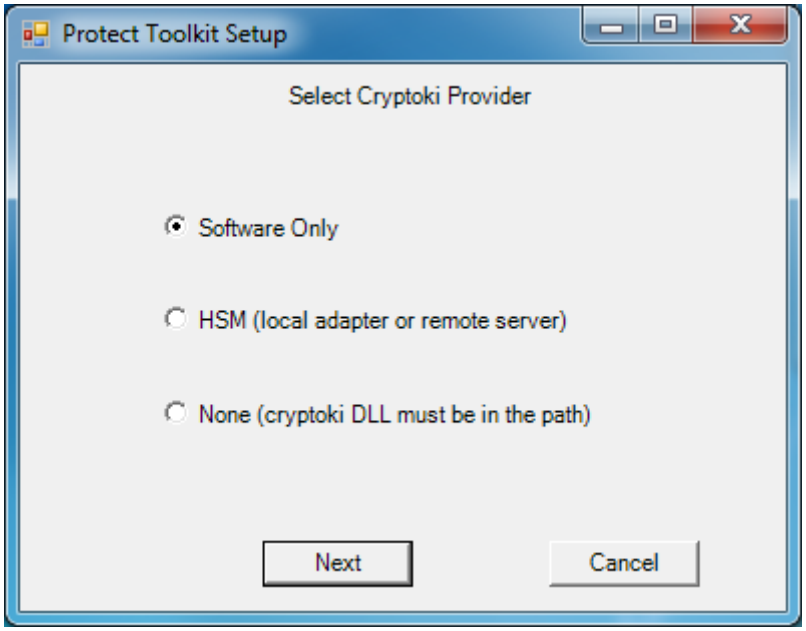
1. Locate the installation DVD and execute the file *PTKcpsdk.msi*. This is the ProtectToolkit C SDK package.

2. Work through the installation wizard to complete the installation.

3. A dialog is displayed during the installation process (shown below) that gives the option to update the *Path* to include the Cryptoki provider required. This will make the correct installed programs and libraries available from the command prompt.

If...	then select...
The SDK is to be used without access to a HSM (software only mode)	**Software Only**
A HSM will be available (PCI or network operating modes)	**HSM**
The Cryptoki provider required is already in the path (this might be the case if you are upgrading)	**None**

For further information regarding the available options see Installation Overview.



Note that the selection made here can be changed later. To do this, edit the system path to point to the Cryptoki provider required. For further information see Changing the Cryptoki Provider.

If you intend to use an HSM at this time, skip ahead to the chapters on HSM Provider Installation.

Uninstallation Procedure

To uninstall the *ProtectToolkit C Runtime* or *SDK* package, use the Windows **Programs and Features** control panel.

Chapter 4
Basic Installation on Unix/Linux

This chapter covers first time and upgrade installation of the Runtime and SDK packages on a Unix/Linux based operating system. Find Unix/Linux uninstallation instructions at the end of this chapter.

Review

The Runtime Package

The Runtime package provides all the necessary tools and interfaces needed to implement a ProtectToolkit C based Cryptoki service provider.

The SDK Package

The SDK package is provided as a software development platform. Header files are included in addition to all the necessary tools and interfaces needed to implement a ProtectToolkit C based Cryptoki service provider.

Developers may work using a HSM, installed locally (PCI mode) or accessible across a network (network mode), to most closely approximate the operating environment. Alternatively, software only mode can be used.

Preparation

Before proceeding:

- Please ensure that you have completed any preparatory steps required for the particular operating mode to be used. See Operating Mode Setup for further information.
- Please ensure that you are the super-user on the host system. In order to be able to add or remove software you must be the super-user on the host system.
- The Runtime and SDK packages cannot be installed concurrently. To move from one package to the other, uninstall the package that is no longer required (see the *Uninstallation Procedure* section below) and then install the new one using the instructions that follow.

Note: The SafeNet Luna VKD driver conflicts with the PTK e8k driver. Before installing PTK-C, you must uninstall the Luna VKD driver. If the VKD driver is required on the workstation, you cannot install PTK-C.

Upgrading

Uninstall the previous version first (see the Uninstallation Procedure section below) before proceeding with a new installation.

Installation Procedure

The ProtectToolkit C installation commands differ across the different supported Unix/Linux platforms. These differences are documented in Appendix A: Using the Unix/Linux Installation Utility. To take account of these differences automatically it is recommended that the package be installed using the **Unix Installation Utility**. Simply select the package required from the *Install Menu*.

Setting Up Your Environment

After installing the software, you must run the PTK **setvars.sh** script to configure your environment to use the PTK software. You cannot run the script directly, but instead you must source it or add it to a startup file (for example, **.bashrc**).

To set up your environment

1. Go to the PTK software installation directory:

   cd /opt/safenet/protecttoolkit5/ptk

2. Source the **setvars.sh** script:

   . ./setenv.sh

Once installed and configured, the software is ready to use under `/opt/safenet`.

Cryptoki Provider Selection (SDK Package Only)

The *software only* Cryptoki provider is made active by default on Unix/Linux systems. To change to the *SafeNet HSM Cryptoki provider* use the Unix/Linux Installation Utility. For further information see Changing the Cryptoki Provider.

Uninstallation Procedure

The ProtectToolkit C uninstallation commands differ across the different Unix/Linux platforms supported. These differences are documented in Using the Unix/Linux Installation Utility.. To take account of these differences automatically it is recommended that the package be uninstalled using the **Unix/Linux Installation Utility**. Simply select the package required from the *Install Menu*. See Appendix A for further guidance if required.

Alternatively, if for any reason you wish to enter platform specific commands manually then the commands given in Using the Unix/Linux Installation Utility can be used.

Chapter 5
Changing the Cryptoki Provider

This chapter applies to the SDK package only.

Different ProtectToolkit C Cryptoki provider files are required depending upon whether a HSM is being used (PCI and network modes) or not (software only mode).

When the SDK package is installed both Cryptoki provider files are installed. On Windows systems either one may be made active when prompted during installation. The software only Cryptoki provider is made active by default on Unix/Linux systems.

To change the active Cryptoki provider set up during installation or subsequently, refer to the section below for your operating system.

Procedure on Windows

The Windows Cryptoki provider is named *cryptoki.dll*. There are two versions of this file installed with PTK-C, as follows:

Mode	Default path
Software-only	C:\Program Files\Safenet\Protect Toolkit 5\ProtectToolkit C SDK\bin\sw\cryptoki.dll
HSM	C:\Program Files\Safenet\Protect Toolkit 5\ProtectToolkit C SDK\bin\hsm\cryptoki.dll

When you install the PTK-C software, you are prompted to select which Cryptoki provider you want to use. In response to the prompt, the installer performs the following actions to make the selected provider active:

- It adds the path to the selected Cryptoki provider to the **Path** environment variable
- It copies the selected Cryptoki provider *cryptoki.dll* file to **C:\Windows\System32**

To change the active Cryptoki provider

1. Edit the **Path** environment variable to point to the folder containing the *cryptoki.dll* file you want to use.

   For example, to change from software-only mode to HSM mode, edit the **Path** environment variable to change the path from:

   ```
   C:\Program Files\Safenet\Protect Toolkit
   5\ProtectToolkit C SDK\bin\sw
   ```

   to the following:

```
C:\Program Files\Safenet\Protect Toolkit
5\ProtectToolkit C SDK\bin\hsm
```

2. Copy the cryptoki.dll file for the Cryptoki provider you want to use to the **C:\Windows\System32** folder.

To access the Path environment variable

To access the **Path** environment variable for editing, follow the standard procedure for your system. Typically, the following steps are used:

1. Go to **Computer** on the desktop and select **System Properties**.
2. In the **System Properties** dialog box click **Advanced System Settings**. The **System Properties** dialog is displayed.
3. Click the **Environment Variables** button. The **Environment Variables** dialog is displayed.
4. In the **Environment Variables** dialog box locate and select the **Path** variable under **System Variables** and select the **Edit** button.
5. In the **Edit System Variable** dialog box make the change to the **Variable Value** as outlined above and click **OK** to action this change and close the dialog box.
6. Close all other dialog boxes to complete the operation.

Procedure on Unix/Linux

To change the default Cryptoki provider selection, simply use the Unix Installation Utility. See Appendix A: Using the Unix Installation Utility for further information on how to use this utility if required.

Alternatively, the change can be made manually. See the section Changing the Cryptoki Provider in Appendix A: Using the Unix/Linux Installation Utility for details.

It is recommended, unless there is good reason to do otherwise, that the installation utility be used. Using this method should prove to be easier and with less scope for making errors, it is more likely to result in a trouble free installation or uninstallation.

The utility provides a simple, uniform menu driven interface. In addition to handling installation and uninstallation on Unix/Linux systems it can also be used for other tasks. Specifically, the utility can be used to:

- List *SafeNet* packages already installed
- Uninstall *a SafeNet* package
- List DVD contents for the current platform only or all platforms
- Install a package from the DVD (also installs the utility in /usr/bin)

- Change the default operating mode (PCI, network or software only).

Whenever a SafeNet package is installed with the utility it also installs itself on the host system hard disk (in `/usr/bin/safeNet-install.sh`). It can be used when the DVD is not available, e.g. to uninstall or configure the software.

Startup

Should you encounter any problems while following this procedure, please see the section Unix Installation Utility Troubleshooting at the end of this chapter.

1. The *SafeNet Unix Installation Utility* can be found in the root of the installation DVD. Mount the DVD by following standard procedure for your particular platform and installation.

2. Change directory to the DVD and start the utility using the following commands:

```
# cd /misc/cd
# ./safeNet-install.sh
```

Note: A number of options available can be specified when executing the `safeNet-install.sh` command. These options are not normally required and are mainly of use for troubleshooting purposes. For further information see the Command Reference section at the end of this chapter.

The utility scans the system and the DVD and displays the *Main menu*.

```
SafeNet Unix Installation Utility (version 28):
Hostname: leknek (Linux 2.6.9-22.EL)

Main menu

1 list SafeNet packages already installed
2 list packages on CD
3 install a package from this CD
4 uninstall a SafeNet package
5 set the default cryptoki and/or hsm link


q quit the utility
```

Utility Navigation

Every menu screen shows the current Unix/Linux host and version, as well as the menu location at the top of the screen. For example: `Main Menu >> List CD menu.`

The valid key strokes for the current screen are shown at the bottom of the screen together with the default action (usually *Redraw*) which is shown in square brackets. To carry out the default action, click *Enter*.

To select a command from the menu press the corresponding numeric key.

'b' is used for “back to the previous menu” and 'q' to quit the utility. You can also quit with the system *INTR* key (normally ^C).

Installing ProtectToolkit C

Should you encounter any problems while following this procedure, please see the section Unix Installation Utility Troubleshooting at the end of this chapter.

1. Start the *Unix Installation Utility.* See the Startup section (page 13) for further instructions if required.

2. From the Main Menu select install a package from this DVD.

   A list of *SafeNet* packages that can be installed is displayed.

3. Select the package required by typing the appropriate menu number and *Enter*.

4. The utility verifies the action and then runs the appropriate command for the platform being used.

5. On some platforms, you may be prompted for additional options that may be used with the install command. On Linux for example, you can add a `-nodeps` option to suppress the checking of dependencies. These options should be selected with the normal care that is required whenever packages are installed or uninstalled.

6. You may now need to respond to any platform specific messages. For example, to confirm that you wish to proceed with the installation.

7. After installation, the utility will show “Success” or “Failure”, scan the system again and display the current installation status.

8. Press [*Enter*] to continue.

Uninstalling ProtectToolkit C

Should you encounter any problems while following this procedure, please see the section Unix Installation Utility Troubleshooting at the end of this chapter.

1. Start the *Unix Installation Utility.* See the Startup section above for further instructions if required.

2. From the Main Menu select *uninstall a SafeNet package*. A list of *SafeNet* packages that can be uninstalled is displayed.

3. Select the package required by typing the appropriate menu number and [*Enter*]. The utility verifies the action and then runs the appropriate command for the platform being used.

4. On some platforms, you may be prompted for additional options that may be used with the uninstall command. On Linux for example, you can add a `-nodeps` option to suppress the checking of dependencies. These options should be selected

with the normal care that is required whenever packages are installed or uninstalled.

5. After completing the uninstallation, the utility will show “Success” or “Failure”, scan the system again and display the current installation status.

6. You may now need to respond to any platform-specific messages to confirm that you wish to proceed with the uninstallation.

7. Press [*Enter*] to continue.

Unix Installation Utility Troubleshooting

Problem: Packages to install or uninstall are not visible

If you see no packages to install or uninstall close the utility and check that you are logged on as root and that your current directory is on the DVD before running the utility again.

Problem: The screen is confused or doesn’t display correctly

- This utility relies on the `TERM` environment parameter when creating colors and measuring screen size so make sure this is set accurately. The most common values are `xterm` or `vt100`. For example to set `TERM` to `vt100`:

```
# TERM=vt100
# export TERM
```

- If the screen is confused, run the utility in “plain” mode as follows:

```
# ./safeNet-install.sh -p
```

- If the size of the terminal is not correctly set by termcap (for example, the headings disappear off the top of the screen) then override the screen size with the `-s` option:

```
# ./safeNet-install.sh -s 24x80
```

- If using an X system terminal window, do not re-size the window while running the utility as it cannot sense the change in terminal screen size.

Problem: The backspace key does not operate correctly

On some terminals, the *backspace* key does not operate correctly. If after you type a number and then *backspace* you get something like “`2^H`” instead of an actual backspace you can either:

- Type the current `KILL` character (normally `^U`) and then enter the desired number (you will need to do this each time a backspace is required) or you can
- Exit the utility (perhaps with `^C`) and use the **stty**(1) command to correct the erase character before re-starting the utility. The command is:

```
# stty erase ^H
```

(Note that `^H` was the character created by pressing the *backspace* key)

This will fix the problem on a semi-permanent basis, for the current session in that terminal.

Command Reference

Syntax

```
safeNet-install.sh [-h] [-p] [-s <size>] [-v]
```

Description

This utility is for use on Unix/Linux systems only. The platforms supported are: AIX, Solaris,RHEL, and openSUSE. The utility handles installation uninstallation and configuration tasks using a simple, uniform menu driven interface.

Whenever *a SafeNet* package is installed with the utility it also installs itself on the host system hard disk (in `/usr/bin/safeNet-install.sh`). It can then be used when the DVD is not available, e.g. to uninstall or configure the software.

Options

The following options are supported:

`-h`	Show help.
`-p`	Plain mode. In this mode the ‘tput’ is not used for video enhancements.
`-s` *size*	Override the screen size (default = ‘tput lines/cols’ or 24x80).
`-V`	Print the version of this script.

Chapter 6
HSM Access Provider Installation

Operating Modes and Access Providers

As mentioned at the beginning of this guide, SafeNet high level cryptographic APIs such as ProtectToolkit C can be used in any one of three operating modes. This section applies to :

- **PCI mode** in conjunction with a PSI-E2 card installed locally.
- **Network mode** over a TCP/IP network, in conjunction with a PSE2 external appliance.

HSMs are used in PCI and network modes. In these cases **access provider software** is required. The role of the access provider is to provide the high-level cryptographic API with access to an associated HSM upon demand.

NOTE: You do not need to install/configure an access provider if you are using the software-only mode for development. You can return to this section at a later time if/when you wish to begin using an HSM.

The access provider software packages include the necessary device drivers that the high level cryptographic API uses to access and use and associated software such as maintenance utilities. These are required to establish and maintain a functioning high level cryptographic API using the selected operating mode.

It is not necessary to install access provider software when the high level cryptographic API is used in software-only mode (when available) for development and testing purposes.

In PCI mode an access provider and associated HSM are installed in the same machine.

In network mode the application and the high level cryptographic API are located remotely from the HSM across a network. In this case access providers are required on both the client and server machines. Additionally, if an adapter is used as the HSM, *Net Server* software must be installed on the machine where the HSM is installed.

The following figures show all possible operating mode scenarios and the associated software required in each case. ProtectToolkit C is shown as an example of a SafeNet high-level cryptographic API that may be used.

Figure 4: Example PCI Mode implementation using a PSI-E2

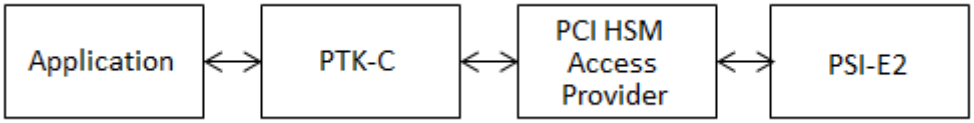
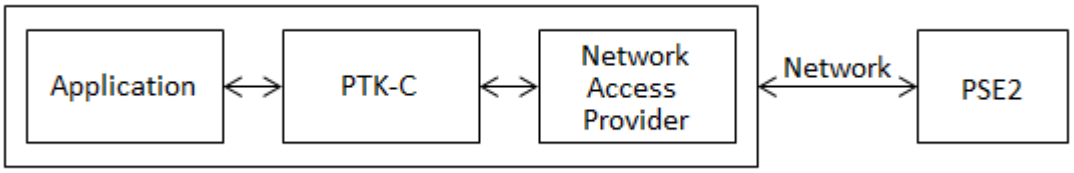


Figure 5: Example Network Mode implementation using a PSE2



Access Provider Types and Selection

To use a high-level cryptographic API in either PCI mode or network mode, HSM access providers must be installed.

PSI-E2 HSM Access Provider

The SafeNet PSI-E2 HSM Access Provider software package (file name: PTKpcihsm2) provides the device driver for a compatible and locally installed SafeNet cryptographic services adapter such as the *PSI-E2* (Figure 1).

- In **PCI mode**, PTKpcihsm2 must be installed, together with the high-level cryptographic API, on the local machine.

- In **network mode,** PTKpcihsm2 must be installed on the server side if a custom solution is developed using a SafeNet cryptographic services adapter such as the *ProtectServer* . Otherwise, it is not necessary to install SafeNet PSI-E2 HSM Access Provider software when using a high-level cryptographic API in network mode.

Network HSM Access Provider

In **network mode** the network HSM access provider software package (filename: PTKnethsm) must be installed, together with the high level cryptographic API, on the client side machine (Figures 1 and 2). The package includes the *Net Client* software required to provide hardware based cryptographic services utilizing remotely located SafeNet hardware devices over a TCP/IP based network.

HSM Net Server

In **network mode,** when a custom HSM solution is used, the HSM Net Server package (filename: PTKnetsvr) must be installed in the server side machine that is being used as the HSM (Figure 3). A SafeNet cryptographic services adapter such as the *ProtectServer* and the PCI HSM access provider software package (file name: PTKpcihsm2) must have been installed first.

Operating Mode Installation Overview

Access provider installation and configuration is part of an operating mode setup, as summarized in the following steps:

1. Install hardware

See the installation manuals provided with the hardware, such as the *ProtectServer Installation Guide.*

2. Install and configure access provider software

Access provider software must be installed and configured to support the operating mode required, as detailed in this Guide.

3. Install the high level cryptographic API

Install the high level cryptographic API to be used on your computer system, as detailed in the relevant installation guide supplied with the product.

4. Configure the high level cryptographic API

Generally, further configuration of the operating mode of the high level cryptographic API may need to be done to finalize installation. Tasks might include:

- establishing a trusted channel (secure messaging system (SMS) between the API and an associated HSM or

- establishing network communication between the client and one or more servers on the same network in network operating mode

For further information refer to your high-level cryptographic API documentation, such as the *ProtectToolkit C Administration Guide.*

PCI Mode Setup

When hardware-based cryptographic services are to be provided by utilizing a SafeNet adapter board (such as the *ProtectServer* installed on the local machine), a high-level cryptographic API is used in PCI mode.

Before configuring the high-level cryptographic API, ensure that you have done the following:

- Installed the SafeNet adapter card on your computer system. Please refer to the appropriate adapter installation manual, such as the *PSI-E2 Installation Guide,* for details on how to complete this installation.

- Installed the *SafeNet PSI-E2 HSM Access Provider* software package on your computer system. The *SafeNet PSI-E2 HSM Access Provider* includes the device driver that is required in order to access the adapter card. For further information see the relevant sections following for Windows systems or for Unix/Linux systems.

- Installed the high level cryptographic API on your computer system. Please refer to the installation guide provided with the API, as was described in the “Basic Installation...” chapters earlier in this guide.

Once the necessary software has been installed and correct operation of the hardware has been confirmed, proceed with configuration of the API including establishing an SMS if required.

Network Mode Setup

When hardware-based cryptographic services are to be provided by utilizing a remotely located (server side) SafeNet hardware device, a high-level cryptographic API is used in network mode. The SafeNet hardware device would typically be a standalone product such as a *ProtectHost* or a *ProtectServer External.* Alternatively, a SafeNet adapter board such as the *ProtectServer* together with SafeNet *Net Server* software could be used to create a custom solution for the server side.

The high-level cryptographic API is installed and configured on the client side computer system.

Before configuring the high-level cryptographic API, ensure that you have done the following:

- Installed the hardware and associated software at the remote location (server side) necessary to implement the planned solution.

  See the section later entitled “Sever Configuration for Network Mode” (if a custom HSM solution is to be used) and the installation manuals provided with the hardware for further information.

- Verified that the server machine is available on the same network as the client machine.

- Installed the *Network HSM Access Provider* software package on the client side.

  The *Network HSM Access Provider* includes the *net client* software. Using the *net client* software, a remotely located SafeNet hardware device can be accessed over a TCP/IP based network to obtain hardware based cryptographic services.

- Installed the high level cryptographic API on your computer system. Please refer to the installation guide provided with the API, such as the *ProtectToolkit C Installation Guide,* for details on how to do this.

  Once the necessary software has been installed and correct operation of the hardware has been confirmed, proceed with configuration of the API including establishing an SMS if required.

Windows Configuration for PCI Mode

Overview

After successful installation of the adapter, the next steps are to:

1. Install the *SafeNet PSI-E2 HSM Access Provider* package that includes the appropriate device driver

2. Confirm the correct operation of the adapter and driver package

This chapter provides the necessary instructions for Windows operating systems only. See 6 Linux Configuration for PCI Mode for Unix/Linux operating systems.

Windows uninstallation instructions are at the end of this chapter.

Installation

Preparation

Before following the procedure below, make sure that you are logged in as a member of the *Windows administrator group*.

Note: If at any time you see a system message stating that a SafeNet driver you are installing is not signed, you can safely ignore the message and proceed. The Microsoft WHQL certification process takes some time, so the first appearance of a new or updated driver might still be pending WHQL certification. SafeNet does not hold back a product release or an important fix for that certification. The same applies to Windows Logo, the successor to WHQL for Vista and Windows Server 2008.

When upgrading

To upgrade the software, first remove earlier versions and then follow the instructions for installation below. See the *Uninstallation* section at the end of this chapter for further information about uninstallation.

If this step is not carried out first the system may lock up. In the event that this happens, kill the session, perform the uninstallation, then perform the installation.

Procedure

1. Locate the installation DVD and execute the file **PTKpcihsm2.msi**. This is the PCI HSM Access Provider package that includes the device driver and hardware maintenance utilities.

2. Work through the installation wizard to complete the installation.

3. **NOTE:** A reboot may be required to successfully load the driver.

To verify correct installation

From a command prompt, type `hsmstate` to execute the *hsmstate* utility. If the adapter has been correctly installed the response will include:

```
HSM in NORMAL MODE. RESPONDING
```

Uninstallation

To uninstall the *SafeNet PSI-E2 HSM Access Provider* package, use the Windows **Programs and Features** control panel.

Linux Configuration for PCI Mode

Overview

After successful installation of the adapter, the next steps are to:

1 Install the SafeNet PSI-E2 HSM Access Provider package that includes the appropriate device driver for your operating system

2 Confirm the correct operation of the adapter and driver package

This chapter provides the necessary instructions for Unix/Linux operating systems only. See *6* Windows Configuration for PCI Mode for Windows operating systems.

Unix/Linux uninstallation is also discussed in the last section of this chapter.

Note: For systems that support 32-bit and 64-bit, the 32-bit libraries and executables are the default.

Installation

Use the Unix Installation Utility. A reboot may be required to successfully load the driver.

Linux

Preparation

Before adding or removing any packages, you must become the super-user on the host system.

The Linux driver is distributed as source code and must be compiled for the running kernel before loading as a dynamic module. In most cases the installation script will do this automatically provided the following points are observed:

1. The C compiler (`gcc`) must be available of the same version as that used to compile the kernel.

2. The **rpmbuild** package is installed.

3. The kernel source package is installed as appropriate to the running system. The kernel source is usually installed in `/usr/src/linux-<VER>` with a symbolic link from either: `/lib/modules/<VER>/build` or `/lib/modules/<VER>/source`

   where `<VER>` is the kernel version as reported by **`uname -r`**

Uninstallation

The simplest way to complete the uninstallation of the *SafeNet PSI-E2 HSM Access Provider* package on any of the Unix/Linux platforms is to use the *Unix Installation Utility.* By using the utility the correct commands for your platform will be executed automatically. See the section *Uninstalling an Access Provider Package* in Appendix A for the procedure.

Alternatively, if for any reason you wish to enter platform specific commands manually then further information can be found in Appendix A.

Client Configuration for Network Mode

When setting up a SafeNet high level cryptographic API such as ProtectToolkit C to operate in network mode the Network HSM Access Provider is used. See Appendix A for more information about network mode.

The Network HSM Access Provider package (PTKnethsm) is installed on the machine where the high level cryptographic API and the application are to be subsequently installed. Installation instructions for the Windows and Unix/Linux operating systems are given separately below.

Windows Installation

Preparation

Before following the procedure below, make sure that you are logged in as a member of the *Windows administrator group*.

When upgrading

To upgrade the software, first remove earlier versions and then follow the instructions for installation below. See the *Windows Uninstallation* section below for further information about uninstallation.

Procedure

1. Locate the installation DVD and execute the file PTKnethsm.msi. This is the Network HSM Access Provider package that includes the net client software.

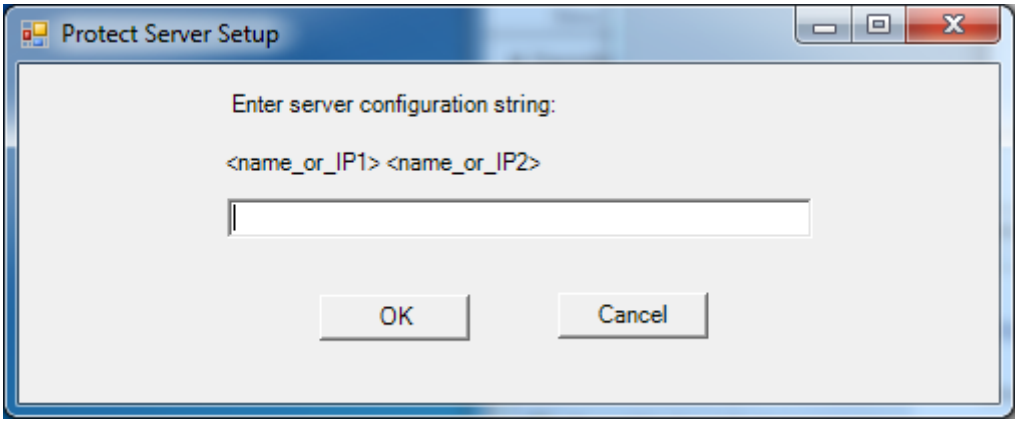
2. Work through the installation wizard to complete the installation.

   By default the PCI HSM Access Provider package is installed in the following directory:

   \Program Files\Safenet\Protect Toolkit 5\Network HSM

   A prompt during the installation allows you to change the default destination if required. Unless you have good reason to do otherwise, accept the default destination given.

   1. When the dialog box below displays, enter a server configuration string to enable access to slots on one or more HSMs across a network. If a configuration string is not entered, then the default server Localhost is used. This setting may be used for testing purposes to simulate access to HSM slots across a network when in fact the HSM is located in the local (client) machine.



You can specify the hostname or IP address of the server HSM. Separate one HSM string from the next using a single space. The server listening port is 12396

The server configuration string is stored as a configuration item (PTK_HSM_NETCLIENT_SERVERLIST) in the Windows registry. After installation, to change server details permanently change this configuration item's value. To change server details temporarily use an environment variable to override the registry setting. For further information about using configuration items see Appendix A.

Windows Uninstallation

To uninstall the *Network HSM Access Provider* package, use the **Programs and Features** Windows control panel.

Linux Installation

Use the Unix Installation Utility.

Making Configuration Changes

Configuration items can be used to customize the installation as required. These configuration items are listed in the following table. Default values are given in each case.

Configuration Item	Meaning
ET_HSM_NETCLIENT_HEARTBEAT =[ON|OFF]	If `ON`, net client is to request and support heartbeat messages from the Network Server. Default=`OFF`
ET_HSM_NETCLIENT_LOG_CHANNEL	Channel (destination) to write log entries to. Values are platform dependant. For Windows, valid values are: `0` – Windows Event Log `1` – Standard out `2` – Standard error Default=`0` For Unix/Linux, valid values are from 0

	to 7 inclusive, and map to syslog LOG_LOCAL# values. Default=0
ET_HSM_NETCLIENT_LOG_NAME	Name of application/context to associate with log entries. Default=etnetclient
ET_HSM_NETCLIENT_READ_TIMEOUT_SECS	Seconds to allow before timing out a TCP/IP read operation. Default=300
ET_HSM_NETCLIENT_SERVERLIST =[host[:port] [host[:port]…]]	Space separated list of hosts (with optional port number) to connect to. Default host=localhost Default port=12396
ET_HSM_NETCLIENT_WRITE_TIMEOUT_SECS	Seconds to allow before timing out a TCP/IP write operation. Default=60
ET_HSM_NETCLIENT_CONNECT_TIMEOUT_SECS	Number of seconds before a connection attempt is timed out. Default=60

Server Configuration for Network Mode

When setting up a SafeNet high level cryptographic API such as ProtectToolkit C to operate in network mode using a custom HSM solution, the HSM Net Server package is used. See the section Network Mode, earlier in this chapter, for more information about network mode.

The HSM Net Server package (filename: **PTKnetsvr**) must be installed in server side machines hosting a SafeNet cryptographic services adapter such as the *ProtectServer*. The cryptographic services adapter and the PCI HSM access provider software package (filename: **PTKpcihsm2**) must be installed first.

Installation instructions for the Windows and Unix/Linux operating systems are given separately below.

Windows Installation

Preparation

- Before following the procedure below, make sure that you are logged in as a member of the *Windows administrator group*.
- Ensure that the SafeNet cryptographic services adapter such as the *ProtectServer* has been installed.
- Ensure that the SafeNet PSI-E2 HSM Access Provider (PTKpcihsm2) has been installed. See 6 Windows Configuration for PCI Mode for further instructions if required.

When upgrading

To upgrade the software, first remove earlier versions and then follow the instructions for installation below. See the *Windows Uninstallation* section below for further information about uninstallation.

Procedure

1. On the installation DVD locate and execute the file PTKnetsrv.msi. This is the HSM Net Server package.

2. Work through the installation wizard to complete the installation.

Windows Uninstallation

To uninstall the Net Server package, use the **Programs and Features** Windows control panel.

Linux Installation

Use the Unix Installation Utility.

Boot Service Operation on Unix/Linux Platforms

To run the server as an `rc.d(init.d)` service, run the following script:

```
/opt/safenet/protecttoolkit5/netserv/bin/etnetsrv_install_rc
```

Making Configuration Changes

Configuration items can be used to customize the installation as required. These configuration items are listed in the following table. Default values are given in each case.

Configuration Item	Meaning
ET_HSM_NETSERVER_OLD_WORKER_COUNT	Number of threads to reserve for processing old ProtectToolkit C remote client connections. Default=3
ET_HSM_NETSERVER_V2_WORKER_COUNT	Number of worker threads, per HSM, to reserve for processing new net client connections. Default=3
ET_HSM_NETSERVER_READ_TIMEOUT_SECS	Number of seconds before a connection is timed out in a read operation. Default=30
ET_HSM_NETSERVER_WRITE_TIMEOUT_SECS	Number of seconds before a connection is timed out in a write operation. Default=30

Configuration Item	Meaning
ET_HSM_NETSERVER_CONN_TIMEOUT_COUNT	Number of inactivity timeouts on a connection that would cause the connection to be closed by the server. Each inactivity timeout period is 60 seconds. Default=3
ET_HSM_NETSERVER_FRAG_SIZE	The threshold value, in number of bytes, where output buffers are coalesced together before being sent via TCP. Servers with fast CPUs can keep this number high, and servers with slow CPUs need to keep this number low for best performance. This is an integer configuration item. Default=5000
ET_HSM_NETSERVER_ALLOW_RESET	Whether the server will allow the reset command to be issued or not. This is a string configuration item with the following valid values: Value — Effect Always — Always allow reset Never — Never allow reset OnHalt — Allow reset only when the HSM is not in normal mode Default=OnHalt
ET_HSM_NETSERVER_PORT	TCP port number to use. Default=12396
ET_HSM_NETSERVER_LOG_CHANNEL	Channel (destination) to write log entries to. Values are platform dependant. For Windows, valid values are: 0 – Windows Event Log 1 – Standard out 2 – Standard error Default=0 For Unix/Linux, valid values are from 0 to 7 inclusive, and map to syslog LOG_LOCAL# values. Default=0
ET_HSM_NETSERVER_LOG_NAME	Name of application/context to associate with log entries. Default=etnetserver

Appendix A

Using the Unix Installation Utility

Introduction

Package installation and uninstallation commands are different for each of the supported Unix/Linux platforms. To account for these differences the package must be installed or uninstalled using one of two possible methods. These are:

- manually, by using the commands that are specific to the operating system you are using
- by using the SafeNet Unix/Linux Installation Utility documented in this chapter

It is recommended that you use the installation utility unless there is good reason to do otherwise. Using the utility is easier and less prone to error. It is also more likely to result in a trouble-free installation or uninstallation.

The installation utility provides a simple, uniform menu driven interface. In addition to handling installation and uninstallation on Unix/Linux systems, it can also be used to perform the following tasks. Specifically, the utility can be used to:

- List SafeNet packages already installed
- Uninstall a SafeNet package
- List DVD contents for the current platform only or all platforms
- Install a package from the DVD (also installs the utility in /usr/bin)
- Change the default operating mode (PCI, network or software only).

Whenever a SafeNet package is installed using the installation utility, the utility is also installed on the host system hard disk (in `/usr/bin/safeNet-install.sh`). This allows you to use the installation utility when the DVD is not available (for example, to uninstall or configure the software).

Startup

Should you encounter any problems while following this procedure, please see the section Unix Installation Utility Troubleshooting at the end of this chapter.

The SafeNet *Unix Installation Utility* can be found in the root of the installation DVD.

1. Mount the DVD by following standard procedure for your particular platform and installation.

2. Change directory to the DVD and start the utility. For example:

```
# cd /misc/cd
# ./safeNet-install.sh
```

Note: There are options that can be specified when executing the `safeNet-install.sh` command. These options are not normally required and are mainly of use for troubleshooting purposes. The utility scans the system and the DVD and displays the *Main menu*.

```
SafeNet Unix Installation Utility
Hostname: leknek (Linux 2.6.38)
Main Menu
1 list SafeNet packages already installed
2 list packages on CD
3 install a package from this CD
4 uninstall a SafeNet package
5 Set the default cryptoki and/or hsm link

q quit the utility

Choice (1 2 3 4 5 q) [Redraw]:
```

Utility Navigation

Every menu screen shows the current Unix/Linux host and version as well as the menu location at the top of the screen (for example, "`Main Menu >> List CD menu`").

The valid key strokes for the current screen are shown at the bottom of the screen together with the default action (usually *Redraw*) which is shown in square brackets. To carry out the default action, press the *Enter* key.

To select a command from the menu press the corresponding numeric key.

Note: '`b`' is used for "back to the previous menu" and '`q`' to quit the utility. You can also quit with the system *INTR* key (normally `^C`).

Installing a Package

Should you encounter any problems while following this procedure, please see the section Unix Installation Utility Troubleshooting at the end of this chapter.

1. Start the *Unix Installation Utility.* See the Startup section above for further instructions if required.

2. From the Main Menu, select option **3 install a package from this CD**. A list of SafeNet packages that can be installed is displayed.

3. Select the package required by typing the appropriate menu number and *Enter*.

The utility verifies the action and then runs the appropriate command for the platform being used.

4. On some platforms, you may be prompted for additional options that may be used with the install command. On Linux for example, you can add a `–nodeps` option to suppress the checking of dependencies. These options should be selected with the normal care that is required whenever packages are installed or uninstalled.

5. You may now need to respond to any platform specific messages (for example, to confirm that you wish to proceed with the installation).

6. After installation, the utility will show "Success" or "Failure", scan the system again and display the current installation status.

7. Press the *Enter* key to continue.

Setting Up Your Environment

After installing the software, you must run the PTK **setvars.sh** script to configure your environment to use the PTK software. You cannot run the script directly, but instead you must source it or add it to a startup file (for example, **.bashrc**). If you source the script your environment will be set for the current session only. If you add it to your startup file, your environment will be set each time you log in.

To set up your environment

1. Go to the PTK software installation directory:

   cd /opt/safenet/protecttoolkit5/ptk

2. Source the **setvars.sh** script:

   . ./setenv.sh

Once installed and configured, the software is ready to use under `/opt/safenet`.

Uninstalling an Access Provider Package

Should you encounter any problems while following this procedure, please see the section Unix Installation Utility Troubleshooting at the end of this chapter.

1. Start the *Unix Installation Utility.* See the Startup section above for further instructions if required.

2. From the Main Menu select *uninstall a SafeNet package*.
   A list of SafeNet packages that can be uninstalled is displayed.

3. Select the package required by typing the appropriate menu number and *Enter*.

   The utility verifies the action and then runs the appropriate command for the platform being used.

4. On some platforms, you may be prompted for additional options that may be used with the uninstall command. On Linux for example, you can add a `-nodeps` option to suppress the checking of dependencies. These options should be selected with the normal care that is required whenever packages are installed or uninstalled.

5. After completing the uninstallation, the utility will show "Success" or "Failure", scan the system again and display the current installation status.

6. You may now need to respond to any platform-specific messages to confirm that you wish to proceed with the uninstallation.

7. Press the *Enter* key to continue.

Unix Installation Utility Troubleshooting

Problem: Packages to install or uninstall are not visible

If you see no packages to install or uninstall close the utility and check that you are logged on as root and that your current directory is on the DVD before running the utility again.

Problem: The screen is confused or does not display correctly

This utility relies on the `TERM` environment parameter when creating colors and measuring screen size so make sure this is set accurately. The most common values are `xterm` or `vt100`. For example to set `TERM` to `vt100`:

```
# TERM=vt100
# export TERM
```

If the screen is confused, run the utility in "plain" mode as follows:

```
# ./safeNet-install.sh -p
```

If the size of the terminal is not correctly set by termcap, (for example, the headings disappear off the top of the screen) then override the screen size with the `-s` option:

```
# ./safeNet-install.sh -s 24x80
```

If using an X system terminal window, do not re-size the window while running the utility as it cannot sense the change in terminal screen size.

Problem: The backspace key does not operate correctly

On some terminals, the *backspace* key does not operate correctly. If after you type a number and then *backspace* you get something like "`2^H`" instead of an actual backspace you can either:

- Type the current `KILL` character (normally `^U`) and then enter the desired number (you will need to do this each time a backspace is required) or you can

- Exit the utility (perhaps with `^C`) and use the **stty**(1) command to correct the erase character before re-starting the utility. The command is:

```
# stty erase ^H
```

(Note that `^H` was the character created by pressing the *backspace* key)

This will fix the problem on a semi-permanent basis, for the current session in that terminal.

Appendix B

Unix/Linux Command Reference

The simplest way to complete installation or uninstallation of ProtectToolkit C, or to change the Cryptoki provider on any of the Unix/Linux platforms, is to use the *Unix Installation Utility.* When using the utility, the correct commands for your platform are executed automatically. See the earlier chapters for further information:

Alternatively, if for any reason you wish to enter platform specific commands manually then the commands given in this chapter can be used.

Installation

Preparation

Before adding or removing packages, you must become the super-user on the host system.

The Runtime and SDK packages cannot be installed concurrently. To move from one package to the other, uninstall the package that is no longer required (see the Uninstallation section below) and then install the new one using the instructions that follow.

Procedure

The Runtime and SDK packages are packaged using the standard packaging software for each system. To install the software on your host system:

1. Refer to the following tables to locate the name of the package to be installed on your operating system.

Linux Platforms	
Runtime package	`PTKcprt`
SDK package	`PTKcpsdk`

Refer to the following table for the package required and locate the row for the correct operating system, as installed on the host system.

Use the program and commands listed to install the software.

Runtime Package		
Operating System	**Program**	**Example Commands**
Solaris (SPARC & Intel)	**`pkgadd`**`(1M)`	`pkgadd -d /cdrom/Solaris/PTKC_Runtime`

Linux	**`rpm`**`(8)`	`cd <path to DVD>/Linux/PTKC_Runtime`
		`rpm -i PTKcprt-x.xx-y.i386.rpm`
		(where x.xx-y refers to the version of the software)

AIX	**installp**	cd <path to DVD>/AIX/PTKC_Runtime installp -acgNQqwX -d . PTKcprt.rte

SDK Package		
Operating System	**Program**	**Example Commands**
Solaris (SPARC & Intel)	**pkgadd**(1M)	pkgadd -d /cdrom/Solaris/PTKC_SDK
Linux	**rpm**(8)	cd <path to DVD>/Linux/PTKC_SDK rpm -i PTKcpsdk-x.xx-y.i386.rpm (where x.xx-y refers to the version of the software)
AIX	**installp**	cd <path to DVD>/AIX/PTKC_SDK installp -acgNQqwX -d . PTKcpsdk.rte

Add the /opt/PTK/bin directory to the execution path and the /opt/PTK/lib directory to the library path. The following commands may be used to configure your paths for the **sh**(1) shell. Please consult your operating system manual for other shells.

Operating System	**Commands**
Solaris (SPARC & Intel) Linux	PATH=$PATH:/opt/PTK/bin export PATH LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/PTK/lib export LD_LIBRARY_PATH
Solaris (x86) 64-bit	PATH=$PATH:/opt/PTK/bin/amd64 export PATH LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/PTK/lib export LD_LIBRARY_PATH
AIX	PATH=$PATH:/opt/PTK/bin export PATH LIBPATH=$LIBPATH:/opt/PTK/lib export LIBPATH

Once installed, the software is ready to use under /opt/PTK.

Changing the Cryptoki Provider

Background

This section applies to the SDK package only.

Different ProtectToolkit C Cryptoki provider links are required depending upon whether an HSM or the software emulation is being used.

When the SDK package is installed both Cryptoki provider files are installed. The software only Cryptoki provider is made active by default.

Procedure

To change the default Cryptoki provider selection, simply use the appropriate item in the Unix/Linux Installation Utility **or** remove the soft-link:

```
/opt/safenet/protecttoolkit5/ptk/lib/libcryptoki.so or
/opt/safenet/protecttoolkit5/ptk/lib/libcryptoki.a (for AIX)
```

and recreate it to point to the SafeNet HSM Cryptoki provider. For example, the following shell commands may be used to enable the HSM (executed as the super-user):

```
# cd /opt/safenet/protecttoolkit5/ptk/lib
# rm libcryptoki.so
# ln -s libcthsm.so libcryptoki.so
```

The following shell commands may be used to enable the software emulation (executed as the super-user):

```
# cd /opt/safenet/protecttoolkit5/ptk/lib
# rm libcryptoki.so
# ln -s libctsw.so libcryptoki.so
```

Uninstallation

Preparation

Before adding or removing any packages, you must become the super-user on the host system.

Procedure

To uninstall the software from your host system:

1. Locate the row in the next table for the correct operating system, as installed on the host system

2. Identify the name of the package to be uninstalled from the following tables.

Linux, Solaris and AIX Platforms	
Runtime package	`PTKcprt` and/or `ERACcp8k` and/or `ERACcprc`
SDK package	`PTKcpsdk` and/or `ERACcpsdk`

3. Use the program and command listed to remove the software. Replace <*package name*> with the correct name of the package to be uninstalled.

Operating System	Program	Command
Solaris (SPARC & Intel)	**pkgrm**(1M)	pkgrm <*package name*>
Linux	**rpm**(8)	rpm -e <*package name*>
AIX	**installp***	installp -u <*package name*>

* **smit** can also be used

** **sam** can also be used

Appendix C

Configuration Items

Overview

Configuration items are created and maintained on the host operating system (platform) where the high level cryptographic API and access provider software is installed to store configuration information.

This appendix covers configuration items in detail so that access provider configuration changes can be made successfully if required.

If a change controlled by a configuration item is to be made then the applicable configuration item must be manually created and set to the value required using the information contained in this section.

Configuration items may exist at any one of four configuration levels. When a configuration item is queried, four locations corresponding to these levels are searched in order of precedence. This is explained in more detail below.

The four levels, in order of precedence, are:

- temporary configuration
- user configuration
- system configuration and
- default configuration

Default configuration items cannot be changed, however changes to configuration items can be made at the system, user or temporary levels and these changes will override the corresponding values at the default configuration level.

Any entries made at the temporary configuration level override any corresponding entries at the user or system levels and any entries at the user configuration level will override corresponding entries at the system level.

The exact nature and location of these configuration areas is platform specific. On Windows systems, user and system configuration information is stored in the Registry. On Unix/Linux based systems, configuration files are used. Temporary configuration items are implemented using environment variables on both Windows and Unix/Linux based platforms.

Regardless of the platform used a common convention has been followed to name configuration items. Understanding this naming convention will assist you to locate and change the appropriate configuration items when required.

Configuration items are hierarchical in structure, with the root node always being "PTK". Child nodes of the root represent the class of the item, and are typically product abbreviations, such as "PTKC" (ProtectToolkit C) or "HSM" (Hardware Security Module). Nodes under class represent the component, such as "LOGGER" or "SMS". Finally, nodes under component represent the configuration item, such as "FILE" or "MODE". Putting it all together, configuration items are of the form:

PTK_<class>_<component>_<item>

Platform Specific Details

Windows

Temporary Configuration is implemented using environment variables. Since environment variables are not hierarchical in nature, the hierarchy is implicitly defined by the name of the variable.

User Configuration is the registry tree starting from HKEY_CURRENT_USER\SOFTWARE\SafeNet.

System Configuration is the registry tree starting from HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet.

The User and System Configuration registry trees have a corresponding key for the class and component nodes. Entries contained in the component node key are strings whose names are of the form: PTK_<class>_<component>_<item>.

Example

The name of the ProtectToolkit C file where the *logger library* writes log information (*ctlog.log*) is stored in the Windows registry as a string value for the entry:

PTK_PTKC_LOGGER_ FILE

This is located in the key:

HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\PTKC\LOGGER

Unix/Linux

Temporary Configuration is implemented using environment variables. Since environment variables are not hierarchical in nature, the hierarchy is implicitly defined by the name of the variable.

User Configuration is a set of files located in the $HOME/.SafeNet directory.

System Configuration is a set of files located in the /etc/default directory.

The User and System Configuration files are of the form: et_<class>. Entries in the file are of the form: PTK_<class>_<component>_<item>=<value>.

Example

The name of the ProtectToolkit C file where the *logger library* writes log information (*ctlog.log*) is stored in the */etc/default/et_ptkc* file as the entry:

PTK_PTKC_LOGGER_FILE=/ctlog.log

Appendix D

Troubleshooting

The most common problems encountered when installing ProtectToolkit C and an encryption adapter card such as the ProtectServer, are due to the fact that access provider software for the adapter has not been loaded or is functioning incorrectly.\

Of particular note is a warning message that might appear when a Windows driver is being installed; if Windows complains that the SafeNet driver is not signed, you can safely ignore the warning, dismiss the dialog, and resume the installation. The message does not mean that your new SafeNet software is defective or dangerous. It merely means that the version you have received was released before it completed the Microsoft WHQL process. While we often do submit the Windows versions of our drivers for Windows Hardware Quality Labs (WHQL) certification, we do not normally hold back a product release or an important update while validation is pending. Note, however, that this assurance applies only to software that you have received directly from SafeNet or via a trusted third party seller.

If you encounter any difficulties:

- Check that you have followed all the installation instructions in this Guide and any associated manuals for the hardware and access provider software
- Follow any troubleshooting guidance given in the hardware and access provider manuals

Should you encounter any difficulties with the **gctadmin** and **kmu** utilities:

- The Java runtime might not have been installed prior to ProtectToolkit C. Uninstall both packages and reinstall them in the correct order.

If the issue is still not resolved please contact SafeNet Technical Support.

END OF DOCUMENT