SafeNet ProtectServer HSM Access Provider

Installation Guide

gemalto
security to be free

Part Number 007-006731-007
Version 5.2

Trademarks

Gemalto Rebranding

In early 2015, Gemalto NV completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the HSM product portfolio has been streamlined under the SafeNet brand. As a result, the ProtectServer/ProtectToolkit product line has been rebranded as follows:

Old product name	New product name
Protect Server External 2 (PSE2)	SafeNet ProtectServer Network HSM
Protect Server Internal Express 2 (PSI-E2)	SafeNet ProtectServer PCIe HSM
ProtectToolkit	SafeNet ProtectToolkit

Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the

product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

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 Gemalto support. Gemalto 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 Gemalto 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	
Address	Chapter 1 Gemalto NV 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	Global	+1 410-931-7520
	Australia	1800.020.183
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	000.800.100.4290
	Netherlands	0800.022.2996
	New Zealand	0800.440.359
	Portugal	800.1302.029
	Singapore	800.863.499
	Spain	900.938.717
	Sweden	020.791.028
	Switzerland	0800.564.849
	United Kingdom	0800.056.3158
	United States	(800) 545-6608
Web	www.safenet-inc.com	
Support and Downloads	Chapter 2 www.safenet-inc.com/support Provides access to the Gemalto Knowledge Base and quick downloads for various products.	
Technical Support Customer Portal	Chapter 3 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 Gemalto Knowledge Base.	

Revision History

Revision	Date	Reason
A	14 March 2016	Release 5.2

Contents

Chapter 1
Introduction

Before SafeNet HSMs such as the ProtectServer cryptographic adapter card can be used, a Hardware Security Module (HSM) access provider package must be installed. Access provider packages include any device drivers that may be required.

This guide will assist users to install access provider software, troubleshoot installations and make configuration changes. The contents of this guide is summarized below.

Chapter 2 provides an overview, covering the key concepts that must be understood in order to complete the installation and configuration successfully.

Chapters 3 through 6 cover the specifics of installation for each possible scenario. Read the chapters that apply in your case. Uninstallation instructions are also given in these chapters.

Chapter 7 covers the Unix Installation Utility, used for installation and configuration tasks on Unix machines.

Chapter 8 is a utilities command reference. It covers two command-line utilities, *hsmstate* and *hsmreset* (used to perform various hardware maintenance functions) and the Unix Installation Utility, *safeNet-install.sh*.

Chapter 9 is a Unix installation command reference. If the Unix Installation Utility is used then a knowledge of this information is not required.

Chapter 10 explains configuration items. Configuration items may need to be used to reconfigure the access provider software after a successful installation.

Chapter 11 provides help with troubleshooting.

Chapter 2
Operating Modes and Access Providers

SafeNet high level cryptographic APIs such as 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 *SafeNet ProtectServer Network HSM*
- Software-only mode, on a local machine without access to a hardware adapter, for development and testing purposes

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.

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 an SafeNet high-level cryptographic API that may be used.

Figure 1: PCI Mode

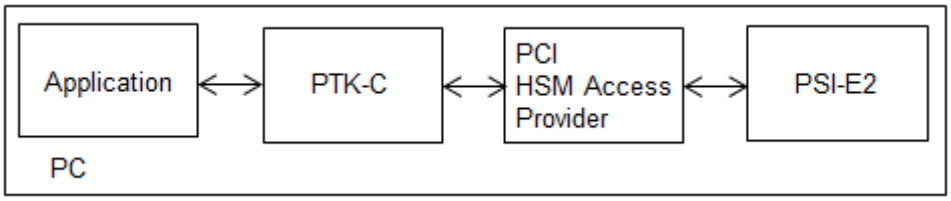


Figure 2: Network Mode using a SafeNet standalone HSM

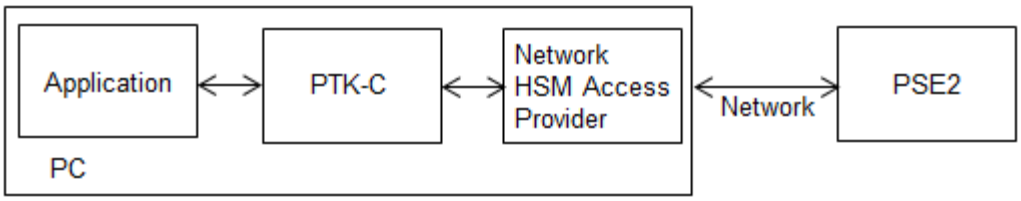
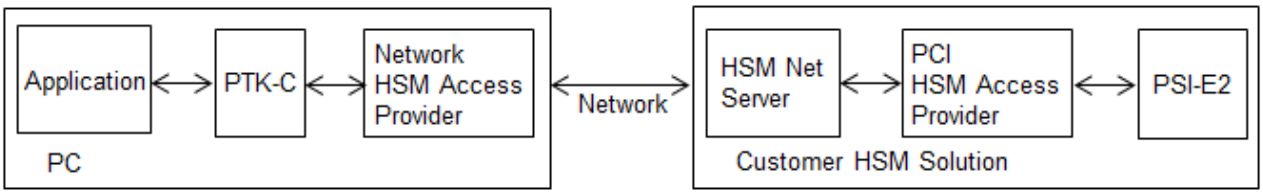


Figure 3: Network Mode using a SafeNet ProtectServer adapter



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.

PCI HSM Access Provider

The SafeNet ProtectServer PCI 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 *ProtectServer* (Figure 1).

- In PCI mode PTKpcihsm2 must be installed, together with the high-level cryptographic API, on the local machine.
- In network mode PTKpcihsm must be installed on the server side if a custom solution is developed using an SafeNet cryptographic services adapter such as the *ProtectServer.* Otherwise, it is not necessary to install the SafeNet ProtectServer

PCI HSM Access Provider software when using a high-level cryptographic API in network mode.

Network HSM Access Provider

In network mode the SafeNet ProtectServer 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 Network Server

In network mode, when a custom HSM solution is used, the SafeNet 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 SafeNet ProtectServer 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 *SafeNet ProtectServer Network HSM Installation Guide* and the *SafeNet ProtectServer PCIe HSM 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 *SafeNet ProtectToolkit C Administration Guide.*

PCI Mode Setup

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

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 *ProtectServer Installation Guide,* for details on how to complete this installation.
- Installed the SafeNet ProtectServer PCI HSM Access Provider software package on your computer system. The SafeNet ProtectServer PCI HSM Access Provider includes the device driver that is required in order to access the adapter card. For further information see for Windows systems and for Unix systems.
- 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.

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 *SafeNet ProtectServer Network HSM.* 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 (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 SafeNet ProtectServer 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 *SafeNet 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.

Chapter 3
Windows Configuration for PCI Mode

Overview

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

1. Install the *SafeNet ProtectServer PCI 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 Linux Configuration for PCI Mode for Unix 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*.

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 see *D* Troubleshooting for recovery instructions.

Procedure

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

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

   By default the *SafeNet PCI HSM AccessProvider* package is installed in the following directory:

   `\Program Files\SafeNet\Protect Toolkit 5\PCI HSM 2`

   A prompt during the installation allows you to change the default destination if required. Unless there is good reason, the default should be accepted.

   You will be prompted to install the driver. The driver is required.

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
```

For further information about the *hsmstate* utility refer to the hsmstate section in *A* Utilities Command Reference.

Uninstallation

To uninstall the *SafeNet PCI HSM AccessProvider* package, open the Windows *Control Panel* and double-click on the *Add/Remove Programs* icon. Then, locate the entry for the *SafeNet PCI HSM AccessProvider* and click on the *Change/Remove* button.

Chapter 4
Linux Configuration for PCI Mode

Overview

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

1. Install the SafeNet PCI HSM AccessProvider package that includes the appropriate device driver for your operating system

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

Installation

After reading the following section on the Unix Installation Utility, refer to and follow the instructions in the section for the operating system installed on the host computer system.

The Unix Installation Utility

The SafeNet PCI HSM AccessProvider installation and uninstallation commands are different for each of the supported Unix platforms. These differences are in *B* Unix Installation Command Reference. To account for these differences automatically during installation of the package, you should use the Unix Installation Utility as directed in the platform-specific procedures.

Alternatively, if for any reason you wish to enter platform-specific commands manually. then the commands given in *B* Unix Installation Command Reference can be used.

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`**

To install the device driver for Linux

1. Mount the installation CD-ROM and change to the directory. For example:

   ```
   # cd /cdrom/cdrom0/
   ```

2. Use the Unix Installation Utility. Select the PCI HSM AccessProvider device driver package from the Install Menu. See "Using the Unix Installation Utility" for further guidance if required. This will install the PCI HSM AccessProvider package that includes the device driver, and test utilities as well as the manual pages for these programs. By default they will be installed into `/opt/safenet`.

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

Chapter 5
Client Configuration for Network Mode

When setting up an SafeNet high level cryptographic API such as ProtectToolkit C to operate in network mode the Network HSM Access Provider is used. See Operating Modes and Access Providers for more information about network mode.

The SafeNet ProtectServer 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 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.

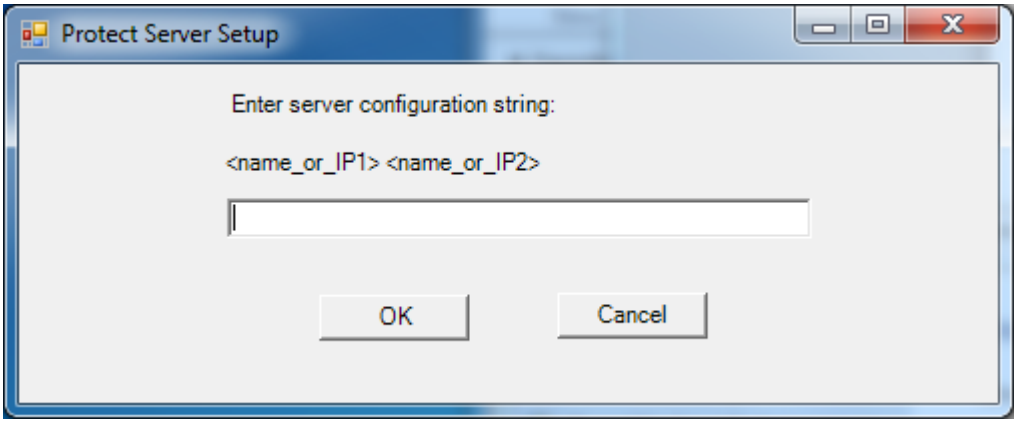
2. Work through the installation wizard to complete the installation.

   By default the *SafeNet ProtectServer Network 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.

3. 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 *C* Configuration Items.

To verify correct installation

Correct installation can be verified using the *ctkmu* command line utility. With ProtectToolkit C installed, type `ctkmu l` from a command prompt. If the package has been correctly installed a listing of all available slots on the server side HSM(s) displays.

If required, further information about the *ctkmu* command line utility can be found in the *SafeNet ProtectToolkit C Administration Manual*.

Windows Uninstallation

To uninstall the *SafeNet ProtectServer 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. For further information about using configuration items see *C* Configuration Items.

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, 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` IPv6 addresses must be enclosed in square brackets.
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`

Chapter 6
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 Operating Modes and Access Providers for more information about network mode.

The SafeNet 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 (file name: PTKpcihsm2) must be installed first. Installation instructions for the Windows and Unix 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 PCI HSM AccessProvider (PTKpcihsm2) has been installed. See 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 *SafeNet HSM Net Server* package.

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

Windows Uninstallation

To uninstall the *SafeNet HSM 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/netsrv/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. For further information about using configuration items see Appendix C Configuration Items.

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
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

Configuration Item	Meaning
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 dependent. For Windows, valid values are: 0 – Windows Event Log 1 – Standard out 2 – Standard error Default=0 For Unix, 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
ET_HSM_NETSERVER_LOG_LEVEL	Amount of tracing to generate 0 = Startup and Errors 1 = Startup + errors + client connections Default=0

Chapter 7
Using the Unix Installation Utility

Introduction

Access provider installation and uninstallation commands are different for each of the supported Unix platforms. These differences are documented in *B* Unix Installation Command Reference. 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 as given in Unix Installation Command Reference that are specific to the operating system you are using or
- by using the SafeNet Unix Installation Utility documented in this chapter

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 also more likely to result in a trouble free installation or uninstallation.

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

- List SafeNet packages already installed
- Uninstall an 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 (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.

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. For example:

   ```
   # cd /misc/cd
   ```

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

Note:
Options 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 `safeNet-install.sh` entry in *A* Utilities Command Reference.

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

```
SafeNet Unix Installation Utility (version 28):
Hostname: leknek (Linux 2.6.18-92.el5xen)
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

q quit the utility


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

Utility Navigation

Every menu screen shows the current Unix 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 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 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 followed by *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:

   . ./setvars.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 an 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.

Chapter 8
Utilities Command Reference

Overview

This chapter provides command reference details for the Unix Installation Utility and the SafeNet hardware maintenance utilities.

Unix Installation Utility

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

Hardware Maintenance Utilities

The SafeNet hardware maintenance utilities are installed during the PCI HSM and network HSM access provider installations. The utilities provided depends upon whether you are using the legacy platform, or the new updated platform. The utilities are named as follows:

- *e8kstate* and *e8kreset* (on systems using the older ERACe8k packages) or
- *hsmstate* and *hsmreset*, (on systems using the newer PTKpcihsm2 packages)

safeNet-install.sh

Syntax

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

Description

This utility is for use on Unix/Linux systems only. 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 CD-ROM is not available (for example, to uninstall or configure the software).

For further information about using this utility see Using the Unix Installation Utility.

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.

hsmstate

Syntax

`hsmstate [-d<instance>] [-h] [-?] [-v] [-q]` or

Description

The utility is used to display the current status of the HSM(s). By default it will report all HSMs found in the system. Each HSM device will be listed as it is found.

Some of the potential states reported may include:
- HSM in NORMAL MODE.
- HSM is responding to tamper.
- HSM is initializing performing POST.

Options

The following options are supported:

`–d instance`	`--device=instance`	This will make the utility report only on the device instance specified if found present in the system.
`-h,-?`	`--help`	Display helpful usage information.
`-v`	`--verbose`	Verbose flag. This will display a more detailed report about the HSM.
`-q`	`--quick`	Quick mode. Prints the state of the HSM and then exits (does not send any requests).

Examples

The command "`hsmstate`" will show all devices found in the system. For example:

```
HSM device 0:      HSM in NORMAL MODE. RESPONDING
HSM device 1:      HSM in NORMAL MODE. RESPONDING
HSM device 2:      HSM in NORMAL MODE. RESPONDING
```

The command "`hsmstate -d1 –v`" will show a report with full details about device 1. For example:

```
HSM device 1:      HSM in NORMAL MODE. RESPONDING to requests.
State = (0x8000, 0x41403)
I2O_INBOARD_MF_OFFSET = 0kb Reserved memory at beginning of
PCI Window
I2O_FRAME_LENGTH = 4kb Length of an I2O Message Frame in
KiloBytes
I2O_NUM_FRAMES = 20  Number of message frames in one direction
Host Interface version = V0.3
```

Note: There is no requirement to interpret the information presented from the –v option, since these values may only be required when contacting technical support.

hsmreset

Syntax

`hsmreset [-d<instance>] [-f] [-h] [-?] [-v]` or

Description

The utility is used to clear the HSM of any outstanding requests, ready the device to load any new command and continue normal operation. It can be used when the HSM is either in normal or halt state.

Options

The following options are supported:

`–d instance`	`--device=instance`	This will make the utility reset only the device instance specified if found to be present in the system.
`-f`	`--force`	Force an HSM reset without prompting for confirmation.
`-h,-?`	`--help`	Display helpful usage information.
`-v`	`--verbose`	Verbose flag. This will display a more detailed report about the HSM.

Example

- The command "`hsmreset`" will reset the first HSM. Upon execution the following message displays.

  ```
  HSM is in normal mode. Resetting it might disturb other applications.

  Continue [N/Y]:
  ```

- Type `Y` to complete the operation.

Chapter 9
Unix Installation Command Reference

The simplest way to complete installation or uninstallation of an *Access Provider* package on any of the Unix platforms is to use the *Unix Installation Utility.* By using the utility the correct commands for your platform will be executed automatically. See Windows Configuration for PCI Mode and Linux Configuration for PCI Mode 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

Locate the section below for the correct access provider type and the operating system installed on the host computer system. Then follow any instructions and the syntax given.

PCI HSM Access Provider Commands

Linux

The driver is installed by executing the following as 'root' (super-user):

```
# cd /cdrom/cdrom0/Linux/pci_hsm_access_provider
rpm -i PTKpcihsm2-X.X-X.i386.rpm
```

If the compile fails or the driver does not come up automatically (hsmstate fails) you will need to correct the problem and then "`cd /opt/ETpcihsm/src`" and invoke `make(1)` as root. The `Makefile` in that directory has some notes to help you get the driver compiled correctly.

Uninstallation

Locate the section below for the correct access provider type and the operating system installed on the host computer system. Then follow any instructions and the syntax given.

PCI HSM Access Provider Commands

Linux

To remove the software from your host system simply use the **`rpm`**`(8)` command with the appropriate package name as a parameter.

For example:

```
# rpm -e PTKpcihsm2
```

Chapter 10
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 based systems, configuration files are used. Temporary configuration items are implemented using environment variables on both Windows and Unix 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 "ET". 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:

ET_<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: ET_<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:

ET_PTKC_LOGGER_ FILE

This is located in the key:

HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\PTKC\LOGGER

Unix

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: ET_<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:

ET_PTKC_LOGGER_FILE=/ctlog.log

Chapter 11
Troubleshooting

Overview

If you have difficulties during installation, please first check that you have followed all the installation instructions in this guide and other applicable guides where referenced. The information provided below may be of further assistance. If you still cannot resolve the issue, please contact your supplier or SafeNet support. See the *Preface* for further information.

Known Issues

System Locks Up

The system locks up after installation of the SafeNet PCI HSM AccessProvider device driver package. This may happen if a prior version of the device driver exists on the system.

Solution:

1. Power-down and remove the adapter.
2. Power up.
3. Uninstall all versions (old and new) of the SafeNet PCI HSM AccessProvider / device driver package.
4. Power-down and re-install the adapter.
5. Power-up and reinstall the SafeNet PCI HSM AccessProvider package

Adapter Not Responding

Following re-installation of a previously removed adapter or the addition of another adapter, the device driver cannot find the device or an adapter is not responding.

Confirm that the adapter(s) are firmly seated in the PCI slot, then uninstall the SafeNet PCI HSM AccessProvider package. Following this, perform a fresh install of the SafeNet PCI HSM AccessProvider package.

Simple Fault Diagnosis

Fault Diagnosis Utilities

To carry out simple fault diagnosis, SafeNet hardware maintenance utilities hsmstate and hsmreset can be used. These are installed as part of the SafeNet PCI HSM AccessProvider installation.

Further information about these utilities, beyond that covered in this chapter, can be found in *A* Utilities Command Reference.

Fault Diagnosis Procedure

- From a command prompt, execute either the *hsmstate* or the *e8kstate* utility as applicable (see above).

  The output from the utility should include "... NORMAL mode, Responding".

- If the utility reports "... HALTED due to a failure":

  Execute either the *hsmreset* or the *e8kreset* utility as applicable (see above).

  After the reset, check to see if the *hsmstate* or the *e8kstate* utility is now reporting NORMAL operation.

- If the utility reports "... waiting for tamper cause to be removed" and an adapter PCI card is being used:

- Check to see that external tamper detectors connected to the board are correctly configured if these are being used.

- Make sure the adapter is seated firmly and correctly in the PCI slot.

END OF DOCUMENT