SafeNet ProtectServer PCIe HSM

Installation Guide

gemalto
security to be free

Part Number 007-002924-007
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	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	www.safenet-inc.com/support Provides access to the Gemalto Knowledge Base and quick downloads for various products.	
Technical Support Customer Portal	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

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 1
Introduction

Product Overview

The SafeNet ProtectServer PCIe HSM is the second-generation intelligent ProtectServre cryptographic services PCIe adapter, replacing the ProtectServer PSI-E.

When using Safenet ProtectServer, generic processing or high-speed DES and RSA hardware acceleration may be employed. Secure key storage is provided using persistent, tamper protected memory. In addition, multiple adapters may be used in a single host computer in order to improve throughput or to provide redundancy.

About This Manual

This manual is provided as an instructional aid for the installation of a SafeNet ProtectServer cryptographic services hardware adapter.

Installation of the associated *SafeNet ProtectServer PCIe HSM Access Provider* package (PTKpcihsm2) is described in the companion manual, *SafeNet ProtectServer HSM Access Provider Installation Guide*. The *SafeNet PCI HSM Access Provider* package includes the device driver.

Chapter 2 provides the overall installation procedure.

Chapter 3 provides some troubleshooting guidance.

Appendix A is a hardware reference. This provides instructions on how to modify the adapter's printed circuit board when external tamper detectors are to be used. The adapter's serial port specifications are also documented here.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 2
SafeNet ProtectServer PCIe HSM Installation

Installation Summary

To install and commission a SafeNet ProtectServer PCIe HSM card and its associated software, follow the steps below. Where required, these steps are covered in more detail in the sections that follow.

1. Check the items received to ensure none are missing. A separate page that lists the items included is provided for this purpose.

2. Move the battery jumper from the OFF position to the ON position (see “The Battery Jumper Header” on page 4).

3. If an external tamper detector is to be used, ensure that the external device has a two-conductor cable with a connector suitable to mate with the tamper-detect connector on the ProtectServer adapter (detailed at the beginning of Appendix A).

4. Install the SafeNet ProtectServer PCIe HSM card in the host computer system.

5. Install the HSM Access Provider package that includes the device driver and confirm the correct operation of the adapter and driver installation.

6. Use the included USB-to-serial cable to attach a serial device Install the smart card reader if provided.

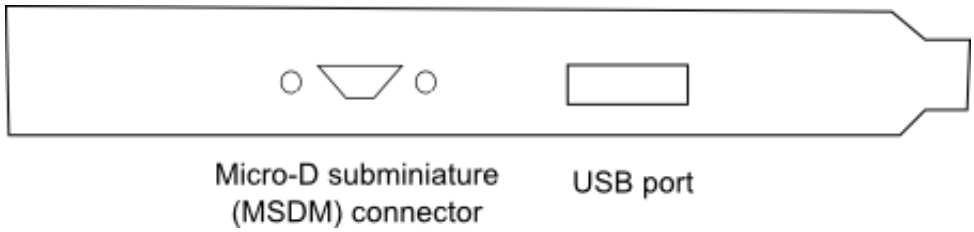
7. Install the SafeNet application programming interface (API) or net server software supplied with the product.

Adapter Features

The SafeNet ProtectServer PCIe HSM is a standard PCIe device that can be fitted into any spare PCIe slot on the motherboard in formats x4, x8, or x16.

The Card Faceplate

The faceplate of the card provides two ports, as illustrated below:



The USB Port

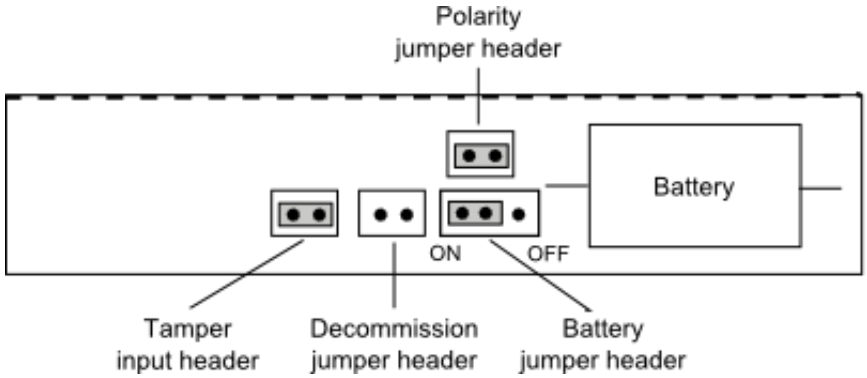
The USB port is used to connect a serial device, such as a smart card reader, to the card using the included USB-to-serial adapter.

The MSDM Connector

The micro-D subminiature (MDSM) connector is not used.

Battery and Jumper Headers

The card is also equipped with a battery and a series of jumper headers located at the rear of the card, as illustrated below:



The Battery

The battery mounted directly to the card and maintains the internal flash memory. Transport mode requires that the battery remain connected.

If the HSM is to be kept in storage (without keys present) it is recommended that you isolate or disconnect the battery to avoid wearing it down, thus extending its lifespan. You can use the **ctconf** command to test the condition of the battery. If the Battery Status indication does not report as GOOD, backup the HSM keys before powering down the PC to avoid losing the keys.

Note: Disconnecting the battery deletes all key material on the HSM. Ensure that you back up you HSM before disconnecting the power. The keys are not deleted immediately. Capacitors continue to supply power for approximately 30 seconds after battery disconnect.

The Battery Jumper Header

The battery jumper is a three-pin jumper that is used to engage or disengage the battery.

The battery is in the ON position when a jumper is inserted on the center and left pins, as shown above.

The battery is in the OFF position when a jumper is inserted on the center and right pins. This setting is not required for normal operation.

CAUTION! Do not change the jumper setting unless instructed by SafeNet support.

The Decommission Jumper Header

Place a jumper on the decommission jumper header to decommission the HSM. Decommissioning deletes all of the key material on the HSM.

The Tamper Input Header

The tamper-input header used to connect an external tamper device to the card. By default it has a jumper in place, across the two pins in the header. If an external tamper detection device is to be used, run a two-wire cable to your chassis-tamper switch or other device that must operate to open the circuit if a tamper event occurs.

The Polarity Jumper Header

The polarity jumper header is used to configure the operating mode of the card. Do not change the jumper setting for this header.

Installing the Adapter

The adapter is a PCI Specification 2.2 compliant device. It may be fitted in any spare PCIe slot on the motherboard in formats x4, x8, or x16. If you are unsure which is a PCIe slot, please consult the documentation accompanying your host system motherboard.

If you are using a tamper-detection device, route the cable to it before closing the computer cover.

PCI HSM Access Provider Installation

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

1. Install the *HSM Access Provider* package (PTKpcihsm2).
2. Confirm the correct operation of the adapter and driver package.

These steps are covered in the SafeNet *ProtectServer HSM Access Provider Installation Guide* for both Windows and Unix/Linux systems.

Smart Card Reader Installation

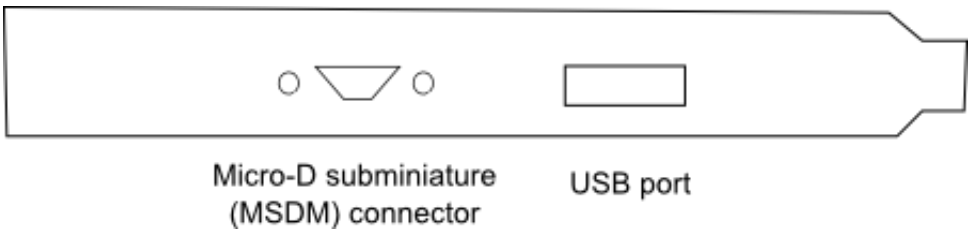
The SafeNet ProtectServer PCIe HSM offers functionality supporting the use of smart cards. To make use of these features, you must use a SafeNet-supplied smart card reader. Smart card readers, other than those supplied by SafeNet, are not supported.

The SafeNet ProtectServer PCIe HSM supports two different card readers, as follows:

- the new USB card reader (introduced in 5.2)
- the legacy card reader, which provides a serial interface for data (via a USB-to-serial cable) and a PS/2 inteface for power (direct or via a PS/2 to USB adapter)

Installing the USB smart card reader

To install the USB card reader, simply plug the card reader into the HSM USB port, as illustrated below.



Installing the legacy card reader

To install the smart card reader, use the included USB-to-serial cable to connect it to the HSM USB port on the card faceplate.

The card reader qualified with the ProtectServer product also requires connection to a PS/2 port for its power. Many newer servers have USB ports, but do not provide a PS/2 connection.

The options are:

- Connect a PS/2-to-USB adapter cable (pink) between the card reader and a USB port on the host computer.
- If you prefer to not expose USB ports on your crypto server (for security reasons), then connect a PS/2-to-USB adapter cable between the card reader and a standalone powered USB hub.

Again, the USB connection is for power only. No data transfer occurs.

Completing Installation

Following the PCI HSM Access Provider installation, to make use of the ProtectServer, you will need to install the supplied SafeNet API or net server software.

Please refer to the installation instructions in the appropriate manual, such as the *SafeNet ProtectToolkit C Installation Guide*.

Chapter 3
Troubleshooting

Overview

The most common problem encountered with installing the SafeNet ProtectServer PCIe HSM is that the device driver is not loaded or functioning correctly.

Should you encounter any difficulties, first check that you have followed all the installation instructions in this manual and the *HSM Access Provider Installation Guide*. 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

Problem

The MSI (Microsoft Installer) application does not complete installation, or is left in an unstable state.

Solution

This fault can occur if there are no free IRQs that can be assigned to the device. Make sure the device is assigned an IRQ. The IRQs assigned to devices are usually displayed when a system is powered up.

Problem

The system locks up after installation of the HSM Access Provider 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 HSM Access Provider / device driver package.

4. Power down and re-install the adapter.

5. Power up and reinstall the HSM Access Provider package.

Problem

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.

Solution

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

Problem

When operating multiple adapters under Windows 2000 or later, the adapters run slowly or even stall. Some commands may work correctly on one adapter, but not the other.

Solution

This problem may be resolved by resetting the configuration data in the host system BIOS.

Simple Fault Diagnosis

Fault Diagnosis Utilities

To carry out simple fault diagnosis, SafeNet hardware maintenance utilities can be used. These are installed as part of the ProtectServer PCI HSM Access Provider installation. There are two utilities: ***hsmstate*** and ***hsmreset***

Further information about these utilities, beyond what is covered in this chapter, can be found in the *HSM Access Provider Installation Guide.*

Fault Diagnosis Procedure

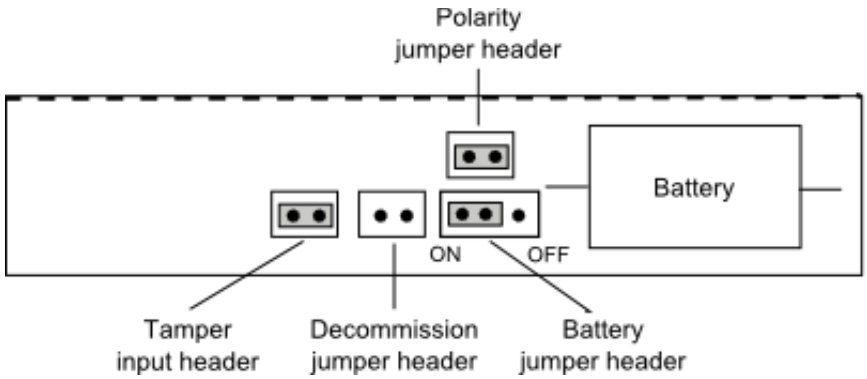
From a command prompt, execute ***hsmstate***. The output from the utility should include "... NORMAL mode, Responding".

- If the utility reports "... HALTED due to a failure":
    - Execute ***hsmreset***.
    - Following the reset, check to see if the ***hsmstate*** is now reporting NORMAL operation.
- If the utility reports "... waiting for tamper cause to be removed":
- Check to see that external tamper detectors connected to the board are correctly configured if these are being used.
- Make sure the adapter is sitting firmly and correctly in the PCI slot.

Chapter 4
Hardware Reference

Adapter Modification for External Tamper Detectors

Provision has been made to allow users to connect additional tamper detection devices using the tamper input header, located on the rear of the card, as illustrated below.



To fit an external tamper detection device, such as a micro switch on the cover of the host system, first remove the default jumper/shunt that bridges the two posts in the ProtectServer adapter's tamper input header. Connect your external tamper device in place of that shunt. You will need the cable end from your tamper-detection device to match the Molex socket on the adapter.

The required insertable shell, or connector housing is Molex part 35507-0200. It must be installed on the end of your tamper-device's two-wire cable, in order to insert into the tamper-detection socket on the ProtectServer adapter.

Crimp a pair of Molex 50212-8100, 2mm WTB crimp terminals to the ends of the wires coming from your tamper switch, and insert the crimped terminal sockets into the Molex connector housing.

Plug the connector end of the assembled cable into the tamper-detect socket on the PCIe adapter.

In the un-tampered condition, any external device must provide a low impedance path (i.e., short circuit) between the posts of the tamper-detect connector.In the tampered condition, the external device must show an open circuit.

The Battery

The adapter is fitted with a battery, which is used to maintain keys and the correct time on the adapter when the PCIe connector is un-powered (such as, when the Host computer is shutdown).

The expected lifetime of the battery is 10 years, so it should not require replacement in the normal lifetime of the adapter.

Testing the battery

You can use the utilities provided with the adapter to query the state of the battery, but it reports only “low” or not (see below). For example, if ProtectToolkit C is being used, then the ctconf utility displays the state of the battery (Good/Low). See the Administration Guides for the software you are running for details on how you can check the battery status.

The RealTime Clock and memory retain their data as long as the adapter is in a powered system. The RTC performs a check of battery level daily. If a low-battery warning is detected on an adapter that has been un-powered/removed from a system, then the data in the memory can be considered suspect. If a low-battery warning is detected on an adapter that has been continuously powered, then the data in memory can be trusted (for you to make a backup before proceeding with battery replacement).

Port Specifications

The USB-to-serial cable provides an RS232 port with pin outs as shown in *Figure 6*. That port can be used for connecting a smart card reader or some other serial device.

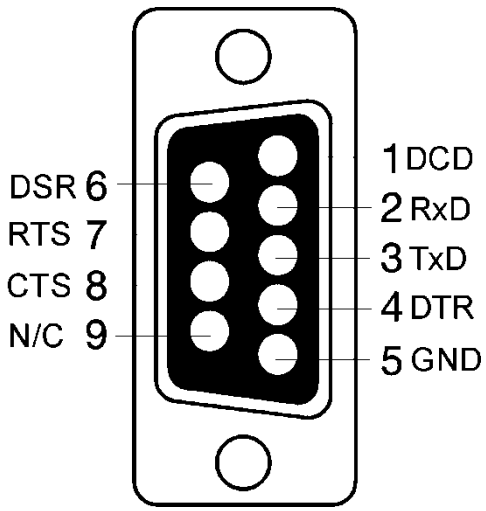


Figure 6 – Adapter serial connector

END OF DOCUMENT