

SafeNet ProtectServer Network HSM Plus 5.5

INSTALLATION AND CONFIGURATION GUIDE



Document Information

Product Version	5.5
Document Part Number	007-013682-003
Release Date	08 January 2020

Revision History

Revision	Date	Reason
Rev. A	08 January 2020	Initial release

Trademarks, Copyrights, and Third-Party Software

Copyright 2009-2020 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto 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, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- > This document shall not be posted on any publicly accessible 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.

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of Gemalto.

CONTENTS

Preface: About the SafeNet ProtectServer Network HSM Plus Installation and Configuration Guide	6
Customer Release Notes	6
Audience	6
Document Conventions	7
Notes	7
Cautions	7
Warnings	7
Command Syntax and Typeface Conventions	8
Support Contacts	9
Customer Support Portal	9
Telephone Support	9
Chapter 1: Product Overview	10
Physical Features	10
Front panel view	11
Rear panel view	12
Cryptographic architecture	13
Summary of Cryptographic Service Provider setup	14
Chapter 2: SafeNet ProtectServer Network HSM Plus Hardware Installation	15
SafeNet ProtectServer Network HSM Plus Required Items	16
Installing the SafeNet ProtectServer Network HSM Plus Hardware	18
Installation Notes	18
Installing the SafeNet ProtectServer Network HSM Plus Hardware	18
Chapter 3: Deployment Guidelines	22
Secure Messaging System (SMS)	22
Networking and Firewall Configuration	23
Separation of Roles	23
Chapter 4: Testing and Configuration	25
First Log in and System Test	25
Access the Console	25
Power on and Log in	26
Run System Test	26
Network Configuration	27
Gathering Appliance Network Information	27
Configuring the Network Parameters	28
SSH Network Access	30

Powering off the SafeNet ProtectServer Network HSM Plus	30
Troubleshooting	31
Appendix A: Technical Specifications	32
Appendix B: Glossary	33

PREFACE:

About the SafeNet ProtectServer Network HSM Plus Installation and Configuration Guide

This Guide is provided as an instructional aid for the installation and configuration of a SafeNet ProtectServer Network HSM Plus cryptographic services hardware security module (HSM). It contains the following sections:

- > ["Product Overview" on page 10](#)
- > ["SafeNet ProtectServer Network HSM Plus Hardware Installation" on page 15](#)
- > ["Testing and Configuration" on page 1](#)
- > ["Technical specifications" on page 1](#)
- > ["Glossary" on page 33](#)

This preface also includes the following information about this document:

- > ["Customer Release Notes" below](#)
- > ["Gemalto Rebranding" on page 1](#)
- > ["Audience" below](#)
- > ["Document Conventions" on the next page](#)
- > ["Support Contacts" on page 9](#)

For information regarding the document status and revision history, see ["Document Information" on page 2](#).

Customer Release Notes

The customer release notes (CRN) provide important information about this release that is not included in the customer documentation. It is strongly recommended that you read the CRN to fully understand the capabilities, limitations, and known issues for this release. You can view or download the latest version of the CRN for this release at the following location:

http://www.securedbysafenet.com/releasenotes/ptk/crn_ptk_5-4.pdf

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet ProtectToolkit users and security officers, key manager administrators, and network administrators.

All products manufactured and distributed by Gemalto are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

It is assumed that the users of this document are proficient with security concepts.

Document Conventions

This document uses standard conventions for describing the user interface and for alerting you to important information.

Notes

Notes are used to alert you to important or helpful information. They use the following format:

NOTE Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. They use the following format:

CAUTION! Exercise caution. Contains important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. They use the following format:

****WARNING**** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command Syntax and Typeface Conventions

Format	Convention
bold	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> > Command-line commands and options (Type dir /p.) > Button names (Click Save As.) > Check box and radio button names (Select the Print Duplex check box.) > Dialog box titles (On the Protect Document dialog box, click Yes.) > Field names (User Name: Enter the name of the user.) > Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) > User input (In the Date box, type April 1.)
<i>italics</i>	In type, the italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Represent optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
{a b c} {<a> <c>}	Represent required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
[a b c] [<a> <c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or [Gemalto Customer Support](#).

Gemalto Customer 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.

Customer Support Portal

The Customer Support Portal, at <https://supportportal.gemalto.com>, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone. Calls to Gemalto Customer Support are handled on a priority basis.

Region	Telephone number
	(Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Global	+1 410-931-7520
Australia	1800.020.183
China	North: 10800-713-1971 South: 10800-1301-932
France	0800-912-857
Germany	0800-181-6374
India	000.800.100.4290
Israel	180-931-5798
Italy	800-786-421
Japan	0066 3382 1699
Korea	+82 2 3429 1055
Netherlands	0800.022.2996
New Zealand	0800.440.359
Portugal	800.863.499
Singapore	800.1302.029
Spain	900.938.717
Sweden	020.791.028
Switzerland	0800.564.849
United Kingdom	0800.056.3158
United States	(800) 545-6608

CHAPTER 1:

Product Overview

The SafeNet ProtectServer Network HSM Plus is a self-contained, security-hardened server providing hardware-based cryptographic functionality through a TCP/IP network connection. Together with high-level SafeNet application programming interface (API) software, it provides cryptographic services for a wide range of secure applications.

The SafeNet ProtectServer Network HSM Plus is PC-based. The enclosure is a heavy-duty steel case with common PC ports and controls. Necessary software components come pre-installed on a Linux operating system. Network setting configuration is required, as described in this document.

The full range of cryptographic services required by Public Key Infrastructure (PKI) users is supported by the SafeNet ProtectServer Network HSM Plus's dedicated hardware cryptographic accelerator. These services include encryption, decryption, signature generation and verification, and key management with a tamper resistant and battery-backed key storage.

The SafeNet ProtectServer Network HSM Plus must be used with one of SafeNet's high-level cryptographic APIs. The following table shows the provider types and their corresponding SafeNet APIs:

Table Section Outside Table: API	Table Section Outside Table: SafeNet Product Required
PKCS #11	SafeNet ProtectToolkit-C
JCA / JCE	SafeNet ProtectToolkit-J
Microsoft IIS and CA	SafeNet ProtectToolkit-M

These APIs interface directly with the product's FIPS 140-2 Level 3 certified core using high-speed DES and RSA hardware-based cryptographic processing. Key storage is tamper-resistant and battery-backed.

A smart card reader, supplied with the HSM, allows for the secure loading and backup of keys.

Physical Features

The standard appliance is the 1U-high, rack-mount device:

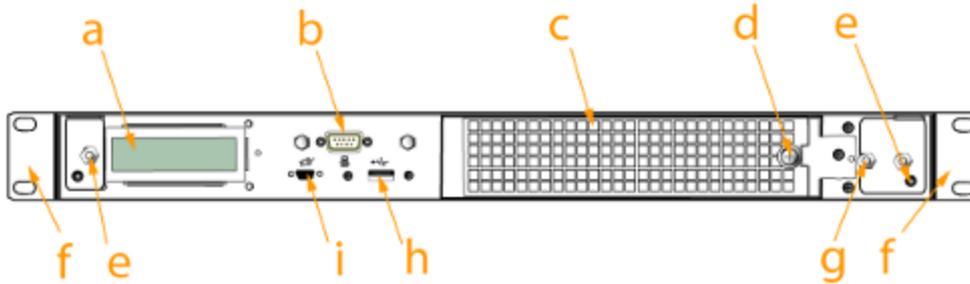


Here are some of the physical features of the SafeNet ProtectServer Network HSM Plus:

Front panel view

The features on the front panel of the SafeNet ProtectServer Network HSM Plus are illustrated below:

Figure 1: SafeNet ProtectServer Network HSM Plus front panel

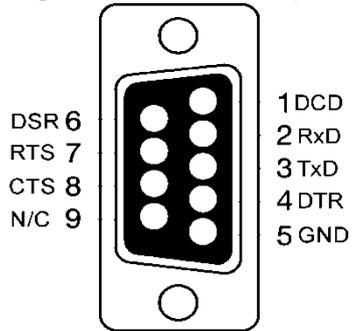


Item	Name	Description
a	LCD system status screen	Displays "ProtectServer +" when system is operational.
b	Serial (console) port	Local connection for initial setup, and for admin account reset (local-only action for security purposes).
c	Ventilation fan-filter cover	Removable bracket allows cleaning of air filter.
d	Fan filter cover retaining screw	A captive thumb-screw (no tool needed).
e	Mounts for removable front bezel	The protective front bezel mounts on the appliance front panel. Spring clips behind the bezel engage the mounting posts at the left and right ends of the appliances front panel.
f	Rack-mount tabs (removable)	Use the tabs on the front and the sliding tabs towards the rear of the appliance to support your SafeNet appliance in a compatible equipment rack.
g	Securing screw for fan bay	Torx screw secures the fan bay. CAUTION! Opening the fan bay will trigger a tamper event on the device.
h/i	USB ports	Unconfigured USB ports. These ports are not necessary for any ProtectServer operations and are left unconfigured for security purposes.

HSM serial port pin configuration

The serial port on the USB-to-serial cable, illustrated below, uses a standard RS232 male DB9 pinout:

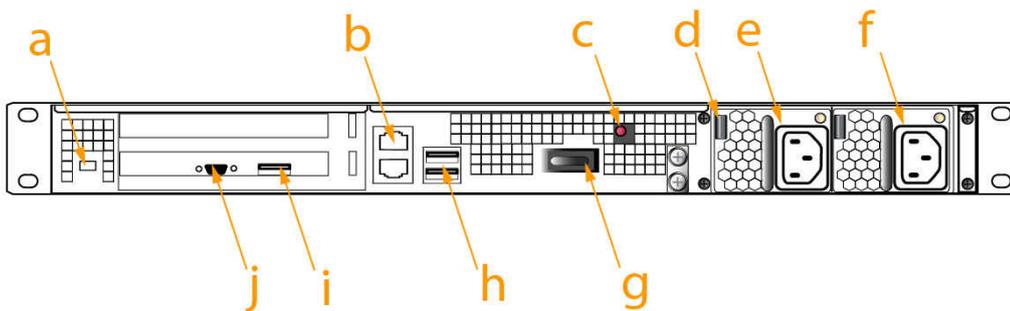
Figure 2: HSM serial port pinout



Rear panel view

The features on the rear panel of the SafeNet ProtectServer Network HSM Plus are illustrated below:

Figure 3: SafeNet ProtectServer Network HSM Plus rear panel



Item	Name	Description
a	Kensington security slot	Attach an industry-standard locking cable for additional physical security.
b	Ethernet ports	For network connection of your SafeNet appliance.
c	Tamper switch	Recessed for safety, the tamper switch is used during commissioning or decommissioning of the appliance to destroy any keys currently stored on the HSM. <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p>CAUTION! Activating the tamper switch deletes any keys currently stored on the HSM. Deleted keys are not recoverable. Ensure that you always back up your keys. To avoid accidentally deleting the keys on an operational SafeNet ProtectServer Network HSM Plus, ensure the users with access to the appliance are familiar with the switch.</p> </div>
d	Power supply release tab	Press tab to release the catch, and remove the power supply from the appliance.
e	Removable power supply	One of two redundant power supplies.

Item	Name	Description
f	Second removable power supply	The other of two redundant power supplies.
g	Start/stop switch	Use to stop the system if the command-line shutdown is not available; use to restart the system if it has been switched off.
h	USB ports	Unconfigured USB ports. These ports are not necessary for any ProtectServer operations and are left unconfigured for security purposes.
i	HSM USB port	Connects USB devices such as the USB smart card reader and the legacy card reader to the HSM.
j	Unused port	This port is not used for the SafeNet ProtectServer Network HSM Plus; we recommend that you do not remove the covers that are installed at the factory.

Cryptographic architecture

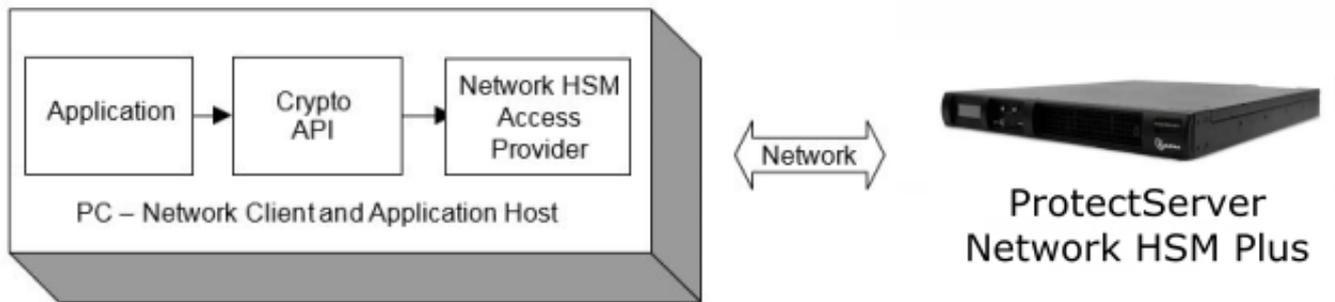
A hardware-based cryptographic system consists of three general components:

- > One or more hardware security modules (HSMs) for key processing and storage.
- > High-level cryptographic API software. This software uses the HSM's cryptographic capabilities to provide security services to applications.
- > Access provider software to allow communication between the API software and the HSMs.

Operating in network mode, a standalone SafeNet ProtectServer Network HSM Plus can provide key processing and storage.

In network mode, access provider software is installed on the machine hosting the cryptographic API software. The access provider allows communication between the API and the SafeNet ProtectServer Network HSM Plus over a TCP/IP connection. The HSM can therefore be located remotely, improving the security of cryptographic key data

The figure below depicts a cryptographic service provider using the SafeNet ProtectServer Network HSM Plus in network mode.

Figure 4: SafeNet ProtectServer Network HSM implementation

Summary of Cryptographic Service Provider setup

These steps summarize the overall procedure of setting up a cryptographic service provider using a SafeNet ProtectServer Network HSM Plus in network mode. Relevant links to more detailed documentation are provided at each step.

1. **Install the SafeNet ProtectServer Network HSM** (See "[SafeNet ProtectServer Network HSM Plus Hardware Installation](#)" on page 15).
2. **Check that the SafeNet ProtectServer Network HSM is operating correctly** (see "[First Log in and System Test](#)" on page 25).
3. **Configure the SafeNet ProtectServer Network HSM network settings** (see "[Network Configuration](#)" on page 27).
4. **Install and configure the Network HSM Access Provider software** (see the *SafeNet ProtectServer HSM Access Provider Installation Guide*).
5. **Install the high-level cryptographic API software.**

Please refer to the relevant installation guide supplied with the product:

- *SafeNet ProtectToolkit-C Administration Guide*
- *SafeNet ProtectToolkit-J Installation Guide*
- *SafeNet ProtectToolkit-M User Guide*

6. **Configure the high-level cryptographic API to allow preferred operating modes.** Some of these tasks may include:

- establishing a trusted channel or secure messaging system (SMS) between the API and the Safenet ProtectServer Network HSM Plus.
- establishing communication between the network client and the Safenet ProtectServer Network HSM Plus.

Please refer to the relevant high-level cryptographic API documentation:

- *SafeNet ProtectToolkit-C Administration Guide*
- *SafeNet ProtectToolkit-J Administration Guide*
- *SafeNet ProtectToolkit-M User Guide*

CHAPTER 2:

SafeNet ProtectServer Network HSM Plus Hardware Installation

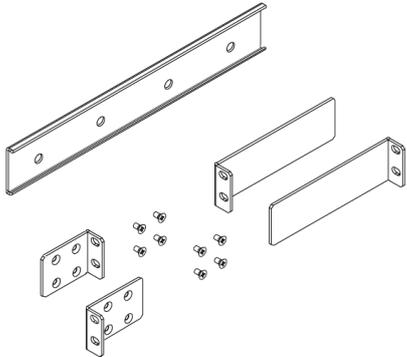
This chapter describes how to install and connect a SafeNet Protect Server Network HSM Plus. To ensure a successful installation, perform the following tasks in the order indicated:

1. Ensure that you have all of the required components, as listed in ["SafeNet ProtectServer Network HSM Plus Required Items" on the next page](#)
2. Install and connect the hardware, as described in ["Installing the SafeNet ProtectServer Network HSM Plus Hardware" on page 18](#)

SafeNet ProtectServer Network HSM Plus Required Items

Follow this checklist to verify that you have all of the items required for the installation.

Qty	Item
1	 <p>SafeNet ProtectServer Network HSM Plus Appliance</p>
2	 <p>Power Supply Cord (one for each power supply; style to suit country for which you ordered) (*)</p>
1	 <p>Null-Modem Serial Cable</p>

Qty	Item
1	 <p data-bbox="225 667 611 699">USB 2.0 to RS232 Serial Adapter</p>
1	 <p data-bbox="225 1140 1177 1272">Set of: - 2 front Mounting Brackets with Screws, - 2 Side Bracket Guides, and - 2 Sliding Rear Brackets (fit into the guides for rear support adjustable positioning).</p>
1	Client / SDK Software (**)

(* Power cables are no longer included with the shipment from our factory. Many customers are buying HSMs from one country, but shipping them for final deployment to different countries, which has resulted in many wasted power cables that are incorrect format for destination countries. Please source your power cables locally for the deployment destination.)

(** Software is available by download from Gemalto. Physical media for software and documentation are special-request items.)

Installing the SafeNet ProtectServer Network HSM Plus Hardware

This section provides basic SafeNet Network HSM hardware installation instructions (mounting in a rack, connecting cables, etc.). The SafeNet Network HSM appliance comes with front brackets and side-rails and sliders for the rear brackets, packed separately in the carton.

Installation Notes

1. Any computer that is to act as a client to the SafeNet ProtectServer Network HSM Plus appliance must have the Client software installed. Windows users should log in to your computer as a user with Administrator privileges.
2. A computer that is to be used only for administering the SafeNet ProtectServer Network HSM Plus does not need the Client software – only an SSH client such as the PuTTY program that we have provided for Windows, or the SSH utilities that come standard with most Linux and UNIX platforms.
3. All two tasks (Client, and administration) can be performed on a single computer, but in normal practice they are often separate tasks for separate computers.

Installing the SafeNet ProtectServer Network HSM Plus Hardware

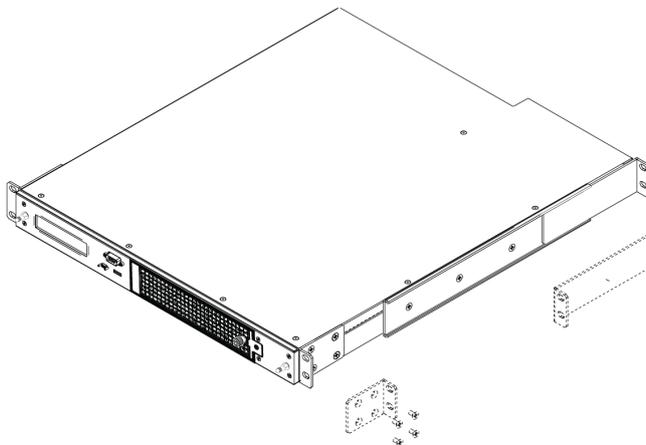
You can optionally install the brackets if they suit your equipment rack. The front brackets can be installed with their tabs forward (for flush-mount of the appliance) or reversed, to allow the front of the appliance to stand out from the rack. The rear brackets install in either direction – as appropriate for your rack post spacing – with the brackets simply sliding into the rails on each side of the appliance.

The supplied brackets are designed and intended for 4-point support of the appliance, in racks with rear-post depth up to 22 inches.

CAUTION! Do not attempt to mount the appliance using only the front brackets – damage can occur.

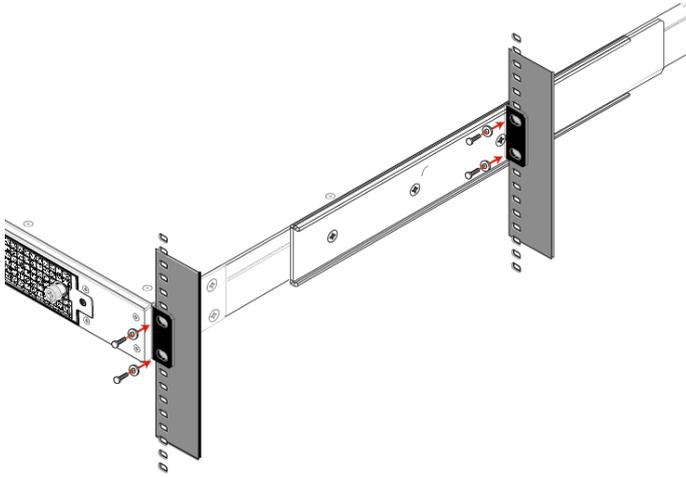
To install the SafeNet Network HSM hardware

1. Install and adjust rails and brackets to suit your equipment rack



- Mount the appliance in your equipment rack. Alternatively, ignore the rails and mounting tabs, and rest the SafeNet ProtectServer Network HSM Plus appliance on a mounting tray or shelf suitable for your specific style and brand of equipment rack.

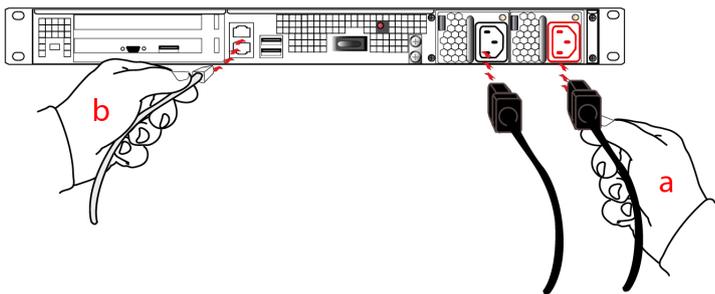
CAUTION! Support the weight of the appliance until all four brackets are secured.



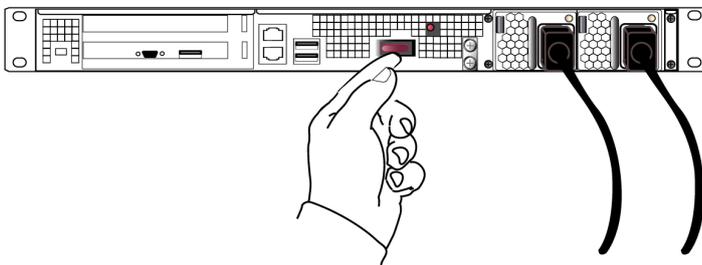
- Insert the power (a) and network (b) cables at the rear panel.

The SafeNet ProtectServer Network HSM Plus is equipped with two NICs (*eth0* and *eth1*) incorporating an IPv4/IPv6 dual stack, allowing you to configure both an IPv4 and IPv6 address on each interface. If you intend to use both NICs, connect Ethernet cables to both LAN connectors.

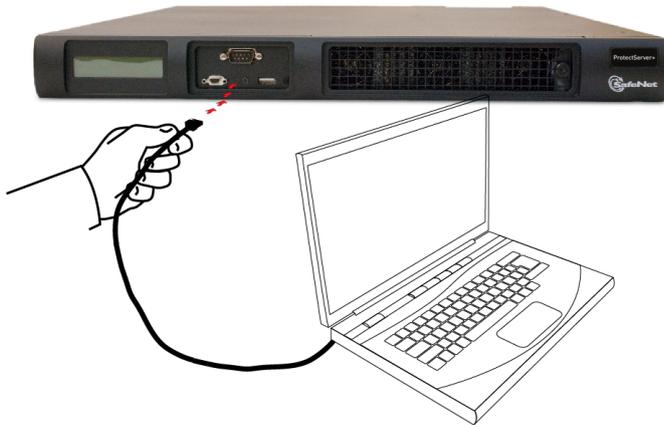
For proper redundancy and best reliability, the power cables should connect to two independent power sources.



- Press and release the Start/Stop switch, on the rear panel.



- Connect a terminal to the serial connector on the front panel.



6. If you have already installed SafeNet ProtectToolkit client software, refer to the *SafeNet ProtectToolkit-C Administration Guide*.

Smart Card Reader Installation

The unit supports the use of smart cards with a SafeNet-supplied smart card reader. Other smart card readers are not supported.

The SafeNet ProtectServer Network HSM Plus supports two different card readers:

- > 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 interface 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 on the back of the device, as illustrated below.



Installing the legacy card reader

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

The legacy card reader must also be connected to a PS/2 port for its power. Many newer servers have USB ports, but do not provide a PS/2 connection.

If there is no available PS/2 connection, there are two options:

- > Connect a PS/2-to-USB adapter between the card reader and a USB port on the SafeNet ProtectServer Network HSM Plus.
- > If, for security reasons, you prefer to not expose USB ports on your crypto server, connect a PS/2-to-USB adapter cable between the card reader and a standalone powered USB hub.

NOTE The USB connection is for power only. No data transfer occurs over this connection.



Next, see ["Testing and Configuration" on page 25.](#)

CHAPTER 3:

Deployment Guidelines

Users must consider the following best practices for security and compliance when deploying SafeNet ProtectServer Network HSMs for their network/application environment:

- > ["Secure Messaging System \(SMS\)" below](#)
- > ["Networking and Firewall Configuration" on the next page](#)
- > ["Separation of Roles" on the next page](#)

Secure Messaging System (SMS)

SafeNet ProtectServer HSMs store cryptographic keys and objects in tamper-resistant secure memory, which is erased when a tamper is detected. The stored keys are accessed through PKCS#11 calls from the client. Client calls to a Network HSM traverse the network layer (TCP/IP). In the default security mode, this communication channel between the HSM and the client is unencrypted. Configure the HSM security policy to improve this channel's security. Refer to ["Security Flags" on page 1](#) in the *PTK-C Administration Guide* for descriptions of the available flags and how they affect your implementation.

The Secure Messaging System (SMS) greatly enhances the security of the client-HSM channel. SMS provides an encrypted channel between the client and the HSM and authenticates messages on that channel using a Message Authentication Code (MAC) approved by the FIPS 140-2 standard. Refer to ["Secure Messaging" on page 1](#) in the *PTK-C Administration Guide* for a detailed description of SMS functionality.

NOTE SMS encrypts and authenticates messages between the client and HSM, but does not provide means for the HSM to authenticate client credentials or vice-versa.

The HSM supports the following SMS modes:

- > HIMK
- > ADH
- > ADH2 (PTK 5.4 and above)

For secure deployment, use ADH or ADH2. Refer to ["Secure Messaging" on page 1](#) in the *PTK-C Administration Guide* for descriptions of the difference between these modes.

The SMS feature is flexible and can be configured to:

- > Encrypt/decrypt all messages
- > Sign/verify all messages
- > Allow only FIPS-approved mechanisms
- > Rotate signing and encryption keys after a specified number of packets or hours
- > All of the above

For maximum security, enable all of the above features. See ["Security Flags" on page 1](#) in the *PTK-C Administration Guide* for flag descriptions and setup instructions.

NOTE Enabling FIPS mode will block all mechanisms that are not FIPS-approved. If you are using unapproved mechanisms and understand the implications, do not enable FIPS mode.

Networking and Firewall Configuration

There is no means to authenticate the client to the HSM or vice-versa. It is therefore recommended that the HSM and client are connected to the same secure network segment, to prevent sensitive data from traveling through insecure intermediate network(s). This configuration prevents Man-in-the-Middle and other malicious attacks. If possible, connect the HSM directly to the client using a cross-cable.

The SafeNet ProtectServer Network HSM includes two network ports, each of which can be connected to a different network. It is highly recommended that you keep the management network and the network running your applications isolated from each other at all times. Further restrictions on communication between network segments can be enforced by means of static routes. See ["Network Configuration" on page 27](#) for instructions on setting up static routes.

The SafeNet ProtectServer Network HSM supports an iptables-based firewall. The firewall must be configured with appropriate rules to restrict access to identified network resources only. See ["Network Configuration" on page 27](#) for details on setting iptables.

Separation of Roles

The SafeNet ProtectServer Network HSM has two role categories: Appliance and HSM users. For optimal security, maintain these roles and their credentials separately; do not share between users. Do not share the appliance management, HSM Administration, and User terminals.

Appliance Users

The following roles can log in to the PSE shell (PSESH) to configure and manage the appliance:

- > admin
- > pseoperator
- > audit

See ["Using PSESH" on page 1](#) in the *PSESH Command Reference Guide* for the responsibilities of each role.

HSM Users

The following roles can log in to manage the HSM token and perform cryptographic operations:

- > Administration Security Officer (ASO)
- > Administrator
- > Security Officer (SO)
- > Token Owner (User)

See ["User Roles" on page 1](#) in the *PTK-C Administration Guide* for the responsibilities of each role.

CHAPTER 4:

Testing and Configuration

This chapter provides a step-by-step overview of how to confirm correct operation of the Safenet ProtectServer Network HSM Plus, and configure its network settings. These instructions assume that the installation process covered in "[SafeNet ProtectServer Network HSM Plus Hardware Installation](#)" on page 15 is complete.

This chapter contains the following sections:

- > "[First Log in and System Test](#)" below
- > "[Network Configuration](#)" on page 27
- > "[Powering off the SafeNet ProtectServer Network HSM Plus](#)" on page 30
- > "[Troubleshooting](#)" on page 31

First Log in and System Test

When starting up your SafeNet ProtectServer Network HSM Plus for the first time, follow these steps:

- > "[Access the Console](#)" below
- > "[Power on and Log in](#)" on the next page
- > "[Run System Test](#)" on the next page

Access the Console

To test the system and configure the network, you must first access the SafeNet ProtectServer Network HSM Plus console. You must connect a terminal directly to the serial port on the front end of the appliance with a null modem serial cable. Use the console port to configure at least one of the network interfaces.



To access the console:

1. Connect a null-modem serial cable (supplied) between the serial port on the HSM appliance front panel and a dumb terminal or a PC or laptop that will serve as the administration workstation.

2. Use a terminal emulation package provided with your operating system. Set the Serial connection parameters:
 - Serial port baud rate: 115200
 - N,8,1 (no parity, 8 data-bits, one stop-bit)
 - VT-100 terminal emulation
 - hardware flow control selected

Power on and Log in

Power on the SafeNet ProtectServer Network HSM Plus and the monitor (if applicable). The startup message will be displayed on the monitor.

Power-up is complete when the SafeNet ProtectServer Network HSM Plus log in prompt appears:

```
Protect Server External 5.5.0
PSE+ login:
```

You can login as **admin** or **pseoperator** to access the PSE shell (PSESH), which provides a CLI for configuring and managing the appliance. See the *PSESH Command Reference Guide* for command syntax. There is a third account, **audit**, which is used to configure audit logging on the appliance. This account cannot be used to perform administrative tasks.

The default passwords for the **admin** and **pseoperator** users are:

User name	Default password
admin	password
pseoperator	password

After logging in, you will be prompted to change the password for the account. Please remember your password. To change the account password at any time, login to the account and use the command **user password**.

The **admin** user can reset all account passwords to their factory defaults at any time with the PSESH command **sysconf appliance factory**. This command will also reset the SNMP and network settings to their factory defaults.

CAUTION! Executing **sysconf appliance factory** over an SSH connection may cause you to lose connection with the appliance when the IP address is reset. To avoid this, use a serial connection instead when using this command.

Run System Test

Before field testing and deployment, run the diagnostic utility. While logged in as the **admin** or **pseoperator** enter the command **hsm state** to display the current status:

```
psesh:>hsm state
```

```
HSM device 0:   HSM in NORMAL MODE. RESPONDING to requests. Usage Level=0%
State = (0x8000, 0xffffffff)
Host Interface  = PSIE2
```

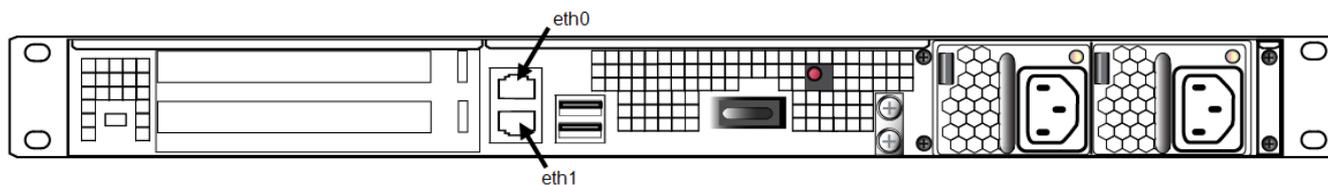
Command Result : 0 (Success)

You can also use the PSESH command **status** to check each of the HSM's processes. See the *PSESH Command Reference Guide* for command syntax.

Network Configuration

The SafeNet ProtectServer Network HSM Plus is intended to be installed in a data center and accessed remotely over a network. Network access is provided by two Ethernet LAN ports.

The network device interfaces (eth0 and eth1) are located on the back of the appliance, as illustrated below:



Appliance configuration

The following network parameters are configured at the appliance level:

- > Appliance hostname. A hostname is optional, unless you are using DNS.

Ethernet LAN device configuration

The SafeNet ProtectServer Network HSM Plus is equipped with two individually-configurable Ethernet LAN network devices. You can configure the following network settings for each device:

- > IPv4 or IPv6 address. You can configure the addresses using static or DHCP addressing.
- > Network gateway. Devices must use a gateway appropriate for the network (IPv4 or IPv6).
- > Network mask. IPv4 devices must use dotted-quad format (for example, 255.255.255.0). IPv6 devices can use full or shorthand syntax.
- > Static network route.
- > DNS configuration. Although you configure DNS at the device level, the settings you configure for a device are available to all devices on the appliance if the configured device is connected to the network. To ensure DNS access, it is recommended that you configure each device. You can configure the following settings:
 - DNS nameservers
 - DNS search domains

These settings apply to static network configurations only. If you are using DHCP, the DNS search domains and DNS nameservers configured on the DHCP server are used.

Gathering Appliance Network Information

Before you begin, obtain the following information (see your network administrator for most of these items):

HSM Appliance Network Parameters

- > IP address and subnet mask for each LAN port you want to use (if you are using static IP addressing)
- > Hostname for the HSM appliance (registered with network DNS)
- > Domain name (per port)
- > Default gateway IP address (per port)
- > DNS Name Server IP address(es) (per port)
- > Search Domain name(s) (per port)
- > Device subnet mask (per port)

DNS Entries

- > Ensure that you have configured your DNS Server(s) with the correct entries for the appliance and the client.
- > If you are using DHCP, then all references to the Client and the HSM appliance (as in Certificates) should use hostnames.

Configuring the Network Parameters

You can use the serial connection to configure all of your network parameters, or configure a single port and use it to access the appliance over the network and complete the configuration.

NOTE Use a locally-connected serial terminal when changing the appliance IP address, to avoid SSH admin console disconnection.

To configure the appliance and port network parameters:

It is recommended that you configure and test each device. You need to know the IP address of at least one network interface to establish an SSH connection to the appliance.

1. Login to the appliance as **admin** or **pseoperator**.
2. Configure the IP address, network mask, and gateway (optional) on at least one of the Ethernet LAN ports (eth0 or eth1). You can specify a static address, or retrieve one from a DHCP server. You can configure each port to use an IPv4 or IPv6 address.

Static	psesh:> network interface static -device <netdevice> -ip <IP_address> -netmask <netmask> [-gateway <IP_address>]
DHCP	psesh:> network interface dhcp -device <netdevice>

Either of these commands will prompt you to restart the network service.

3. [Optional] Set the appliance hostname and domain name.

```
psesh:> network hostname <hostname>
```

```
psesh:> network domain <netdomain>
```

You must configure your DNS server to resolve the hostname to the IP address configured on the Ethernet port of the appliance. Do this for each Ethernet port connected to a network. See your network administrator for assistance.

4. [Optional] Add a domain name server to the network configuration for the appliance. The name server is added to the appliance DNS table. There is one DNS table that applies to all network devices (ports) on the appliance.

```
psesh:> network dns add nameserver <IP_address> -device <net_device>
```

NOTE The domain name settings apply to static network configurations only. If you are using DHCP, the DNS name servers configured on the DHCP server are used.

When you add a DNS server to a specific network device, it is added to the DNS table for the appliance and becomes available to both devices, provided the device you added it to is connected to the network. For example, if you add a DNS server to eth0, eth1 will be able to access the DNS server if eth0 is connected to the network. If eth0 is disconnected from the network, eth1 also loses DNS server access. To ensure that any DNS server you add is available in the event of a network or port failure, it is recommended that you add it to both network-connected devices.

5. [Optional] Add a search domain to the network configuration. These are automatically appended to an internet address you specify in PSESH. For example, if you add the search domain **mycompany.com**, entering the command **network ping hsm1** would search for the domain **hsm1.mycompany.com**. If the domain resolves, it pings the device with that hostname.

```
lunash:> network dns add searchdomain <domain> -device <net_device>
```

The search domain is added to the appliance DNS table.

NOTE The search domain settings apply to static network configurations only. If you are using DHCP, the DNS search domains configured on the DHCP server are used.

When you add a DNS search domain to a specific network device, it is added to the DNS table for the appliance and becomes available to both devices, provided the device you added it to is connected to the network. For example, if you add a DNS server to eth0, eth1 will be able to access the DNS server if eth0 is connected to the network. If eth0 is disconnected from the network, eth1 also loses DNS server access. To ensure that any DNS server you add is available in the event of a network or port failure, it is recommended that you add it to both network-connected devices.

If you have chosen to perform setup via SSH, you will likely lose your network connection as you confirm the change of IP address from the default setting.

6. [Optional] Add iptables ACCEPT and DROP rules to manage network access to the appliance.

By default, the SafeNet ProtectServer Network HSM allows access to all networks and hosts. The default policy for the INPUT and OUTPUT chain is set to ACCEPT. The default policy for the FORWARD chain is set to DROP, since the SafeNet ProtectServer Network HSM is not used to forward packets, as in a router or proxy.

CAUTION! If you are configuring iptables via SSH, a malformed rule can cause a lockout.

- a. To add an ACCEPT rule, specify a host or network:

```
psesh:> network iptables addrule accept host -ip <IP_address>
```

```
psesh:> network iptables addrule accept network -net <IP_address> -mask <netmask>
```

- b. To add a DROP rule, specify a host or network:

```
psesh:> network iptables addrule drop host -ip <IP_address>
```

```
psesh:> network iptables addrule drop network -net <IP_address> -mask <netmask>
```

- c. To see the current list of rules:

```
psesh:> network iptables show
```

- d. To delete a rule, specify the rule's position on the list:

```
psesh:> network iptables delrule -rulenum <number>
```

A rule's number is based on its current list position, so executing **network iptables delrule -rulenum 1** multiple times will eventually delete the entire list.

- e. Save your iptables changes:

```
psesh:> network iptables save
```

You must execute this command, or any changes will be lost on the next appliance reboot.

7. After making any change to the network configuration, reboot the appliance:

```
psesh:> sysconf appliance reboot
```

8. View the new network settings:

```
psesh:> network show
```

SSH Network Access

After you have completed the network configuration, you can access the SafeNet ProtectServer Network HSM Plus over the network using the SSH protocol. You need an SSH client such as puTTY (available for free from www.putty.org).

Powering off the SafeNet ProtectServer Network HSM Plus

Use PSESH to power off the appliance.

To power off the SafeNet ProtectServer Network HSM Plus:

While logged in to PSESH as **admin** or **pseoperator**, issue the command:

```
psesh:> sysconf appliance poweroff
```

Wait for the appliance to perform shutdown procedures. The fan and LEDs will remain operational until shutdown is complete.

Troubleshooting

Each SafeNet ProtectServer Network HSM Plus is tested during manufacture to ensure a high level of quality. In the unlikely event the unit is not functioning correctly please re-check the installation procedure, paying particular attention to the power source and network cable connection. Running the diagnostic command **hsm state**, as described in ["First Login and System Test" on page 1](#), is the only method available to test the unit.

NOTE The unit has no user-serviceable parts. Please do not disassemble the unit to resolve problems unless directed by a Gemalto Technical Support engineer.

For further assistance contact your supplier or Gemalto Technical Support with the following details at hand:

- > The product serial number (at the back of the unit)
- > A detailed description of the current system configuration
- > Details of any error messages pertaining to the problem

For contact numbers in your home country, see ["Support Contacts" on page 9](#).

APPENDIX A:

Technical Specifications

The SafeNet ProtectServer Network HSM Plus specifications are as follows:

Hardware

- > Protective, heavy duty steel, industrial PC case
- > Intel® Pentium® CPU G6950 2.80GHz
- > 2 Gb RAM
- > 250 Gb hard disk drive
- > 10/100/1000 Mbps autosensing Network Interface with RJ45 LAN connector
- > Dual power supplies

Pre-installed Software

- > Linux operating system
- > SafeNet PCI HSM Access Provider software
- > SafeNet HSM Net Server software

Power Supply

- > Nominal power consumption: 156 W
- > Input AC voltage range: 100-240 V
- > Input frequency range: 50-60 Hz

Physical properties

- > 482 mm (W) x 533 mm (D) x 44 mm (H) (1U)
- > 19" rack mounting brackets included
- > Weight 12.7 kg (28 lb)

Operating Environment

- > Temperature: 0 to 40 °C (32 to 104 °F)
- > Relative Humidity: 5 to 85%

APPENDIX B:

Glossary

A

Adapter

The printed circuit board responsible for cryptographic processing in a HSM

AES

Advanced Encryption Standard

API

Application Programming Interface

ASO

Administration Security Officer

Asymmetric Cipher

An encryption algorithm that uses different keys for encryption and decryption. These ciphers are usually also known as public-key ciphers as one of the keys is generally public and the other is private. RSA and ElGamal are two asymmetric algorithms

B

Block Cipher

A cipher that processes input in a fixed block size greater than 8 bits. A common block size is 64 bits

Bus

One of the sets of conductors (wires, PCB tracks or connections) in an IC

C

CA

Certification Authority

CAST

Encryption algorithm developed by Carlisle Adams and Stafford Tavares

Certificate

A binding of an identity (individual, group, etc.) to a public key which is generally signed by another identity. A certificate chain is a list of certificates that indicates a chain of trust, i.e. the second certificate has signed the first, the third has signed the second and so on

CMOS

Complementary Metal-Oxide Semiconductor. A common data storage component

Cprov

ProtectToolkit C - SafeNet's PKCS #11 Cryptoki Provider

Cryptoki

Cryptographic Token Interface Standard. (aka PKCS#11)

CSA

Cryptographic Services Adapter

CSPs

Microsoft Cryptographic Service Providers

D

Decryption

The process of recovering the plaintext from the ciphertext

DES

Cryptographic algorithm named as the Data Encryption Standard

Digital Signature

A mechanism that allows a recipient or third party to verify the originator of a document and to ensure that the document has not be altered in transit

DLL

Dynamically Linked Library. A library which is linked to application programs when they are loaded or run rather than as the final phase of compilation

DSA

Digital Signature Algorithm

E

Encryption

The process of converting the plaintext data into the ciphertext so that the content of the data is no longer obvious. Some algorithms perform this function in such a way that there is no known mechanism, other than decryption with the appropriate key, to recover the plaintext. With other algorithms there are known flaws which reduce the difficulty in recovering the plaintext

F

FIPS

Federal Information Protection Standards

FM

Functionality Module. A segment of custom program code operating inside the CSA800 HSM to provide additional or changed functionality of the hardware

FMSW

Functionality Module Dispatch Switcher

H

HA

High Availability

HIFACE

Host Interface. It is used to communicate with the host system

HSM

Hardware Security Module

I

IDEA

International Data Encryption Algorithm

IIS

Microsoft Internet Information Services

IP

Internet Protocol

J

JCA

Java Cryptography Architecture

JCE

Java Cryptography Extension

K

Keyset

A keyset is the definition given to an allocated memory space on the HSM. It contains the key information for a specific user

KWRAP

Key Wrapping Key

M

MAC

Message authentication code. A mechanism that allows a recipient of a message to determine if a message has been tampered with. Broadly there are two types of MAC algorithms, one is based on symmetric encryption algorithms and the second is based on Message Digest algorithms. This second class of MAC algorithms are known as HMAC algorithms. A DES based MAC is defined in FIPS PUB 113, see <http://www.itl.nist.gov/div897/pubs/fip113.htm>. For information on HMAC algorithms see RFC-2104 at <http://www.ietf.org/rfc/rfc2104.txt>

Message Digest

A condensed representation of a data stream. A message digest will convert an arbitrary data stream into a fixed size output. This output will always be the same for the same input stream however the input cannot be reconstructed from the digest

MSCAPI

Microsoft Cryptographic API

MSDN

Microsoft Developer Network

P

Padding

A mechanism for extending the input data so that it is of the required size for a block cipher. The PKCS documents contain details on the most common padding mechanisms of PKCS#1 and PKCS#5

PCI

Peripheral Component Interconnect

PEM

Privacy Enhanced Mail

PIN

Personal Identification Number

PKCS

Public Key Cryptographic Standard. A set of standards developed by RSA Laboratories for Public Key Cryptographic processing

PKCS #11

Cryptographic Token Interface Standard developed by RSA Laboratories

PKI

Public Key Infrastructure

ProtectServer

SafeNet HSM

ProtectToolkit C

SafeNet's implementation of PKCS#11. Protecttoolkit C represents a suite of products including various PKCS#11 runtimes including software only, hardware adapter, and host security module based variants. A Remote client and server are also available

ProtectToolkit J

SafeNet's implementation of JCE. Runs on top of ProtectToolkit C

R

RC2/RC4

Ciphers designed by RSA Data Security, Inc.

RFC

Request for Comments, proposed specifications for various protocols and algorithms archived by the Internet Engineering Task Force (IETF), see <http://www.ietf.org>

RNG

Random Number Generator

RSA

Cryptographic algorithm by Ron Rivest, Adi Shamir and Leonard Adelman

RTC

Real Time Clock

S

SDK

Software Development Kits Other documentation may refer to the SafeNet Cprov and Protect Toolkit J SDKs. These SDKs have been renamed ProtectToolkit C and ProtectToolkit J respectively. ⌚ The names Cprov and ProtectToolkit C refer to the same device in the context of this or previous manuals. ⌚ The names Protect Toolkit J and ProtectToolkit J refer to the same device in the context of this or previous manuals.

Slot

PKCS#11 slot which is capable of holding a token

SlotPKCS#11

Slot which is capable of holding a token

SO

Security Officer

Symmetric Cipher

An encryption algorithm that uses the same key for encryption and decryption. DES, RC4 and IDEA are all symmetric algorithms

T

TC

Trusted Channel

TCP/IP

Transmission Control Protocol / Internet Protocol

Token

PKCS#11 token that provides cryptographic services and access controlled secure key storage

TokenPKCS#11

Token that provides cryptographic services and access controlled secure key storage

U

URI

Universal Resource Identifier

V

VA

Validation Authority

X

X.509

Digital Certificate Standard

X.509 Certificate

Section 3.3.3 of X.509v3 defines a certificate as: "user certificate; public key certificate; certificate: The public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it"