THALES

SafeNet ProtectServer PCIe HSM 5.9

INSTALLATION GUIDE

Document Information

Product Version	5.9
Document Part Number	007-013682-007
Release Date	08 January 2020

Revision History

Revision	Date	Reason
Rev. A	08 January 2020	Initial release

Thales 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 Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales 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.

CONTENTS

PREFACE: About the ProtectServer PCIe HSM Installation Guide

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

SafeNet ProtectServer may employ either generic processing or high-speed DES and RSA hardware acceleration. Key storage security is ensured by persistent, tamper-protected memory. Multiple adapters may be installed in a single host computer to improve throughput or provide redundancy.

This guide provides instructions for installing a SafeNet ProtectServer cryptographic services hardware adapter.

The companion manual, *ProtectServer HSM Access Provider Installation Guide*, provides instructions for installing the associated *ProtectServer HSM Access Provider* package (**PTKpcihsm2**), including the device driver.

This manual contains the following sections:

> "ProtectServer PCIe HSM Hardware Installation" on page 9

> "Troubleshooting" on page 16

> "Hardware Reference" on page 18

   This appendix provides the adapter's serial port specifications, and instructions for modifying the circuit board to use external tamper detectors.

This preface also includes the following information about this document:

> "Gemalto Rebranding" below

> "Audience" on the next page

> "Document Conventions" on the next page

> "Support Contacts" on page 8

For information regarding the document status and revision history, see "Document Information" on page 2.

Gemalto Rebranding

In early 2015, Gemalto completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the SafeNet name has been retained. As a result, the product names for SafeNet HSMs have changed as follows:

Old product name	New product name
ProtectServer External 2 (PSE2)	SafeNet ProtectServer Network HSM

Old product name	New product name
ProtectServer Internal Express 2 (PSI-E2)	SafeNet ProtectServer PCIe HSM
ProtectServer HSM Access Provider	SafeNet ProtectServer HSM Access Provider
ProtectToolkit C (PTK-C)	SafeNet ProtectToolkit-C
ProtectToolkit J (PTK-J)	SafeNet ProtectToolkit-J
ProtectToolkit M (PTK-M)	SafeNet ProtectToolkit-M
ProtectToolkit FM SDK	SafeNet ProtectToolkit FM SDK

> **NOTE** These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

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 Thales 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	The bold attribute is used to indicate the following: > 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**.)
italics	In type, the italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* 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>|<b>|<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>|<b>|<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 Thales Customer Support.

Thales 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 Thales 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.thalesgroup.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

The support portal also lists telephone numbers for voice contact (Contact Us).

CHAPTER 1:   ProtectServer PCIe HSM Hardware Installation

This chapter describes how to install and connect a ProtectServer PCIe HSM. 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 "ProtectServer PCIe HSM Required Items" on the next page.

2. Install and connect the hardware, as described in "ProtectServer PCIe HSM Installation" on page 11.

ProtectServer PCIe HSM Required Items

This section provides a list of the components you should have received with your ProtectServer PCIe HSM order.

Contents Received

The following table contains the standard items you received with your order.

Qty	Item
1	**ProtectServer PCIe HSM Adapter Card**, short-form-factor (performance level 25, 220, or 1500, as ordered, indicated on label).
1	**Smart card reader**
2	**Smart cards** (in a single media case)

Optional Items

The following table describes additional items which you can use with your ProtectServer HSM. Contact your Thales sales representative to order these items.

Qty	Item
1+	**SafeNet 110 Time-Based OTP Token** (enables multifactor authentication on ProtectServer HSM tokens) Thales recommends ordering at least two (2) OTP tokens for each slot on the HSM (one each for the Security Officer and Token User). PN: 955-000237-001
1	**ProtectServer-compatible Verifone PIN pad** (enables manual key component entry) PN: 934-000087-001

ProtectServer PCIe HSM Installation

Follow these general steps to install and commission a ProtectServer PCIe HSM card and its associated software. More detailed instructions are provided in the following sections.

To install and commission a ProtectServer PCIe HSM card

1. Ensure you have all the necessary components on the list provided. For more information, see "Adapter Features" on the next page.

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

3. If you plan to use an external tamper detector, ensure that it has a two-conductor cable compatible with the tamper-detect connector on the SafeNet adapter (detailed in "Adapter Modification for External Tamper Detectors" on page 18).

4. Install the ProtectServer PCIe HSM card in the host computer system. See "Installing the Adapter" on page 13.

5. Install the ProtectServer HSM Access Provider package and confirm that the adapter and driver are working correctly. See "ProtectServer HSM Access Provider Installation" on page 13.

6. Install the smart card reader if provided, or another serial device. See "Smart Card Reader Installation" on page 13.

7. Install the SafeNet application programming interface (API) or the supplied net server software. See "Completing Installation" on page 14.

Adapter Features

The ProtectServer PCIe HSM is a standard PCIe device that fits into any motherboard PCIe slot of formats x4, x8, or x16.

The Card Faceplate

The card faceplate has two ports:

Micro-D subminiature
(MSDM) connector
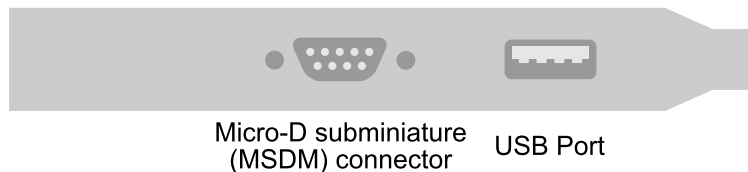
USB Port

The MDSM Connector

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

The USB Port

The USB port connects a serial device, such as a smart card reader, to the card with the included USB-to-serial adapter.

The Rear Face

The battery and a series of jumper headers are located on the rear face of the card.

Battery
Polarity
Decommission
Tamper input

On   Off
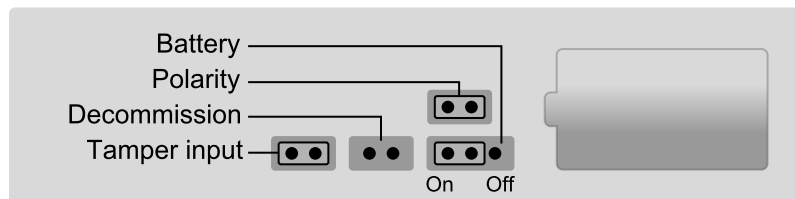
The Battery

The battery maintains the internal flash memory. The battery must remain connected for transport mode.

When keeping the HSM in storage (without keys present) it is recommended that you isolate or disconnect the battery to extend its lifespan. You can use the **ctcheck -b batterystatus** command to test the battery's condition. If the Battery Status indication reports as **LOW**, back up the HSM keys before powering down the PC.

> **CAUTION!** Disconnecting the battery deletes all key material on the HSM. Ensure that you back up your 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 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 in
"ProtectServer PCIe HSM Installation" on page 11.

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 Thales support.

The Decommission Jumper Header
This header is currently unused; do not change its default setting (open).

The Tamper-Input Header
The tamper-input header connects an external tamper device to the card. By default, it has a jumper in place
across both pins. To use an external tamper device, run a two-wire cable to your chassis-tamper switch or
similar device to open the circuit in the case of a tamper event.

The Polarity Jumper Header
The polarity jumper header is used to configure the card's operating mode. Do not change this jumper setting.

Installing the Adapter

The adapter is a PCI Express Specification 1.1-compliant device. It can be fitted in any spare PCIe slot on the
motherboard of formats x4, x8, or x16. If necessary, please consult the documentation accompanying your
host system motherboard to find the PCIe slots.

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

ProtectServer HSM Access Provider Installation

After successful installation of the adapter:

1. Install the ProtectServer HSM Access Provider package (**PTKpcihsm2**).
2. Confirm the adapter and driver package are operating correctly.

These steps are covered in detail by the *ProtectServer HSM Access ProviderInstallation Guide* for both
Windows and Unix/Linux systems.

Smart Card Reader Installation

The ProtectServer PCIe HSM supports the use of smart cards with a SafeNet-supplied smart card reader.
Readers not supplied by Thales are unsupported.

The ProtectServer PCIe HSM 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.

Micro-D subminiature (MSDM) connector   USB Port
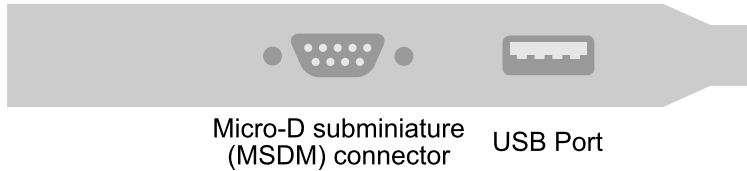
Installing the legacy card reader

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 as shown in "The connected legacy card reader" below (The illustration shows the card reader connected to a ProtectServer Network HSM).

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

The options are:

> Use a PS/2-to-USB adapter (pink) to connect the card reader to a USB port on the host computer.

> If you prefer not to expose USB ports on your crypto server (for security reasons), use a PS/2-to-USB adapter to connect the card reader to a standalone powered USB hub.

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

Figure 1: The connected legacy card reader

Completing Installation

After you have installed the ProtectServer HSM Access Provider, install the supplied SafeNet API or net server software.

Please refer to the installation instructions in the appropriate manual:

> *SafeNet ProtectToolkit-C Administration Guide*

> *SafeNet ProtectToolkit-J Reference Guide*
> *SafeNet ProtectToolkit-M User Guide*

CHAPTER 2:   Troubleshooting

The most common problem encountered when installing the 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 *ProtectServer 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 Thales Support. See "Support Contacts" on page 8 for further information.

Problem	Solution
The MSI (Microsoft Installer) application does not complete installation, or is left in an unstable state.	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.
The system locks up after the ProtectServer HSM Access Provider device driver package is installed. This may happen if a prior version of the device driver exists on the system.	1. Power down and remove the adapter. 2. Power up. 3. Uninstall all versions (old and new) of the ProtectServer HSM Access Provider / device driver package. 4. Power down and re-install the adapter. 5. Power up and reinstall the ProtectServer HSM Access Provider package.
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 PCIe slot, then uninstall the ProtectServer HSM Access Provider package. Following this, perform a fresh install of the ProtectServer HSM Access Provider package.
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.	This problem may be resolved by resetting the configuration data in the host system BIOS.

Fault Diagnosis Utilities

The SafeNet hardware maintenance utilities **hsmstate** and **hsmreset** can be used to carry out simple fault diagnosis. These utilities are included in the ProtectServer HSM Access Provider installation.

For more information, see the *ProtectServer 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`":

1. Execute **hsmreset**.

2. 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`":

1. Check to see that any connected external tamper detectors are correctly configured.

2. Make sure the adapter is sitting firmly and correctly in the PCIe slot.

CHAPTER 3: Hardware Reference

This Appendix contains hardware specifications and instructions on how to fit the HSM with an external tamper detector such as a micro switch.

Adapter Modification for External Tamper Detectors

Connect additional tamper detection devices using the tamper input header, located on the rear face of the card, as illustrated in "Rear face of the card" below.

Figure 2: Rear face of the card
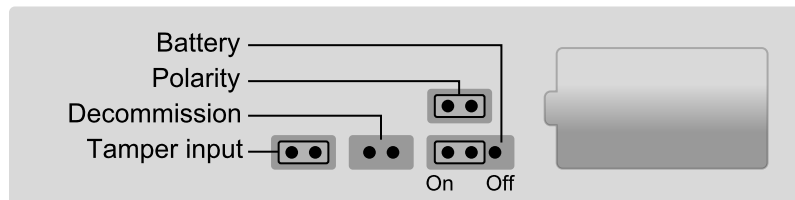
To fit an external tamper detection device

1. Remove the default jumper/shunt that bridges the two posts in the ProtectServer PCIe HSM's tamper input header (see "Rear face of the card" above).

2. Connect your external tamper device in the shunt's place.

   The cable end from your tamper-detection device must match the Molex socket on the adapter, which is designed to fit with an insertable connector housing (Molex part 35507-0200).

   a. Crimp a pair of 2mm WTB crimp terminals (Molex part 50212-8100) to the ends of your tamper detector's two-wire connector cable.

   b. Insert the crimped terminal sockets into the Molex connector housing.

3. Plug the newly-fitted connector cable into the PCIe adapter's tamper input header.

The external tamper detector must provide the following conditions:

> In the **untampered** condition, the device must provide a low-impedance path (short circuit) between the tamper-detection posts.

> In the **tampered** condition, the device must show an open circuit.

The Battery

The adapter is fitted with a backup battery, which maintains cryptographic keys and the correct time when the host computer is shut down, or when the adapter is otherwise disconnected from a power source.

The battery has an expected lifetime of ten years. It should not require replacement within 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. In SafeNet ProtectToolkit-C, use **ctcheck -b batterystatus** to return a state of **Good**/**Low**. See the *Administration Guide* for your SafeNet ProtectToolkit software for more information.

The RealTime Clock and memory retain their data as long as the adapter is in a powered system. The RTC performs a daily battery check. If it detects a low-battery warning, the battery may need to be replaced. If the adapter has been de-powered or removed from its system, the data in its memory is suspect. If the adapter has been continuously powered, then the data in memory can be trusted and you can make a backup before replacing the battery.

Port Specifications

The USB-to-serial cable provides an RS232 port with pin outs as shown in "Adapter serial connector" below. This port can be used for connecting a smart card reader or another serial device.

Figure 3: Adapter serial connector

1: DCD
2: RxD
3: TxD
4: DTR
5: GND
6: DSR
7: RTS
8: CTS
9: N/C
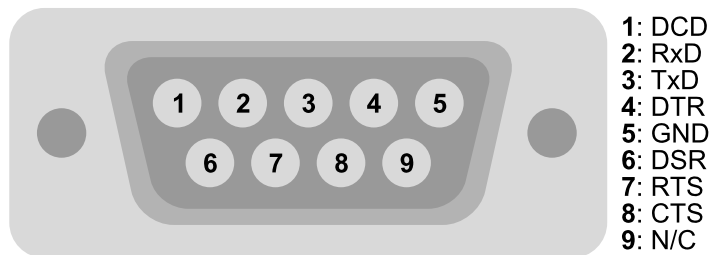
Glossary

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"