SafeNet ProtectToolkit J

Installation Guide

gemalto
security to be free

Part Number 007-002855-009
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
OVERVIEW

Introduction

ProtectToolkit J is a Cryptographic Service Provider for the Java Cryptographic Architecture Architecture (JCA) / Java Cryptographic Extension (JCE) interface. ProtectToolkit J implements a number of cryptographic algorithms that are supported by SafeNet's hardware encryption devices. These devices support encryption, signature generation and verification, message digests, key storage and message authentication. ProtectToolkit J also includes a clean-room implementation of the JCA/JCE framework allowing for immediate use with Java 1.5 and Java 1.6.

This document details the ProtectToolkit J software installation for supported platforms. For hardware installation instructions the reader is advised to refer to the *Adapter Installation* guide.

Who Should Read This Manual?

This manual is intended for the administrator responsible for installing software applications on a host computer system. It deals explicitly with the issues and concepts involved during the ProtectToolkit J software installation and uninstallation.

System Requirements

- A SafeNet cryptographic services adapter (not required for software only mode of operation).
- Java runtime (for ProtectToolkit J Runtime) or JDK (for ProtectToolkit J SDK). The product has been tested using Java runtime versions 1.5.x and 1.6.x. It may also operate correctly using other versions of the runtime however SafeNet does not warrant this.

  NOTE: Java runtime or JDK must be installed before installing ProtectToolkit J.

Supported Platforms

The supported platforms are listed in the following table.

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

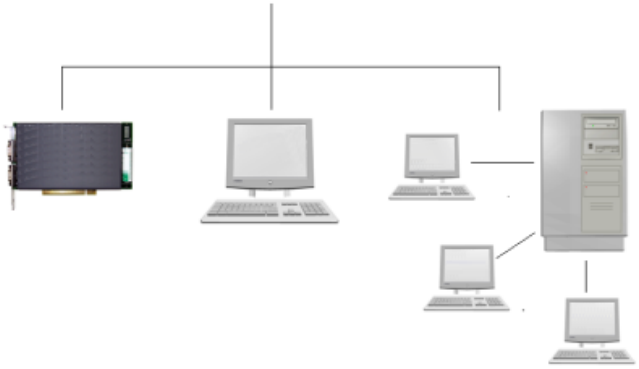
Operating system	32-bit binary 32-bit O/S		32-bit binary 64-bit O/S		64-bit binary 64-bit O/S	
	Network	PCIe	Network	PCIe	Network	PCIe
Windows Server 2012 R2 x86			–	–	C/M/J	C/M/J
Windows Server 2008 R2 x86	–	–	–	–	C/M/J	C/M/J
Windows 7	C/J	C/J			C/M/J	C/M/J
RedHat Enterprise Linux 6 x86	C/J	C/J			C/J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

Product Overview

ProtectToolkit J is SafeNet's Java Cryptographic Architecture (JCA) / Java Cryptographic Extension (JCE) provider. This allows Cryptographic processing using the Java development language. It requires SafeNet's ProtectToolkit C Runtime and an appropriate Access Provider installed.

The **ProtectToolkit C Runtime** package is needed to perform Cryptoki (PKCS#11) processing. The PTK C Hardware Runtime needs an Access Provider. There are two Access Provider install packages in order to operate the Runtime in a local PCI bus or network attached remote server arrangement.

The **ProtectToolkit C Software Development Kit (SDK)** is provided to develop applications using PKCS#11 processing. Refer to the ProtectToolkit C Installation Guide for instructions on how to install this SDK. The PTK C SDK includes the PTK C Runtime as well as a Software Emulation that does not require any Access Providers.



Hardware

The hardware version of ProtectToolkit C requires a SafeNet ProtectServer HSM. Refer to the Installation Manuals for instructions on how to install the adapter and the **ProtectToolkit C** Installation Guide for how to install the hardware Runtime

Software

The software only version of **ProtectToolkit C** requires a compatible PC, and would primarily be used in a development or testing environment. Refer to the **ProtectToolkit C** Installation Guide for instructions on how to install the software only Runtime package.

Remote Client/Server

This version of **ProtectToolkit C** requires a TCP/IP network with one or more workstations and a server. PTKC processing is performed by the server at the request of the client. The server must be running the hardware version of the Runtime package.

The Software

The following ProtectToolkit J packages can be found on the installation DVD:

Package	Windows	UNIX
ProtectToolkit J Runtime	PTKjprt.msi	PTKjprov
ProtectToolkit J SDK	PTKjpsdk.msi	PTKjpsdk

The ProtectToolkit J Runtime includes the necessary shared libraries required to interface to the ProtectToolkit C Runtime, as well as the Java class libraries that implement the JCE specification and the ProtectToolkit J provider. For installation instructions of the PTK C Runtime, please refer to the *ProtectToolkit C Installation Guide*.

The ProtectToolkit J SDK is provided as a software development platform.

NOTE: If you will be using larger key sizes or non-FIPS algorithms, install the SUN Unlimited Strength Jurisdiction Policy Files patch. Go to the SUN Web site (www.java.sun.com) and download.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2
RUNTIME

As stated in the overview section of this document, the ProtectToolkit J Runtime is a required component of the ProtectToolkit J software. The Runtime provides the application with the interface to perform cryptographic processing.

Note that this installation will install the necessary classes and libraries required to allow Java applications to access the provider. However, further configuration of your Java Runtime may be required to make the provider visible to your applications. Please consult your Java Runtime documentation for details on provider installation.

The following instructions are for installing the ProtectToolkit J Runtime environment. Each section details the installation instructions for various operating systems. Please refer to the section that corresponds to your operating system.

Windows

Installation

Before continuing with the ProtectToolkit J installation, ensure that you have installed a ProtectToolkit C Runtime. For details, please refer to the *ProtectToolkit C Installation Guide*.

NOTE: In order to be able to add or remove software you must have "Administrator" privileges.

The installation also provides for the automatic addition of the ProtectToolkit J Runtime directory to the system's execution path. This will make the newly installed programs and libraries available from the command prompt.

Uninstallation

To uninstall the ProtectToolkit J Runtime, open your Windows Control Panel and double-click on the Add/Remove Program icon. Then, locate the entry for the ProtectToolkit J Runtime installation and click on the remove button.

Solaris (SPARC & INTEL Versions)

Installation

Before continuing with the ProtectToolkit J installation, ensure that you have installed a ProtectToolkit C Runtime. For details, please refer to the *ProtectToolkit C Installation Guide*.

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

The ProtectToolkit J Runtime for Solaris is packaged using the standard Solaris packaging software.

Installation File	Details
PTKjprov	ProtectToolkit J Runtime Package

To install the desired software shown above, simply use the **pkgadd**(1M) program.

For example:

```
# cd <Solaris directory on the installation CD>
# pkgadd -d `pwd`/PTKjprov
```

Once installed, the software will be ready to use under `/opt/safenet/protecttoolkit5/ptk`.

To make use of the software you will need to add the `/opt/safenet/protecttoolkit5/ptk/bin` directory to your execution path and `/opt/safenet/protecttoolkit5/ptk/lib` to your library path. The following commands may be used to configure your paths for the **sh**(1) shell (please consult your Solaris manual for other shells):

Example under Solaris:

```
# PATH=/opt/safenet/protecttoolkit5/ptk/bin:$PATH
# export PATH
#
LD_LIBRARY_PATH=/opt/safenet/protecttoolkit5/ptk/lib:$LD_LI
BRARY_PATH
# export LD_LIBRARY_PATH
```

Uninstallation

To remove the software from your host system simply use the **pkgrm**(1M) program and select the appropriate package for removal.

For example:

```
# pkgrm PTKjprov
```

Linux

Installation

Before continuing with the ProtectToolkit J installation, ensure that you have installed a ProtectToolkit C Runtime. For details, please refer to the *ProtectToolkit C Installation Guide*.

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

The ProtectToolkit J Runtime for Linux is packaged using the standard **rpm**(8) packaging software.

Installation File	Details
PTKjprov-x.xx-y.i386	ProtectToolkit J Runtime Package

To install the desired software shown above, simply use the `rpm` program.

For example:

```
# cd <Linux directory on the installation CD>
# rpm -i PTKjprov-x.xx-y.i386.rpm
```

(where x.xx-y refers to the version of the software)

Once installed, the software will be ready to use under `/opt/safenet/protecttoolkit5/ptk`.

To make use of the software you will need to add the `/opt/safenet/protecttoolkit5/ptk/bin` directory to your execution path and `/opt/safenet/protecttoolkit5/ptk/lib` to your library path. The following commands may be used to configure your paths for the **sh**(1) `shell` (please consult your Linux manual for other shells):

```
# PATH=/opt/safenet/protecttoolkit5/ptk/bin:$PATH
# export PATH
#
LD_LIBRARY_PATH=/opt/safenet/protecttoolkit5/ptk/lib:$LD_
LIBRARY_PATH
# export LD_LIBRARY_PATH
```

Uninstallation

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

For example:

```
# rpm -e PTKjprov
```

IBM AIX

Installation

Before continuing with the ProtectToolkit J installation, ensure that you have installed a ProtectToolkit C Runtime. For details, please refer to the *ProtectToolkit C Installation Guide*.

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

The ProtectToolkit J Runtime for AIX is packaged using the standard AIX packaging software.

Installation File	Details
PTKjprov	ProtectToolkit J Runtime Package

To install the desired software shown below, simply use the **`installp`** program.

For example:

```
# installp -acgNQqwX -d . PTKjprov.rte
```

Once installed, the software will be ready to use under `/opt/safenet/protecttoolkit5/ptk`.

To make use of the software you will need to add the `/opt/safenet/protecttoolkit5/ptk/bin` directory to your execution path and `/opt/PTK/lib` to your library path. The following commands may be used to configure your paths for the **`sh`**`(1) shell` (please consult your AIX manual for other shells):

Example under AIX:

```
# PATH=/opt/safenet/protecttoolkit5/ptk/bin:$PATH
# export PATH
# LIBPATH=/opt/safenet/protecttoolkit5/ptk/lib:$LIBPATH
# export LIBPATH
```

Uninstallation

To remove the software from your host system, simply use the `installp` program and select the appropriate package for removal.

For example:

```
# installp -u PTKjprov
```

CHAPTER 3
SOFTWARE DEVELOPMENT KIT (SDK)

The following sections contain the installation instructions for the ProtectToolkit J Software Development Kit (SDK) package.

To use the SDK, you must have previously installed the PTK J RUNTIME.

Since it is not always feasible to offer the Protect Server hardware to multiple developers, testing can easily be performed on any machine using the software only version of ProtectToolkit C. It must be noted that the software-only variant of ProtectToolkit C is not a secure implementation since key files are located on the host drive. Due to the extra security provided by the adapter, it is recommended that only the hardware-based ProtectToolkit C Runtime be implemented in an operational environment.

The SDK includes the documentation and example code required for development using the ProtectToolkit J provider. In addition to the Javadoc generated documentation for ProtectToolkit J, a number of Adobe PDF reference manuals and tutorials are included.

Windows

Installation

The ProtectToolkit J SDK for Windows is packaged using an MSI package.

NOTE: To order to be able to add or remove software the current user must have "Administrator" privileges.

Installation File	Details
PTKjpsdk.msi	ProtectToolkit J SDK Package

To install the package, simply execute the program `PTKjpsdk.msi`. This will start the installation wizard. Follow the on-screen instructions to install the software.

The installation program will create a new program group named "Safenet\ProtectToolkit J\ SDK" and add it to your Start menu.

Uninstallation

To remove the software from your system please go to the "Add/Remove Programs" item in the Control Panel and select the "ProtectToolkit J SDK" item from the list.

Solaris

Installation

The ProtectToolkit J SDK for Solaris is packaged using the standard Solaris packaging software.

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

Installation File	Details
PTKjpsdk	ProtectToolkit J SDK Package

To install the package simply use the **pkgadd** (1M) program to add the PTKjpsdk package.

For example:

```
# cd <Solaris directory on the installation CD>
# pkgadd -d `pwd`/PTKjpsdk
```

Once installed, the software will be ready to use under /opt/safenet/protecttoolkit5/ptk. To make use of the software, you will need to add the /opt/safenet/protecttoolkit5/ptk/bin directory to your execution path and /opt/PTK/lib to your library path.

The following commands may be used to configure your paths for the **sh**(1) shell (please consult your Solaris manual for other shells).

Example under Solaris:

```
# PATH=/opt/safenet/protecttoolkit5/ptk/bin:$PATH
# export PATH
#
LD_LIBRARY_PATH=/opt/safenet/protecttoolkit5/ptk/lib:$LD_
LIBRARY_PATH
# export LD_LIBRARY_PATH
```

Uninstallation

To remove the software from your host, system simply use the **pkgrm**(1M) program and select the PTKjpsdk package for removal.

For example:

```
# pkgrm PTKjpsdk
```

Linux

Installation

The ProtectToolkit J SDK for Linux is packaged using the standard RPM packaging software.

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

Installation File	Details
`PTKjpsdk-x.xx-y.i386`	ProtectToolkit J SDK Package

To install the package, simply use the **`rpm`**`(8)` command to add the `PTKjpsdk-2.02-1.i386.rpm` package.

For example:

```
# cd <Linux directory on the installation CD>
# rpm -i PTKjpsdk-x.xx-y.i386.rpm
```

(where x.xx-y refers to the version of the software)

Once installed, the software will be ready to use under `/opt/safenet/protecttoolkit5/ptk`. To make use of the software you will need to add the `/opt/PTK/bin` directory to your execution path and `/opt/safenet/protecttoolkit5/ptk/lib` to your library path.

The following commands may be used to configure your paths for the **`sh`**`(8)` shell (please consult your Linux manual for other shells).

```
# PATH=/opt/safenet/protecttoolkit5/ptk/bin:$PATH
# export PATH
#
LD_LIBRARY_PATH=/opt/safenet/protecttoolkit5/ptk/lib:$LD_
LIBRARY_PATH
# export LD_LIBRARY_PATH
```

Uninstallation

To remove the software from your host, system simply use the following command:

```
# rpm -e PTKjpsdk
```

IBM AIX

Installation

The ProtectToolkit J SDK for AIX is packaged using the standard AIX packaging software.

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

Installation File	Details
PTKjpsdk	ProtectToolkit J SDK Package

To install the package, simply use the **`installp`** program to add the `PTKjpsdk` package.

For example:

```
#  installp -acgNQqwX -d . PTKjpsdk.rte
```

Once installed, the software will be ready to use under `/opt/safenet/protecttoolkit5/ptk`. To make use of the software, you will need to add the `/opt/PTK/bin` directory to your execution path and `/opt/safenet/protecttoolkit5/ptk/lib` to your library path.

The following commands may be used to configure your paths for the **`sh`**`(1)shell` (please consult your AIX manual for other shells).

```
# PATH=/opt/safenet/protecttoolkit5/ptk/bin:$PATH
# export PATH
# LIBPATH=/opt/safenet/protecttoolkit5/ptk/lib:$LIBPATH
# export LIBPATH
```

Uninstallation

To remove the software from your host system, simply use the **`installp`** program and select the `PTKjpsdk` package for removal.

For example:

```
# installp -u PTKjpsdk
```

CHAPTER 4
INSTALLATION TROUBLESHOOTING

This section is designed to troubleshoot a ProtectToolkit J installation on ProtectToolkit C using the Protect Server adapter.

The most common problems encountered with installing ProtectToolkit J on ProtectToolkit C and the Protect Server hardware is that the driver for the encryption board 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 consult your *Adapter Installation Guide* for troubleshooting options.

Try running the `hsmstate` utility. It should report each installed HSM (PCI or Network connect) is in NORMAL Mode. If that works, then try running the `ctconf` utility. This will ensure that the Cryptoki runtime is working.

Finally, if neither is of help in resolving the issue, please contact SafeNet support.

END OF DOCUMENT