Protect Server 2 PTK 5.0.1

CUSTOMER RELEASE NOTES

Issue Date: 26 January 2015

Document Part Number: 007-007171-010 Rev. D

Contents

Product Description

ProtectServer 2 is a major upgrade to the ProtectServer product line. ProtectServer2 introduces the PSE2 and PSI-E2 HSMs as direct replacements for the legacy PSE and PSI-E HSMs, which have been declared end of sale, and are no longer available for purchase.

Although the new PSE2 and PSI-E2 HSMs are functionally equivalent to their legacy counterparts, the underlying hardware is significantly different. The major hardware change is to the embedded cryptographic engine used on the HSMs. The legacy PSE/PSI-E HSMs incorporate the K5 cryptographic engine. The new PSE2/PSI-E2 HSMs incorporate the more modern K6 cryptographic engine.

Although every effort has been made to mitigate the impact of these hardware changes, the introduction of a new cryptographic engine impacts the following:

- Functionality modules (FMs). The processor used on the ProtectServer 2 HSMs is different from the processor used on the legacy ProtectServer HSMs. As a result, you must rebuild your FMs to run on the new hardware.
- Serial devices. The serial port on the ProtectServer HSMs has been replaced on the ProtectServer 2 HSMs with a USB port and a USB-to-serial cable. Any serial devices that were previously attached to a ProtectServer HSM will continue to work on a ProtectServer 2 HSM.

Refer to the *ProtectServer 2 Migration Guide* for a detailed list of the changes and enhancements introduced in ProtectServer 2, and how these changes impact migration to the new hardware.

ProtectToolkit (PTK) Software

ProtectServer 2 continues to use the ProtectToolkit (PTK) software. However, due to the hardware changes introduced in ProtectServer 2, the ProtectServer 2 PSI-E2 HSM requires PTK 5.0 or higher software.

> **Note:** PTK 5.0 is not tested or supported on the legacy PSI-E or PSG HSMs. You cannot deploy a mix of ProtectServer PSI-E and ProtectServer2 HSMs on the same client workstation or WLD/HA group. Backwards compatibility with the legacy PSI-E HSM will be added in a future release. Contact your SafeNet representative for more information.

As in previous releases, the PTK software includes the following components:

- PTK-C – Toolkit for PKCS #11 and C Language API calls (Windows/Linux)
- PTK-J – API support for Java (Windows/Linux)
- PTK-M - Microsoft CAPI and CNG support (Windows only)

FM SDK

In previous releases, the FM SDK (formerly called PPO) was provided on a separate CD. The FM SDK software is now bundled with the PTK software on the software DVD. Platform support is as follows:

Embedded FM development	Linux only
FM HOST applications	Windows and Linux

ProtectToolkit (PTK) Documentation

Documentation for all of the PTK software is provided on the PTK documentation DVD.

Release Description

PTK 5.0.1 provides several bug fixes, as listed in “Addressed Issues” on page 5.

Support for legacy PSE HSMs has also been tested and verified to work in PTK 5.0 and PTK 5.0.1. PSI-E and PSG HSMs continue to be unsupported in PTK 5.x.

PTK 5.0

PTK 5.0 is the initial software release for the new ProtectServer2 hardware. PTK 5.0 is compatible with the PSI-E2, PSE2, and legacy PSE only. Do not upgrade to PTK 5.0 if you are using the legacy PSI-E or PSG HSMs. Also do not insert or connect a ProtectServer2 HSM to a workstation connected to a ProtectServer PSI-E HSM.

PTK 5.0 is functionally equivalent to previous PTK releases. The FM SDK has been updated to support developing and building FMs for the new hardware. The FM SDK also includes several enhancements that improve the FM development process. See “New Features and Enhancements”, below, for more information.

Support for Legacy PSE HSMs

You can use both legacy PSE and PSE2 HSMs on the same PTK client workstation, with the following limitations:

HA/WLD limitations

You can use a mix of PSE and PSE2 HSMs with HA/WLD. Note, however, that the firmware version used on PSE HSMs is different than the firmware version used on PSE2 HSMs. Because of the difference in firmware, any keys used in the HA/WLD group must be fully permissive by the operational state of both the PSE and PSE2 firmware.

You cannot create new objects while in HA/WLD mode. To create additional objects, disable WLD/HA, create the new objects, replicate tokens, and re-engage WLD/HA.

FM limitations

The FM delete command will not delete FMs from the older PSE HSMs, it will only disable them, as in PTK 4.x.

Supported Firmware

PTK 5.0 supports firmware version 5.00.02. At the time of release, FIPS validation for the 5.00.02 firmware was in progress. Refer to the following web sites or contact SafeNet Support for the current FIPS validation status:

- Modules in Process: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf
- Completed Validations - Vendor List: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

Release Notes

The most up-to-date version of these release notes is available at the following location:

http://www.securedbysafenet.com/releasenotes/ptk/crn_ptk_5-0.pdf

New Features and Enhancements

ProtectServer 2 introduces the PSE2 and PSI-E2 HSMs. The PTK 5.0 release supports all of the functionality previously provided by the legacy PSE and PSI-E hardware and PTK software. No new features are provided in this release.

Software Changes and Enhancements

The PTK 5.0 FM SDK includes changes required to support FM development on the new hardware. The FM SDK has also been enhanced and updated to provide improved usability and functionality. This release also introduces some changes to the PTK software. Major changes/enhancements include the following:

- New FIPS guidelines have been implemented as per NIST SP 800-131A and FIPS PUB 186-4. These changes affect the list of supported algorithms, key types, and key sizes when operating in FIPS mode, as follows:
  - RSA, DSA and ECDSA signature generation with SHA1 is no longer allowed.
  - RSA and DSA key and signature generation operations are restricted to 2048 and 3072 bit key sizes only, and ECDSA key size to 224 bit or greater.

  Note that previously compliant key sizes will be allowed for signature verification operations. Refer to the *PTK-C Programming Guide* for a complete list of supported algorithms and their FIPS compatibility.
- Emulation mode has been enhanced to support Cryptoki (Cprov) function patching of any application that is run against the emulated cryptoki wrapper built with the emulated FM.
- The toolchain has been enhanced provide C99 support and to use the native system **make**.
- Configuration scripts are provided to automate the configuration of the FM development environment.
- Support for standard C **printf** to write debug messages to the **hsmtrace** log.

Refer to the *ProtectServer 2 Migration Guide*, on the documentation DVD, for a detailed list of all of the changes and enhancements introduced in PTK 5.0.

Hardware Changes and Enhancements

The new PSE2/PSI-E2 HSMs do not include a serial port. The serial port on these HSMs has been replaced with a USB port that provides serial access to the HSMs via the included USB-to-serial cable. Refer to the *PSE2 Installation Guide*, the *PSI-E2 Installation Guide*, and the *ProtectServer 2 Quickstart Guide* for more information.

Advisory Notes

Run “ctconf -t” on First Install of HSM

The first time you install a ProtectServer2 HSM, execute the command **ctconf -t** to synchronize the card clock with the machine clock before running any other command. You should also initialize the user token, as there are some performance tests that are skipped if the user token is not initialized.

Use Tamper to Recover From an Unresponsive State

If the ProtectServer2 HSM enters a non-useful or non-responsive state that does not resolve itself after a system reboot, try “tampering” the card. For the PSI-E2, remove the card from the computer for a few minutes and then re-insert it. For the PSE2, use the tamper key located on the rear of the appliance. If the HSM does not return to normal operation, contact SafeNet Customer Support.

Compatibility and Upgrade Information

Supported Operating Systems

PTK 5.0 is supported on the following operating systems, where **C** = PTK-C, PKCS #11 v2.10/2.20; **M** = PTK-M, MS CSP 2.0 with CNG; **J** = PTK-J, Java runtime 1.6.x/1.7.x

Operating system		32 bit	64 bit
Windows	Server 2012 R2		C/M/J
	Server 2008 R2		C/M/J
	7	C/J (KSP is supported)	C/M/J
Linux	RHEL 6	C/J	C/J

Required Third-Party Software

You must install the following third-party software before installing PTK 5.0:

Operating system	Required third-party software
Windows	• Java runtime 1.6.x or 1.7.x • Microsoft Visual C++ (MSVC) 2005, 2008, and 2010 redistributable runtime packages • .NET 3.5 and 4.5 The MSVC and .NET software is available for free download from Microsoft.
Linux	• Java runtime 1.6.x or 1.7.x

Supported Server Hardware

The PSI-E2 HSM card is designed to the PCIe 1.1 standard, for use in servers with PCIe x4 slots. You can also install the PSI-E2 HSM in servers equipped with larger connector slots (from x4 to x16), with the following caveat:

> Some computer motherboards are equipped with x16 slots that are intended to be used for video cards only. If you install the PSI-E2 card in a video-only x16 slot, it will be detected on startup, but won't respond as a video card. As a result, the system will not boot successfully. This problem is not specific to the PSI-E2 and could happen with any non-video PCIe card. If you encounter this issue on your server, try another available slot.

Modern motherboards increasingly tend to support PCIe 2.0 standard, which is backward compatible with version 1.1 when correctly implemented.

Addressed Issues

This section lists the issues addressed in this release. The following table defines the issue severity codes:

Severity	Classification	Definition
C	Critical	No reasonable workaround exists
H	High	Reasonable workaround exists
M	Medium	Medium level priority problems
L	Low	Lowest level priority problems

List of Addressed Issues

The following table lists the issues addressed in this release.

Issue	Severity	Synopsis
(PSR-744) Linux HSM emulator broken	M	**Problem:** The HSM emulator does not work on Linux platforms. **Resolution:** Fixed.
(PSR-743) Makefile incorrect for building FM SDK samples	M	**Problem:** The makefile used to build the FM SDK samples is incorrect. **Resolution:** Fixed.
(PSR-742) CM_eInfo attribute in cmlib.h breaks existing FM code	M	**Problem:** The **cmlib.h** in PTK5.0 introduces a **CM_eInfo** attribute in the middle of an existing enumeration. This breaks existing FM code. **Resolution**: Fixed. The CM_eInfo attribute has been moved to the end of the enumeration.
(PSR-597) **etnetserver** service fails to start on Windows	M	**Problem:** The **etnetserver** service fails to start on Windows. As a result, you cannot use a network connection (via the Network Access Provider) to access a PSI-E2 HSM installed on a Windows workstation. If you install a PSI-E2 HSM on a Windows workstation you will only be able to access it locally, using the HSM Access Provider. **Resolution:** Fixed. The **etnetserver** service runs on all supported platforms.

Known Issues

This section lists the issues known to exist in the product at the time of release. The following table defines the issue severity codes:

Severity	Classification	Definition
C	Critical	No reasonable workaround exists
H	High	Reasonable workaround exists
M	Medium	Medium level priority problems
L	Low	Lowest level priority problems

List of Known Issues

The following table lists the known issues at time of release. Workarounds are provided where available.

Issue	Severity	Synopsis

(PSR-741) GCC bug requires **-fno-tree-vectorize** to be set	M	**Problem:** In some cases, a bug in the GCC 4.6.x optimizer (the version used for PTK 5 FMs) will cause a compilation failure with the following error:
		`Internal compiler error: in vect_transform_stmt, at tree-vect-stmts.c:4887`
		Workaround: To avoid this bug, add **-fno-tree-vectorize** to the **gcc** command line. This can be done by including the following line in your FM makefiles, or at the end of **opt/safenet/fm-toolchain/fmgcc-ppc440e-1.0.0/fmconfig.mk**:
		`CFLAGS += -fno-tree-vectorize`

Issue	Severity	Synopsis
(PSR-590) KMU, gmadmin, and ctbrowse batch files do not check for mode. (Windows)	L	**Problem**: The PTK Windows software includes hardware and software batch files for KMU, ctbrowse, and gmadmin. If you attempt to run a batch file while not in the correct mode, the mode does not automatically switch and the batch file will not execute. **Workaround**: If you require PTK-M, you must ensure you are in the correct mode before running the batch files. You can reset the mode by configuring your environment or by re-running the installer. If you do not require PTK-M, you can delete the **cryptoki.dll** file from the **C:\Windows\System32** folder to resolve this issue.
(PSR-584) PTK-M: Right-click menus do not work for some functions	L	**Problem**: Some PTK-M right-click menus do not work correctly. **Workaround**: Use the main menu to perform any functions that do not operate correctly using the right-click menus.
(PSR-580) PTK-M Administration Tool (gmadmin) executes all operations on device0 when multiple cards installed	M	**Problem**: If you have multiple ProtectServer 2 devices installed, any operations you perform using the PTK-M Administration Tool (gmadmin) such as tamper, clock sync, transport mode etc. default to device0, regardless of the selected device. As a result, you cannot configure any device other than device0 using gmadmin. **Workaround:** Use the PTK-C utilities to configure your devices when you have multiple devices installed.
(PSR-575) Hardware tamper requires HSM reset and reports a critical HSM crash in the hsmtrace log	M	**Problem:** After a hardware tamper, you must reset your HSM. In addition, the hsmtrace log reports a critical HSM crash related to the hardware tamper. You can ignore this message. This does not occur for a software tamper initiated from the command line.
(PSR-563) HSM Access Provider uninstall does not delete driver (Windows)	M	**Problem:** Using the Programs and Features control panel to uninstall the SafeNet HSM Access Provider on Windows deletes the program but does not delete the driver. **Workaround:** Use the Device Manager to delete the driver.
(PSR-542) Loading an FM causes a halt/reset, which is reported as an error	M	**Problem:** When you load an FM, the HSM is automatically halted and reset. This is expected behavior. The halt/reset, however, is reported as an error in /var/log/messages. You can ignore these messages.
(PSR-541) KMU: No error reported for key export when to smart card when no smart card present	M	**Problem:** If you attempt to export a key to a smart card using the KMU utility when there is no smart card attached, no error message is displayed. **Workaround**: Ensure that a smart card reader, with a smart card inserted, is attached to the HSM before attempting to perform a key export.

Support Contacts

If you have questions or need additional assistance, contact Technical Support using the listings below:

Contact method	Contact information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	(800) 545-6608, (410) 931-7520
	Australia and New Zealand	+1 410-931-7520
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	+1 410-931-7520
	United Kingdom	0870 7529200, +1 410 931-7520
Web	www.safenet-inc.com	
Support and Downloads	www.safenet-inc.com/Support Provides access to the SafeNet 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 SafeNet Knowledge Base.	