SafeNet ProtectServer/ProtectToolkit 5.1

CUSTOMER RELEASE NOTES

Issue Date: 26 September 2016

Document Part Number: 007-007171-010, Rev. G

Contents

Product Description

ProtectToolkit is SafeNet's PKCS # 11 V 2.10-compliant API product. It supports the following hardware platforms:

- ProtectServer External 2 (PSE2) – intelligent cryptographic adapter (external network appliance engine).
- ProtectServer Internal Express 2 (PSI-E2) – intelligent cryptographic adapter (PCIe bus).
- ProtectServer External (PSE) – legacy PSE. This platform has been declared end-of-sale and is no longer available for purchase.
- ProtectServer Internal Express (PSI-E) – legacy PSI-E. This platform has been declared end-of-sale and is 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 and PSI-E HSMs contain the K5 cryptographic engine. The new PSE2/PSI-E2 HSMs contain the more modern K6 cryptographic engine.

ProtectToolkit (PTK) Software

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)

> **Note:** PTK 5.1 is not tested or supported on legacy PSG HSMs.

Release Description

PTK 5.1 is a maintenance software release that extends PTK 5.0.1 functionality to additional operating systems and the legacy PCI-E hardware platform. PTK 5.1 is compatible with the new PSE2 and PSI-E2 HSMs, and the legacy PSE and PSI-E HSMs. Do not upgrade to PTK 5.1 if you are using the legacy PSG HSM.

Support for Legacy PSI-E HSMs

PSI-E with PTK 5.1.x supports all the same functionality as PSI-E2 with PTK 5.1, with the following limitations:

- You cannot use a mix of PSI-E and PSI-E2 HSMs with HA/WLD. PSI-E HSMs connect only with other PSI-E HSMs, and PSI-E2 HSMs connect only with other PSI-E2 HSMs.
- The FM delete command does not delete FMs from legacy PSI-E HSMs. This command only disables them, as in PTK 4.x.

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_5-1.pdf

If needed, the previous version of these release notes can be found at the following location:

http://www.securedbysafenet.com/releasenotes/ptk/crn_ptk_5-0-1.pdf

New Features and Enhancements

This release expands support to the SUSE12, Solaris and AIX operating systems, as well as offering backward compatibility with legacy PSE-I HSMs. New PSI-E2 firmware adds RSA-PSS algorithm support.

Advisory Notes

GCC Tree-Vectorize Error

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
```

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
```

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.

Running ctconf –l has Different Effect on K6 and K5 Cards

If you run **ctconf –l** on a PSE2 with a K6 card or a PSI-E2, the FM is deleted. If you run this command on a legacy PSE with a K5 card or a PSI-E, the FM is only disabled.

Compatibility and Upgrade Information

Supported Operating Systems

PTK 5.1 is supported on the following operating systems.

Operating system		OS type	64 bit PTK	64 bit PTK supported hardware	32 bit PTK	32 bit PTK supported hardware
Windows	Server 2008 (R1 and R2)	64 bit	C/M/J	all platforms	C/J	PSE2, PSE
	Server 2012 R2	64 bit	C/M/J	all platforms	C/J	PSE2, PSE
	7	32 bit	-	-	C/J (KSP supported)	All platforms
	7	64 bit	C/M/J	all platforms	C/J	PSE2, PSE

Operating system		OS type	64 bit PTK	64 bit PTK supported hardware	32 bit PTK	32 bit PTK supported hardware
Linux	RHEL 6	32 bit	-	-	C/J	all platforms
	RHEL 6	64 bit	C/J	all platforms	C/J	PSE2, PSE
	RHEL 7	64 bit	C/J	PSE2, PSI-E2, PSE	C/J	PSE2, PSE
	SUSE12	64 bit	C/J	PSE2, PSI-E2, PSE	C/J	PSE2, PSE
AIX	6.1	64 bit	C/J	PSE2, PSE	C/J	PSE2, PSE
	7.1	64 bit	C/J	PSE2, PSE	C/J	PSE2, PSE
Solaris	10 SPARC, 10 x86, 11 SPARC and 11 x86	64 bit	C/J	PSE2, PSE	C/J	PSE2, PSE

C = PTK-C, PKCS #11 v2.10/2.20.
M = PTK-M, MS CSP 2.0 with CNG
J = PTK-J, Java runtime 6.x/7.x/8.x.

Supported Firmware

PTK 5.1 supports firmware versions 5.00.02 and 3.20.05 as follows:

Firmware Version	Available Platforms	FIPS Approved at time of PTK 5.1 Release?
5.00.02, 5.00.03	PSE2, PSI-E2	No
3.20.05, 3.20.08	PSE, PSI-E	Yes

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

New in Firmware 3.20.08 and 5.00.03

PSI-E firmware 3.20.08 and PSI-E2 5.00.03 firmware both address the following issues:

Issue	Severity	Synopsis
PSR-785, PSR-976	M	Corrected discrepancy in ECDH.
PSR-1122	M	Corrects possible segmentation fault during large C_GenerateRandom calls to PSE.

In addition, PSI-E2 5.00.03 firmware also addresses:

Issue	Severity	Synopsis
PSR-957	M	Corrects information displayed with ctbrowse utility.

As well as specific bug fixes, also adds RSA-PSS support to PSI-E2. Both firmware 3.20.08 and 5.00.03 are available for download separate from PTK 5.1.

Required Third-Party Software

You must install the following third-party software before installing PTK 5.1:

Operating system	Required third-party software
Windows	• Java runtime 6.x, 7.x, or 8.x • Microsoft Visual C++ (MSVC) 2010 redistributable runtime packages • .NET 3.5 and 4.5 The MSVC and .NET software is available for free download from Microsoft.
Linux, AIX, or Solaris	• Java runtime 6.x, 7.x, or 8.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.

Known Issues

Issue Severity

This table serves as a key to the severity and classification of the issues listed in the **Known Issues** table.

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-809)	M	**Problem:** PTK-M is not available for Windows 32 bit. **Workaround:** Develop with KSP.

Issue	Severity	Synopsis
(PSR-1100)	M	**Problem:** If you run ctfm to install an FM in an AIX environment, the HSM halts with the error “could not verify Functionality Module image: error 0x5, general error.” Despite the error, the FM successfully installs. **Workaround:** Reset the HSM using the command **hsmreset**.
(PSR-1081)	M	**Problem:** If you update the firmware on a PSE2, the HSM halts with the error “Could not verify firmware image: 0x5, general error.” Despite the error, the firmware successfully updates. **Workaround:** Reset the HSM using the command **hsmreset**.
(PSR-953)	M	**Problem:** Firmware upgrade via gtcadmin fails with the error code 0x80000384, and the HSM is left in a tampered state. **Workaround:** Upgrade firmware using ctconf.
(PSR-951)	L	**Problem:** The ctconf temperature reading does not function with legacy K5 cards. Therefore, the temperature displayed on PSE and PSI-E is 0 Celsius, which is the default value. **Workaround:** None.

Product Documentation

The product documentation has been updated to include new support contact information, and to include a navigable table of contents frame in each PDF file. In addition, the technical content was updated in the following documents. With the exception of these documents, the 5.0 documentation applies to the PTK 5.1 release:

- PTK-C Administration Guide (P/N: 007-008393-007, Rev A)
- FM SDK Programming Guide (P/N: 007-012739-002, Rev A)

Support Contacts

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

Contact method	Contact	
Address	SafeNet, Inc. 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	https://safenet.gemalto.com/	
Support and Downloads	https://safenet.gemalto.com/technical-support Provides access to the SafeNet Knowledge Base and quick downloads for various products.	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com/eservice_ENU 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.	