PTK 4.3

CUSTOMER RELEASE NOTES

Issue Date: 21 October 2013

Document Part Number: 007-007171-009 Rev. A

Contents

Product Description 2
Release Description 2
Release Notes 2
New Features and Enhancements 2
PTK release history 2
Advisory Notes 3
Run “ctconf -t” on first install of card 3
PSI-E if in doubt, tamper 3
Compatibility and Upgrade Information 4
Supported Operating Systems 4
Supported Server Hardware 4
Upgrade Instructions 4
Resolved Issues 5
List of Resolved Issues 5
Known Issues 6
List of Known Issues 6
Documentation Addendums 7
ProtectToolkit C Installation Guide addendums 7
ProtectToolkit C Administration Manual addendums 7
ProtectToolkit C Programmers Manual addendums 8
Support Contacts 8

Product Description

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

- ProtectServer External (PSe) – intelligent cryptographic adapter (external network appliance)
- ProtectServer Internal (PSI-E) – intelligent cryptographic adapter (PCIe bus)
- ProtectServer Gold – legacy intelligent cryptographic adapter (PCI bus)

ProtectToolkit includes the following software components:

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

Release Description

PTK 4.3 is a maintenance release that addresses defects discovered in previous PTK releases. PTK 4.3 supports firmware versions 3.20.00 or 3.20.03, as follows:

3.20.00	Provides support for the bug fixes listed in "Resolved Issues" on page 5, except for the following issues, which require firmware 3.20.03: • 186550 • 183586 • 181166 **Note:** Firmware 3.20.00 is FIPS approved.
3.20.03	Provides support for all of the fixes listed in "Resolved Issues" on page 5. **Note:** Firmware 3.20.03 is not currently FIPS approved.

You can apply firmware 3.20.00 or 3.20.03 to PSe, or PSI-E devices running firmware 3.11.01 or higher. See "Upgrade Instructions" on page 4 for more information.

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_4-3.pdf

New Features and Enhancements

PTK 4.3 addresses the defects listed in "Resolved Issues" on page 5.

PTK release history

The following table summarizes the features and enhancements included in the previous PTK releases. See the release notes for each listed release for more information.

PTK release	Feature summary
4.2.1	Bug fixes.
4.2.0	Increased Performance Level on PSI-e Balanced Performance Throttling PTK-C High Availability RHEL6/OpenSuse11 support ECDSA_SHA2 support Seimens CardOS V4.4 smart card support Bug Fixes The following FIPS-mode restrictions have been relaxed to enhance compatibility with the European EMV specification when operating in FIPS mode: • 2-Key Triple-DES Encryption is ALLOWED for use until December 31, 2015 • 2-Key Triple-DES Decryption is NOT-ALLOWED for use past December 31, 2010. It is allowed for use to decrypt already encrypted data with 2-Key Triple-DES. • RSA/DSA 1024 Signature Generation is ALLOWED for use until December 31, 2013. NOT ALLOWED for use after 2013. • RSA/DSA 1024 Signature Verification is ALLOWED for use until December 31, 2015. • SHA-1 is ALLOWED for use as part of Generating a Signature until December 31, 2013. NOT ALLOWED for use in generating a signature in 2014. • SHA-1 is ALLOWED for use for all non-Signature related activities past 2015 (for example, to identify a key with a hash). • the CKM_ECDH1_DERIVE algorithm is available in FIPS mode
4.1.1	Updated UNIX drivers PSG Hardware Refreshed Bug fixes
4.1.0	Key Usage Limits Remote Activation Bug fixes
4.00	PSI-E (ProtectServer Internal for PCI-E slots) short-form-factor adapter card supported Bug fixes
3.x and earlier	Refer to the release notes for these releases for details.

Advisory Notes

Run “ctconf -t” on first install of card

The first time you install a PSI-E card, 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 a couple of performance tests that are skipped if the user token is not initialized.

PSI-E if in doubt, tamper

If the PSI-E card displays a non-useful or non-responsive state that does not resolve itself after a system reboot, try “tampering” the card by removing it from the computer for a few minutes and then re-inserting it. If the card does not return to normal operation, contact SafeNet Customer Support.

Compatibility and Upgrade Information

Supported Operating Systems

PTK 4.3 is supported on the following operating systems:

Operating system		32 bit	64 bit	32-bit PTK on 64-bit OS
Windows	Server 2008 R2		X	
	Server 2012		X	
	7	X	X	
	8	X	X	
Linux	RHEL 5	X	X	
	RHEL 6	X	X	
	SUSE 10	X	X	
	SUSE 11	X	X	
Solaris	10 SPARC		X	X
	10 x86		X	X
	11 SPARC		X	X
	11 x86		X	X
AIX	6.x		X	X
	7.x		X	X

Supported Server Hardware

PTK 4.3 has been tested to run successfully on the following server hardware. This list is not exhaustive and PTK 4.3 may run successfully on other untested hardware platforms:

- Cisco UCS 210 M1
- Dell R610
- Dell R710
- Dell T610
- Fujitsu Primergy RX 200 S6
- Fujitsu Sun Sparc M4000
- HP DL 380 G2 AMD Based
- HP DL 380 G5
- HP DL 380 G7
- IBM x3650 M2

Upgrade Instructions

Refer to the PTK 4.3 Upgrade Instructions document (P/N 007-007568-009) for detailed instructions describing how to upgrade to PTK 4.3.

Resolved Issues

This section lists the issues that were resolved 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 Resolved Issues

Issue	Severity	Synopsis
(186550) PSIe command collision in multithread	M	**Problem:** Calls to MD_SendReceive when the HSM is under heavy load in a MultiThread environment, may cause the HSM to hang. **Resolution:** This issue has been resolved. Requires firmware 3.20.03.
(183587) Application crash when all HA members fail (PTK 4.2.1)	M	**Problem:** If both the HSMs in a WLD\HA group become unavailable due to a network failure, the application crashes (PTK 4.2.1). **Resolution:** This issue has been resolved.
(183586) Token replication fails after slot deletion	M	**Problem:** If slots are out of order due to deletion and subsequent addition of new slots, the token replication fails between the 2 HSMs in WLD. **Resolution:** This issue has been resolved. Requires firmware 3.20.03.
(181299, 182196) Memory leak in the PTK 4.2.1 netclient library	M	**Problem:** Memory leak in the PTK 4.2.1 netclient library. **Resolution:** This issue has been resolved.
(181296) C_CreateObject fails in HA mode	M	**Problem:** The C_CreateObject() call crashes the JVM in a JCPROV-based application. **Resolution:** This issue has been resolved.
(181166) SMS key rollover may cause PTK-C to lockup	M	**Problem:** Secure Messaging system (SMS) key rollover can cause a lockup in the PTK C Cryptoki library. **Resolution:** This issue has been resolved. Requires firmware 3.20.03.
(181025) No Java 7 support in PTK-J	M	**Problem:** Java 7 is not supported in PTK-J. **Resolution:** Support for Java 7 in PTK-J has been added in PTK 4.3
(179170) PTK-J supports only 16 slots	M	**Problem:** PTK-J only supports 16 slots. **Resolution:** PTK-J now supports up to 64 slots.
(178285) HSM not available on wake up from hibernate/sleep	M	**Problem:** Hibernate\Sleep on Windows causes HSM to become un-available at resume\wakeup. **Resolution:** This issue has been resolved.
(177605) PSIe HSM invisible to application	M	**Problem:** On a server equipped with multiple PSIe HSMs, an HSM may become invisible to the application due to an etnetserver error (PTK 4.2, firmware 3.10.05, Windows 2008 R2). **Resolution:** This issue has been resolved.
(177532) JVM crashes on 64-bit Linux when running 32-bit PTK 4.2.1	H	**Problem:** JVM crashes on 64-bit Linux when running 32-bit PTK 4.2.1 **Resolution:** This issue has been resolved.

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-30) 32-bit PTK on 64-bit Linux is not usable.	M	**Problem:** The 32-bit version of PTK does is not useable on a 64-bit version of Linux. **Workaround:** Only use the 32-bit PTK on 32-bit workstations.
(PSR-187) Cannot configure IIS or CA with KSP	M	**Problem:** KSP can see all available slots after registering the appropriate cryptoki.dll. However, CA and IIS configuration cannot see the SafeNet KSP provider. KSP log indicates no slots are available. **Workaround:** Do not install both KSP and PTK-M at the same time.
(PSR-189) KSP log does not record success messages.	M	**Problem:** KSP log (C:\LunaKSP.txt) previously recorded both success and error messages but now only records errors. **Workaround:** None.
(144698) Power Profile BIOS setting on HP ProLiant DL380 G7 Server series may cause instability	M	**Problem:** On the HP ProLiant DL380 G7 Server series, the setting of the **HP Power Profile** option in the BIOS may cause system instability. **Workaround:** Go into the BIOS and change the setting for the **HP Power Profile** (under **Power Management Options**) to **Maximum.**
(134706) PTK-M admin intermittently shows unhandled exception	M	**Problem:** The PTK-M gmadmin.exe utility intermittently shows an unhandled exception on 32-bit Win2K3 and Win2k8 when you allocate the space. However, it works fine after you click on Continue. **Workaround:** None.
(125961) After reinitializing the token, you are prompted to enter the SO PIN three times.	L	**Problem:** After you reinitialize the token (ctconf -rO), you are prompted to enter the security officer PIN three times. You would normally be prompted to enter the SO PIN only twice. **Workaround:** None.
(111736) PSe powers up automatically following a shutdown	L	**Problem:** After powering off the PSe with the command "poweroff" or "shutdown -h now", the PSe powers up on its own after a few (2.5 to 5) hours. **Workaround:** None.
(111085) ChipDrive card reader is not compatible with PSI-E card	M	**Problem:** The power provided by the 9-pin port on the PSI-E card is not adequate to power the ChipDrive card reader. **Workaround:** If you want to use a ChipDrive card reader with the PSI-E card, the ChipDrive card reader must be equipped with a PS2 power connector and both the 9-pin connector and the PS2 connector must be connected.

Issue	Severity	Synopsis
(88844) ProtectServer performance slows down with an increase in the number of slots	M	**Problem:** Creation of new slots to store a certificate and a key pair fills up the secure memory and slows down the ProtectServer performance. **Workaround:** The user must notice the notification on the HSM reaching its memory limit.
(59882) 'ctstat' conflicts with name of Solaris 10 utility	L	**Problem:** There is a Solaris 10 utility called 'ctstat', which happens to be the name of a PTK-C utility. This can be a problem if the user has PTK-C tools in his PATH. **Workaround:** If you intend to have your PTK-C ctstat in the PATH, make sure you have /opt/PTK/bin listed before /usr/bin in the PATH.

Documentation Addendums

The product documentation has not been revised for this release. Any known documentation errors or omissions are addressed below.

ProtectToolkit C Installation Guide addendums

VKD Luna driver conflict
The PTK-C installation instructions for Linux should be prefaced with the following note:

Note The Luna VKD driver conflicts with the PTK e8k driver. Before installing PTK-C, you must uninstall the Luna VKD driver. If the VKD driver is required, you cannot install PTK-C.

ProtectToolkit C Administration Manual addendums

Secure storage
The manual states that the PSI-e is equipped with 16 Mb of secure storage. This is incorrect. The PSI-e provides only 4 Mb of secure storage.

Recommended number of slots
The manual states the following:

> "It is recommended that you create no more than 50 slots. If you create more than 80 slots, the HSM may become unstable."

The number of supported slots has been increased. The statement should read as follows:

> "HSM performance degrades as the number of slots increases. Creating too many slots may cause unacceptable performance. To ensure reasonable performance, it is recommended that you create no more than 200 slots."

Battery
The SafeNet Protect Series HSMs are fitted with a battery that is used to preserve the sensitive information stored on the HSM while the PC is powered down or when the HSM is removed from the PC during transport mode (see "Using Transport Mode to Avoid a Board Removal Tamper" in the ProtectToolkit C Administration Manual).

If the HSM is to be kept in storage (without keys present) it is recommended that you isolate or disconnect the battery to avoid wearing it down, thus extending its lifespan.

You can use the **ctconf** command to test the condition of the battery. If the Battery Status indication is not GOOD, backup the HSM keys before powering down the PC to avoid losing the keys.

ProtectToolkit C Programmers Manual addendums

FIPS key sizes
In Table 42: Mechanisms - Key Size Range and Parameters, the legend includes the following notes:

> "All RSA operations performed under FIPS mode are carried out only if the specified key has a modulus of 2048 bits or greater. Any attempt to create an RSA key smaller than 2048 bits while running in FIPS mode results in a CKR_KEY_SIZE_RANGE or CKA_TEMPLATE_INCONSISTENT error."
>
> "All DSA and DH operations performed under FIPS mode are carried out only if the specified key has a modulus of 2048 bits or greater. Any attempt to create a DSA or DH key smaller than 2048 bits while running in FIPS mode results in a CKR_KEY_SIZE_RANGE or CKA_TEMPLATE_INCONSISTENT error."

The minimum required key size for FIPS approved algorithms is 1024 bits, not 2048 bits as stated in the manual.

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
Email	support@safenet-inc.com	
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.	