SafeNet ProtectServer/ProtectToolkit 5.3

CUSTOMER RELEASE NOTES

Issue Date: 08 December 2016

Document Part Number: 007-007171-012 Rev. A

Contents

Product Description

SafeNet ProtectServer/ProtectToolkit is Gemalto's PKCS # 11 V 2.20-compliant API product. It supports the following hardware platforms:

- SafeNet ProtectServer Network HSM – intelligent cryptographic adapter (external network appliance engine).
- SafeNet ProtectServer PCIe HSM – intelligent cryptographic adapter (PCIe bus).
- ProtectServer External (PSE) – legacy network appliance HSM. This platform has been declared end-of-sale and is no longer available for purchase.
- ProtectServer Internal Express (PSI-E) – legacy PCIe HSM. This platform has been declared end-of-sale and is no longer available for purchase.

Although the SafeNet ProtectServer Network HSM and SafeNet ProtectServer PCIe HSM 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 SafeNet ProtectServer Network HSM and SafeNet ProtectServer PCIe HSM contain the more modern K6 cryptographic engine.

SafeNet ProtectServer/ProtectToolkit Software

As in previous releases, the SafeNet ProtectServer/ProtectToolkit software includes the following components:

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

> **Note:** SafeNet ProtectServer/ProtectToolkit 5.3 is not tested or supported on legacy PSG HSMs.

Release Description

SafeNet ProtectServer/ProtectToolkit 5.3 extends the functionality and utility of the SafeNet ProtectServer HSMs. SafeNet ProtectServer/ProtectToolkit 5.3 is compatible with the new SafeNet ProtectServer Network HSM and SafeNet ProtectServer PCIe HSM, and with the legacy PSE and PSI-E HSMs. Refer to "New Features and Enhancements" on the next page for details.

> **Note:** Do not upgrade to SafeNet ProtectServer/ProtectToolkit 5.3 if you are using the legacy PSG HSM.

Support for Legacy PSI-E HSMs

PSI-E with SafeNet ProtectServer/ProtectToolkit 5.3 supports all the same functionality as the SafeNet ProtectServer PCIe HSM with SafeNet ProtectServer/ProtectToolkit 5.3, with the following limitations:

- You cannot use a mix of PSI-E and SafeNet ProtectServer PCIe HSM cards in the same server. When installing multiple HSMs in a server, ensure that all of the HSM PCIe cards are of the same type (all legacy PSI-E or all

SafeNet ProtectServer PCIe HSM).

- The FM delete command (**ctconf –l**) 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_5-3.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_5-2.pdf

New Features and Enhancements

This release provides the following new features and enhancements:

Custom FM calls through Cryptoki, Secure Messaging, and HA/WLD

The new **FMSC_SendReceive** function allows custom FMs to be called directly through the Cryptoki interface, rather than through the Message Dispatcher interface (ETHSM). A new sample FM, **secfmenc**, is provided to demonstrate the use of this function. Custom FM calls can now use the following features:

- **Secure Messaging**: send and receive FM requests in encrypted form
- **High Availability/Work Load Distribution**: configurations can now be used with FMs

FM Compilation Support on Windows

SafeNet ProtectServer/ProtectToolkit 5.3 adds support for a Windows version of the FM emulation libraries, allowing the development, compilation, and testing of FMs on all supported Windows operating systems (see "Supported Platforms" on page 6). Automated scripts are provided that build and install the cross-compiler and set up a MinGW environment.

Support for AIX 7.2

SafeNet ProtectServer/ProtectToolkit 5.3 adds support for the AIX 7.2 operating system. See "Supported Platforms" on page 6 for a full list of supported operating systems.

Vulnerable Mechanisms Restricted by Default

Newly-discovered key extraction techniques have revealed vulnerabilities in some PKCS#11 mechanisms. These mechanisms are now restricted by default in the factory settings of all new HSMs, or when flags are set to "**0**" (all flags cleared). These mechanisms cannot be enabled in FIPS mode. The *Weak PKCS#11 Mechanisms* flag, when set (**ctconf -fw**), allows the use of these less-secure mechanisms.

The following mechanisms are affected:

- `CKM_CONCATENATE_BASE_AND_DATA`
- `CKM_CONCATENATE_BASE_AND_KEY`
- `CKM_CONCATENATE_DATA_AND_BASE`

- `CKM_XOR_BASE_AND_DATA`
- `CKM_XOR_BASE_AND_KEY`
- `CKM_EXTRACT_KEY_FROM_KEY`

Set Mode Tool for Changing Cryptoki Provider

In SafeNet ProtectServer/ProtectToolkit SDK 5.3 for Windows systems, the software emulation batch files for **ctbrowse**, **KMU**, and **gCTAdmin** have been removed, and a new executable binary file called **setmode** has been added. **setmode** allows the user to easily toggle between software emulator and hardware modes without manually editing the Windows registry.

SafeNet ProtectServer PCIe HSM Driver Timeout Configurable

SafeNet ProtectServer/ProtectToolkit now supports changing the environment variable ET_HSM_PCICLIENT_READ_TIMEOUT_SECS, which determines the time (in seconds) the PCIe driver will wait before timing out on a read operation. It should be set long enough to avoid an unintentional timeout, shutting down the HSM.

Advisory Notes

HA/WLD Limitations

While SafeNet ProtectToolkit is designed to be backwards-compatible with older ProtectServer HSMs, capabilities vary between firmware versions, and these differences may cause issues. Newer firmware uses more cryptographic mechanisms, so calls to **C_GetMechanismList** will return different data lengths than with older firmware. Should an HA/WLD handover occur between obtaining the required length of a buffer and reading data into it, a “buffer too small” error may occur. To avoid this, query each HSM in the cluster to establish the correct size for the mechanism list buffer. Calls to the **C_GetMechanismList** function should be handled on a slot-by-slot basis.

GCC Tree-Vectorize Error

In some cases, a bug in the GCC 4.6.x optimizer (the version used for SafeNet ProtectServer/ProtectToolkit 5.x 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 SafeNet ProtectServer 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 SafeNet ProtectServer HSM enters a non-useful or non-responsive state that does not resolve itself after a system reboot, try “tampering” the card. For the SafeNet ProtectServer PCIe HSM, remove the card from the computer for a few minutes and then re-insert it. For the SafeNet ProtectServer Network HSM, use the tamper key located on the rear of the appliance. If the HSM does not return to normal operation, contact Customer Support.

FIPS Mode Operational Restrictions

New operational restrictions have been put in place to reflect changes in FIPS requirements. In FIPS mode, operations of certain cryptographic algorithms are restricted to keys with a minimum modulus. Any attempt to use or create a key smaller than the specified minimum will result in a CKR_KEY_SIZE_RANGE error. The minimum key size for verify operations may be smaller, to verify legacy keys created in earlier versions of FIPS mode. The key sizes are restricted as follows:

- **RSA**: must be 2048, 3072, or 4096 bits (verify - 1024 or 1536 bits)
- **DSA**: must be 2048, 3072, or 4096 bits (verify - 1024 or 1536 bits)
- **EC**: must be 224 bits at minimum (verify - 160 bits)

End-User License Agreement

The EULA for this release (**008-010005-001_EULA_HSM_SW_revK**) is provided at the top level of the SafeNet ProtectServer/ProtectToolkit 5.3 Client package. This revision supersedes any earlier versions of the EULA.

Compatibility and Upgrade Information

Supported Platforms

The supported platforms are listed in the following table.

C=SafeNet ProtectServer/ProtectToolkit-C, PKCS #11 v2.10/2.20

M=SafeNet ProtectServer/ProtectToolkit-M, MS CSP 2.0 with CNG

J=SafeNet ProtectServer/ProtectToolkit-J, Java runtime 6.x/7.x/8.x

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	Network HSM, PSE
	Server 2012 R2	64-bit	C/M/J	All platforms	C/J	Network HSM, PSE
	7	32-bit	-	-	C/J (KSP supported)	All platforms
	7	64-bit	C/M/J	All platforms	C/J	Network HSM, 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	Network HSM, PSE
	RHEL 7	64-bit	C/J	All except PSI-E (K5)	C/J	Network HSM, PSE
	SUSE12	64-bit	C/J	All except PSI-E (K5)	C/J	Network HSM, PSE
AIX	6.1	64-bit	C/J	Network HSM, PSE	C/J	Network HSM, PSE
	7.1	64-bit	C/J	Network HSM, PSE	C/J	Network HSM, PSE
	7.2	64-bit	C/J	Network HSM, PSE	C/J	Network HSM, PSE
Solaris	10 (SPARC, x86) 11 (SPARC, x86)	64-bit	C/J	Network HSM, PSE	C/J	Network HSM, PSE
HP-UX	11	64-bit	C/J	Network HSM, PSE	C/J	Network HSM, PSE

Supported Firmware

Firmware Version	Available Platforms	FIPS Level 3 Certified
5.00.02	Network HSM, PCIe HSM	Yes
5.00.04	Network HSM, PCIe HSM	No
5.00.05	Network HSM, PCIe HSM	No
5.00.06	Network HSM, PCIe HSM	No
3.20.05	PSE, PSI-E	Yes
3.20.09	PSE, PSI-E	Yes
3.20.10	PSE, PSI-E	Yes

Note: The SafeNet ProtectServer Network HSM and SafeNet ProtectServer PCIe HSM ship with firmware 5.00.04. If you require FIPS certification, you can download and install firmware 5.00.02.

FIPS Status

Refer to the following documents or contact Gemalto Support for the current FIPS validation status:

- Modules Under Test: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140IUT.pdf
- 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 5.00.06

Support has been added for the new PKCS#11 mechanism: `CKM_AES_ECB_ENCRYPT_DATA`

Required Third-Party Software

You must install the following third-party software before installing SafeNet ProtectServer/ProtectToolkit 5.3:

Operating system	Required third-party software
Windows	• Java Runtime Environment (JRE) 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, HP-UX	• Java Runtime Environment (JRE) 6.x, 7.x, or 8.x
Solaris	• Java Runtime Environment (JRE) 6.x or 7.x

Supported Server Hardware

The SafeNet ProtectServer PCIe HSM card is designed to the PCIe 1.1 standard, for use in servers with PCIe x4 slots. You can also install the SafeNet ProtectServer PCIe 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 SafeNet ProtectServer PCIe 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 SafeNet ProtectServer PCIe card 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 and Addressed Issues

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

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.

Known Issues

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

Issue	Severity	Synopsis
PSR-1939	M	**Problem**: When deleting an FM from the HSM using **ctfm -d**, the HSM goes into a halted state. **Workaround**: Run **hsmreset** to return HSM from halted state.
PSR-1913	L	**Problem**: When SafeNet ProtectServer/ProtectToolkit-C Runtime is installed on Unix systems, **setvars.sh** cannot be sourced to configure environment variables as specified in the documentation. **Workaround**: Install SafeNet ProtectServer/ProtectToolkit-C SDK to use **setvars.sh** as specified. If environment configuration is unnecessary, **setvars.sh** can be safely ignored or deleted.

Addressed Issues

The following table lists the issues addressed in this release.

Issue	Severity	Synopsis
PSR-1937	H	**Problem**: When creating keys using a PIN pad, the HSM crashes. **Resolution**: Fixed in firmware 5.00.06.
PSR-1772	H	**Problem**: Backup on smart cards with MofN and Increased Security Level fails with "Template Inconsistent" error. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3.
PSR-1755	H	**Problem**: When registering Cryptoki library with KSP, a "Failed to verify the signature for the chosen library" error is returned. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3.
PSR-1737	H	**Problem**: Linux driver issue causes SafeNet ProtectServer Network HSM to go into a halted state. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3 and firmware 5.00.06.
PSR-1794	M	**Problem**: Serial port does not allow login access. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3.
PSR-1753	M	**Problem**: Generating certificate with **ctcert** in FIPS mode results in "Mechanism Invalid" error due to default SHA1 Signing Operation mechanism. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3.
PSR-1712	M	**Problem**: When creating keys with **C_CreateObject**, the CKA_ALWAYS_SENSITIVE attribute is set to TRUE. **Resolution**: Fixed in firmware 5.00.06.
PSR-1169	M	**Problem**: During MofN backup via USB, user is erroneously prompted twice to insert the next smart card. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3.
PSR-357	M	**Problem**: CKM_ECDH1_DERIVE mechanism is defined incorrectly in Cryptoki.

Issue	Severity	Synopsis
		Resolution: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3 and firmware 5.00.06.
PSR-1796	L	**Problem**: When using JProv with a combination of legacy PSE and current SafeNet ProtectServer Network HSMs in WLD/HA mode, a "buffer too small" error is sometimes returned. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3 and firmware 5.00.06.
PSR-1726	L	**Problem**: On Windows, **jcprov** API documentation placed in the wrong directory, causing broken documentation links. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3. Documents are placed in the directory "C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\jcprov_api\safenet\jcprov".
PSR-1114	L	**Problem**: Operating two or more HSMs with an AIX machine produces noticeable lag after commands. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3.
PSR-773	L	**Problem**: ET_HSM_NETCLIENT_CONNECT_TIMEOUT_SECS parameter not working as expected; timeout occurs after 21 seconds regardless of specified or default timeout. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3.
PSR-591	L	**Problem**: SafeNet ProtectServer/ProtectToolkit-M **createcert.exe** utility crashes after execution. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3.
PSR-584	L	**Problem**: Inactive menu buttons in SafeNet ProtectServer/ProtectToolkit-M's **gmadmin** utility. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3.
PSR-582	L	**Problem**: GUI issue - "Keyset password" label not fully visible in SafeNet ProtectServer/ProtectToolkit-M's **gmadmin** utility. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3.
PSR-381	L	**Problem**: When setting the serial number of a certificate made with CKM_ENCODE_X_509, the value is not set if passed using SERIAL_NUMBER. **Resolution**: Fixed in SafeNet ProtectServer/ProtectToolkit 5.3.

Support Contacts

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

Contact method	Contact	
Address	Gemalto 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 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.	

