SafeNet ProtectServer/ProtectToolkit 5.6

CUSTOMER RELEASE NOTES

Issue Date: 09 December 2019

Document Part Number: 007-007171-017 Rev. G

The most up-to-date version of this document is posted to the Technical Support Customer Portal at https://supportportal.thalesgroup.com.

Contents

Product Description

SafeNet ProtectToolkit is Thales's PKCS #11 V 2.20-compliant API product, designed to work with the SafeNet ProtectServer line of hardware security modules (HSMs).

SafeNet ProtectServer Hardware

SafeNet ProtectToolkit supports the following hardware platforms:

- SafeNet ProtectServer Network HSM – intelligent cryptographic adapter (external network appliance engine).
- SafeNet ProtectServer Network HSM Plus – intelligent cryptographic adapter (upgraded external network appliance engine).
- SafeNet ProtectServer PCIe HSM – intelligent cryptographic adapter (PCIe bus).

Although the SafeNet ProtectServer Network HSM, Network HSM Plus, and PCIe HSM are functionally equivalent to their legacy counterparts, the embedded cryptographic engine used on the HSMs has been upgraded:

- The legacy PSE and PSI-E HSMs contain the K5 cryptographic engine.
- The new SafeNet ProtectServer Network HSM, Network HSM Plus, and PCIe HSM contain the upgraded K6 cryptographic engine.

SafeNet ProtectToolkit Software

The SafeNet ProtectToolkit software includes the following components:

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

Release Description

SafeNet ProtectToolkit 5.6 extends the functionality and utility of SafeNet ProtectServer HSMs. SafeNet ProtectToolkit 5.6 is compatible with SafeNet ProtectServer Network HSM, Network HSM Plus, and PCIe HSM.

Upgraded CPU in SafeNet ProtectServer Network HSM

As part of our policy of continuous improvement, new SafeNet ProtectServer Network HSMs contain an upgraded Intel® Atom™ CPU E3827 1.74 GHz processor. These models have appliance software version 5.4 and HSM firmware 5.02.00 installed at the factory, and ship with SafeNet ProtectToolkit 5.5. You can download the latest software from the Customer Support Portal. If you require FIPS-validated firmware immediately, download and install firmware version 5.03.02.

New Features and Enhancements

Release 5.6 provides the following new features and enhancements:

Appliance Software Version Updates

Thales now provides secure package files that allow you to update the appliance software image on any SafeNet ProtectServer Network HSM or Network HSM Plus that includes PSESH. You can download the following update packages from the Thales Customer Support Portal:

- Secure Update Package Patch (**SPKG-0.1-1.i386.rpm**). This patch adds a new PSESH command, **package install**. In the future, this command will be used to apply software updates and any other secure patches released for ProtectServer Network HSMs.
- Secure package containing the latest appliance software image

For detailed instructions for applying the update, refer to the latest version of the SafeNet ProtectToolkit documentation (5.8 or above):

- *Network HSM Installation and Configuration Guide* **>** *Updating the Appliance Software Image*
- *Network HSM Plus Installation and Configuration Guide* **>** *Updating the Appliance Software Image*

Support for SHA3 Hash Algorithms

SafeNet ProtectToolkit 5.6 provides new mechanisms that use the SHA3 standard, as described by NIST in FIPS PUB 202. See "New Mechanisms in Firmware 5.03.00" below for a list of new mechanisms, which can be used interchangeably with their SHA2 counterparts.

Support for PKCS#11 v.2.30-Compliant AES-GCM

SafeNet ProtectToolkit 5.6 supports the Galois/Counter Mode (GCM) option with AES, in compliance with NIST SP 800-38D (see "New Mechanisms in Firmware 5.03.00" below). Refer to product documentation and *PKCS#11 version 2.30 Draft 7* for a description of the AES_GCM mechanism.

PSESH Admin Account Recovery

As a security measure, the **admin** account is locked out after 10 consecutive failed console login attempts. New ProtectServer Network HSMs that are shipped with appliance image 5.6 and above will allow the **admin** user to recover the account, without assistance from Thales, by zeroizing the HSM. The **admin** user can also reset passwords for the **audit** as well as the **pseoperator** user. Consult the product documentation for these procedures.

Updates to OpenSSL and OpenSSH

SafeNet ProtectToolkit 5.6 contains security updates to OpenSSL and OpenSSH.

Kernel Updates Addressing Spectre/Meltdown Vulnerabilities

The SafeNet ProtectServer Network HSM and SafeNet ProtectServer Network HSM Plus appliance kernels have been updated to address the Spectre and Meltdown vulnerabilities in Intel® processors.

New Mechanisms in Firmware 5.03.00

Firmware 5.03.00 provides bug fixes as outlined in "Addressed Issues" on page 12. This firmware supports the latest features from release 5.6. The following new mechanisms are available in firmware 5.03.00:

- CKM_AES_GCM
- SHA3 Signing mechanisms:

- CKM_SHA3_224_RSA_PKCS
- CKM_SHA3_256_RSA_PKCS
- CKM_SHA3_384_RSA_PKCS
- CKM_SHA3_512_RSA_PKCS
- CKM_SHA3_224_RSA_PKCS_PSS
- CKM_SHA3_256_RSA_PKCS_PSS
- CKM_SHA3_384_RSA_PKCS_PSS
- CKM_SHA3_512_RSA_PKCS_PSS
- CKM_ECDSA_SHA3_224
- CKM_ECDSA_SHA3_256
- CKM_ECDSA_SHA3_384
- CKM_ECDSA_SHA3_512

> SHA3 Hashing mechanisms:

- CKM_SHA3_224
- CKM_SHA3_256
- CKM_SHA3_384
- CKM_SHA3_512

> SHA3 HMAC mechanisms:

- CKM_SHA3_224_HMAC
- CKM_SHA3_224_HMAC_GENERAL
- CKM_SHA3_256_HMAC
- CKM_SHA3_256_HMAC_GENERAL
- CKM_SHA3_384_HMAC
- CKM_SHA3_384_HMAC_GENERAL
- CKM_SHA3_512_HMAC
- CKM_SHA3_512_HMAC_GENERAL

> SHA3 Key derivation mechanisms:

- CKM_SHA3_224_KEY_DERIVE
- CKM_SHA3_256_KEY_DERIVE
- CKM_SHA3_384_KEY_DERIVE
- CKM_SHA3_512_KEY_DERIVE

FIPS Restrictions in Release 5.6

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.

In this release, the following new restrictions apply when FIPS Mode is active:

- When using DES3 keys for encryption/wrapping, a maximum of 2^{28} 64-bit packets can be processed by a single key. When this limit is reached, an error occurs (CKR_KEY_NOT_ACTIVE).
- The following mechanisms cannot be used for MAC generation:
  - CKM_DES3_MAC
  - CKM_DES3_MAC_GENERAL
  - CKM_DES3_X919_MAC
  - CKM_DES3_X919_MAC_GENERAL
  - CKM_DES3_RETAIL_CFB_MAC

New Firmware 5.03.01 Contains Vulnerability and Bug Fixes

Firmware 5.03.01 includes the features and restrictions listed for 5.03.00 above, as well as new cryptographic restrictions in accordance with NIST's updates to SP 800-56A and SP 800-56C. Firmware 5.03.01 contains bug and vulnerability fixes, and is a candidate for FIPS certification.

New Firmware 5.03.02 Contains Bug Fixes

Firmware 5.03.02 includes the features and FIPS restrictions listed for 5.03 00 and 5.03.01 above, and also the latest bug fixes (see "Addressed Issues" on page 12). This is the latest candidate firmware for FIPS certification.

Thales IDPrime Smart Card

Firmware 5.03.01 also adds support for the Thales IDPrime smart card. The new smart card provides the same functions as the previous version.

Advisory Notes

Previously Released Versions of Windows Installer Trigger Anti-Virus Software

Windows installer binaries in SafeNet ProtectToolkit 5.4 and earlier are being flagged as malware by anti-virus software. These versions are still usable, but they may conflict with your anti-virus software.

Firmware 5.01.xx and Newer Not Compatible with Older Client Software

Firmware version 5.01.xx is not compatible with client software older than release 5.4. If you are using firmware older than 5.01.xx, upgrade your client software to 5.6 *before* you upgrade the HSM firmware.

> **NOTE** Please refer to Technical Note KB0016370 for more information on this issue.

FMs Compiled With FMSDK 5.4 and Newer Not Compatible With Older Firmware

FMs compiled using FMSDK 5.4 or newer will not load correctly on an HSM with firmware 5.00.xx. If an HSM with a newer FM and firmware 5.01.xx is downgraded to firmware 5.00.xx, the FM will be deleted. To avoid this, use FMSDK 5.3 to compile FMs intended for use with firmware 5.00.xx.

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 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 Thales Technical Support (see "Support Contacts" on page 15).

Loading an FM Causes Halt and Reset

When you load an FM, the HSM is automatically halted and reset. The halt/reset is reported as an error in the event logs and in **/var/log/messages**. This error can be safely ignored.

Legacy PSI-E HSMs

PSI-E with SafeNet ProtectToolkit 5.6 supports all the same functionality as the SafeNet ProtectServer PCIe HSM with SafeNet ProtectToolkit 5.6, 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.

Compatibility and Upgrade Information

Supported Platforms

The supported platforms are listed in the following table.

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

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

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

> **NOTE** Do not upgrade to SafeNet ProtectToolkit 5.6 if you are using the legacy PSG HSM.

Operating System		OS type	64-bit PTK	64-bit PTK supported hardware	32-bit PTK	32-bit PTK supported hardware
Windows	Server 2016	64-bit	C/M/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	Server 2012 R2	64-bit	C/M/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	Server 2008 (R1 and R2)	64-bit	C/M/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	7	32-bit	-	-	C/J (KSP support)	PCIe HSM Network HSM Network HSM Plus
	7	64-bit	C/M/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus

Operating System		OS type	64-bit PTK	64-bit PTK supported hardware	32-bit PTK	32-bit PTK supported hardware
Linux	RHEL 7	64-bit	C/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	RHEL 6	32-bit	-	-	C/J	PCIe HSM Network HSM Network HSM Plus
	RHEL 6	64-bit	C/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	SUSE12	64-bit	C/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
AIX	7.2	64-bit	C/J	Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	7.1	64-bit	C/J	Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	6.1	64-bit	C/J	Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
Solaris	11 (SPARC, x86) 10 (SPARC, x86)	64-bit	C/J	Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
HP-UX	11	64-bit	C/J	Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus

Supported Firmware

Firmware Version	Available Platforms	FIPS Level 3 Certified
5.03.02	Network HSM, Network HSM Plus, PCIe HSM	Yes
5.03.01	Network HSM, Network HSM Plus, PCIe HSM	Yes
5.03.00	Network HSM, Network HSM Plus, PCIe HSM	No
5.02.00	Network HSM, Network HSM Plus, PCIe HSM	No
5.01.03	Network HSM, Network HSM Plus, PCIe HSM	Yes

Firmware Version	Available Platforms	FIPS Level 3 Certified
5.01.02	Network HSM, Network HSM Plus, PCIe HSM	Yes
5.01.01	Network HSM, Network HSM Plus, PCIe HSM	No
5.01.00	Network HSM, Network HSM Plus, PCIe HSM	No
5.00.08	Network HSM, Network HSM Plus, PCIe HSM	No
5.00.06	Network HSM, PCIe HSM	No
5.00.05	Network HSM, PCIe HSM	No
5.00.04	Network HSM, PCIe HSM	No
5.00.02	Network HSM, PCIe HSM	Yes

> **NOTE** The SafeNet ProtectServer Network HSM, Network HSM Plus, and PCIe HSM ship with firmware version 5.02.00. If you require FIPS certification immediately, you can download and install firmware 5.03.02.

FIPS Status

The latest FIPS-certified firmware version is 5.03.02. Refer to the following documents or contact Thales 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

Required Third-Party Software

You must install the following third-party software before installing SafeNet ProtectToolkit 5.6:

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, and those that have been fixed for this 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-2284	M	**Problem**: On HP-UX, the sample C program binaries provided in the PTK-C SDK fail to execute. **Workaround**: Add **-lpthread** as an extra function call in the make file. For example: `cc -L/opt/safenet/protecttoolkit5/ptk//lib -o createslots CreateSlots.o -lctutil -lctextra -lutil -lcryptoki -lpthread`

Issue	Severity	Synopsis

PSR-2211	L	**Problem**: The FM-SDK automated cross-compiler build script fails on Windows operating systems.
		Workaround: In **crossc.cmd**, edit the line:
		`mingw-get install mingw32-base "mingw32-gcc-g++<6" mingw-developer-toolkit mpc-dev mpfr-dev "gmp-dev<6"`
		by breaking it down into the following two lines:
		`mingw-get install mingw32-base mingw-developer-toolkit mpc-dev mpfr-dev`
		`mingw-get install "mingw32-gcc-g++<6" "gmp-dev<6"`

PSR-2119	L	**Problem**: The serial port on SafeNet ProtectServer Network HSM or SafeNet ProtectServer Network HSM Plus becomes unresponsive. **Workaround**: Disconnect and reconnect the provided DB9-to-USB-cable and start a new serial session.
PSR-2046	L	**Problem**: When using PTK-J, stopping an application using **Ctrl-C** causes the HSM to crash. Log reports a "Segmentation Fault". **Workaround**: None.

Addressed Issues

The following table lists the issues addressed in this release.

Issue	Severity	Synopsis
PSR-2929	H	**Problem:** FMSC_SendReceive fails with a general error (PKCS#11 Failure 0x80000384) when security modes **No Clear PINs** or **Full Secure Messaging Encryption** are enabled and the responselen is longer than 3510 bytes. **Resolution:** Fixed in firmware 5.03.02.
PSR-2896	H	**Problem:** HSM halts when **auditverify** is running in parallel with other PKCS#11 applications. **Resolution:** Fixed in firmware 5.03.02.
PSR-2214	M	**Problem**: When creating child keys with more than one level of depth, the parent fingerprint is set to the child's fingerprint. **Resolution**: Fixed in SafeNet ProtectToolkit 5.6.
PSR-2224	L	**Problem**: The HA logs prints an incorrect timestamp (wrong month) on log entries. **Resolution**: Fixed in SafeNet ProtectToolkit 5.6.
PSR-2194	L	**Problem**: If you enter the incorrect original PIN when changing the PIN on a Siemens smart card, an incorrect error message results ("**Device Error**"). **Resolution**: Fixed in SafeNet ProtectToolkit 5.6.

Issue	Severity	Synopsis
PSR-2128	L	**Problem**: In FIPS Mode, creating a keyset in **gmadmin** fails with an error (MMR_ ARGUMENTS_BAD). **Resolution**: Fixed in SafeNet ProtectToolkit 5.6.
PSR-1801	L	**Problem**: The output from **ctfm q** sometimes displays an incorrect build date for FMs. **Resolution**: Fixed in SafeNet ProtectToolkit 5.6.

Revision History

Revision A: 18 April 2018

> Initial Release

Revision B: 31 July 2018

> Added to "Supported Firmware" on page 9:
- Firmware 5.01.02 -- FIPS Level 3 Certified

Revision C: 04 September 2018

> Added to **New Features and Enhancements**:
- "New Firmware 5.03.01 Contains Vulnerability and Bug Fixes" on page 6
- "Thales IDPrime Smart Card" on page 6

> Added to **Supported Firmware**:
- Firmware 5.01.03

Revision D: 15 November 2018

> Additional clarifications regarding firmware 5.03.01

Revision E: 12 February 2019

> Added to **New Features and Enhancements**:
- "New Firmware 5.03.02 Contains Bug Fixes" on page 6

> Added to **Supported Firmware**:
- Firmware 5.03.02

> Added to **Addressed Issues**:
- PSR-2929
- PSR-2896

Revision F: 29 March 2019

> Added to **New Features and Enhancements**:

- "Appliance Software Version Updates" on page 4

> Added to **Advisory Notes**:

- "Loading an FM Causes Halt and Reset" on page 7

Revision G: 09 December 2019

> Added to "Supported Firmware" on page 9:

- Firmware 5.03.02 -- FIPS Level 3 Certified
- Firmware 5.03.01 -- FIPS Level 3 Certified
- Firmware 5.01.03 -- FIPS Level 3 Certified

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer 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 Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone

The support portal also lists telephone numbers for voice contact (Contact Us).