SafeNet ProtectServer/ProtectToolkit 5.7

CUSTOMER RELEASE NOTES

Issue Date: 09 December 2019

Document Part Number: 007-007171-018 Rev. C

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).

  As part of our policy of continuous improvement, new SafeNet ProtectServer Network HSMs contain an upgraded Intel® Atom™ CPU E3827 1.74 GHz processor.
- SafeNet ProtectServer Network HSM Plus – intelligent cryptographic adapter (upgraded external network appliance engine).
- SafeNet ProtectServer PCIe HSM – intelligent cryptographic adapter (PCIe bus).

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 5.7 extends the functionality and utility of SafeNet ProtectServer HSMs. SafeNet ProtectToolkit 5.7 is compatible with SafeNet ProtectServer Network HSM, Network HSM Plus, and PCIe HSM.

With this release, SafeNet ProtectServer HSMs are shipped from factory with the following installed:

- appliance software image 5.7.0 (Network HSM and Network HSM Plus)
- HSM firmware 5.04.00

You can download SafeNet ProtectToolkit 5.7, and all the latest software and firmware releases, from the Thales Customer Support Portal (see "Support Contacts" on page 11). If you require FIPS-validated firmware, download and install firmware version 5.03.02.

New Features and Enhancements

Release 5.7 provides the following new features and enhancements:

Multifactor Authentication (One-Time Password)

SafeNet ProtectToolkit 5.7 now supports multifactor authentication using the SafeNet 110 OTP Token. This authentication scheme adds another layer of security by requiring both the memorized token PIN and a 6-digit number randomly generated by the SafeNet 110 OTP Token.

USB API Support for FMs

On Linux clients, you can now use the USB API to write applications that can interact with the HSM via the card USB port. This functionality can include:

- wrapping of PKCS objects and storing them on a USB flash memory drive
- backup of SMFS stored key (non-PKCS keys)

The USB API works with your custom FM to enable the desired functionality.

Secure Package Updates

On SafeNet ProtectServer Network HSM and Network HSM Plus shipped with SafeNet ProtectToolkit 5.7, you can now update the appliance software image by applying a secure package provided by Thales.

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*

Ed25519 Curve Support

The **ed25519** curve has been added to SafeNet ProtectToolkit 5.7 for sign/verify operations. **Ed25519** uses a new key type, `CKK_EC_EDWARDS`, and the set of new EDDSA sign/verify mechanisms.

AES CCM Support

SafeNet ProtectToolkit 5.7 introduces the AES_CCM mechanism, described at https://tools.ietf.org/html/rfc3610.

OpenSSL Library Supporting Big Numbers Included in FM-SDK

The FM-SDK now includes a pre-compiled OpenSSL library (**libfmbn**), which allows support for Big Numbers in FMs. Use the FM sample **ssldemo** as a reference to use this library with your FMs. OpenSSL documentation can be found at https://www.openssl.org/.

New in Firmware 5.04.00

Firmware 5.04.00 provides bug fixes as outlined in "Addressed Issues" on page 10. This firmware supports the latest features from release 5.7. The following new mechanisms are available in firmware 5.04.00:

- CKM_AES_CCM
- CKM_EC_EDWARDS_KEY_PAIR_GEN
- CKM_EDDSA
- CKM_SHA1_EDDSA
- CKM_SHA3_256_EDDSA
- CKM_SHA3_384_EDDSA
- CKM_SHA3_512_EDDSA
- CKM_SHA224_EDDSA
- CKM_SHA256_EDDSA

- CKM_SHA384_EDDSA
- CKM_SHA512_EDDSA

Advisory Notes

FMs Compiled With FMSDK 5.7 and Newer Not Compatible With Older Firmware

FMs compiled using FMSDK/CProv 5.7 or newer are not compatible with HSM firmware 5.03.xx or older. The FM will fail to load, producing an error (`Could not verify Functionality Module`, logs record `0x0100 incompatible library version`).

If an FM is intended to run on a ProtectServer HSM with firmware 5.04.xx or newer, use FMSDK 5.7 or above to build the FM. If the FM is intended for use with firmware 5.03.xx or older, use FMSDK 5.6 or the version that corresponds with the firmware release.

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 newer than 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 PTK client software to 5.7 *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 Customer Support (see "Support Contacts" on page 11).

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.

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 5.7 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
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

Operating System		OS type	64-bit PTK	64-bit PTK supported hardware	32-bit PTK	32-bit PTK supported hardware
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
5.04.00	Network HSM, Network HSM Plus, PCIe HSM	No
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
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 5.04.00. 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 Customer 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 5.7:

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.

Severity Classification	Definition
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-2700	M	**Problem:** The USB API does not support hybrid USB devices that use the USB 2.0, 3.0, and 3.1 standards. **Workaround:** Use USB 2.0 devices only.
PSR-2751	L	**Problem:** Applications using the USB API are not able to write files larger than 1 MB to the USB memory drive. **Workaround:** None.
PSR-2724	L	**Problem:** On Solaris 10, HP-UX, AIX, and Linux 64-bit operating systems, the C sample **limits.c** fails to compile. **Workaround:** None.
PSR-2677	L	**Problem**: Three failed login attempts using an OTP PIN less than 10 digits long (<4 digits: token PIN, 6 digits: OTP PIN) does not lock further login attempts for 5 seconds as it should. **Workaround**: Set a token PIN at least 4 digits long.
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-2721	H	**Problem**: When generating a BIP32 key pair, the CKA_BIP32_ID field (public key hash) was not set. **Resolved**: Fixed in release 5.7.
PSR-2284	M	**Problem**: On HP-UX, the sample C program binaries provided in the PTK-C SDK failed to execute. **Resolved**: Fixed in release 5.7.

Issue	Severity	Synopsis
PSR-2272	L	**Problem**: The **ctbrowse** tool crashed when using the AES_GCM mechanism for an encrypt operation. **Resolved**: Fixed in release 5.7.
PSR-2211	L	**Problem**: The FM-SDK automated cross-compiler build script failed on Windows operating systems. **Resolved**: Fixed in release 5.7.

Revision History

Revision A: 26 November 2018

> Initial Release

Revision B: 29 March 2019

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

- Information on applying "Secure Package Updates" on page 4

> Added to **Advisory Notes**:

- "FMs Compiled With FMSDK 5.7 and Newer Not Compatible With Older Firmware" on page 5
- "Loading an FM Causes Halt and Reset" on page 6

Revision C: 09 December 2019

> Added to "Supported Firmware" on page 8:

- 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).