Thales ProtectServer/ProtectToolkit 5.9

CUSTOMER RELEASE NOTES

Issue Date: 07 April 2021

Document Part Number: 007-007171-021 Rev. E

The most up-to-date version of this document is posted to the Thales Documentation Hub at https://www.thalesdocs.com/.

Contents

Product Description

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

ProtectServer Hardware

ProtectToolkit supports the following hardware platforms:

- ProtectServer Network HSM - intelligent cryptographic adapter (external network appliance engine).

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

ProtectToolkit Software

The ProtectToolkit software includes the following components:

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

Release Description

ProtectToolkit 5.9 extends the functionality and utility of ProtectServer HSMs. ProtectToolkit 5.9 is compatible with ProtectServer Network HSM, Network HSM Plus, and PCIe HSM.

You can download ProtectToolkit 5.9, and the latest appliance software and firmware releases, from the Thales Group 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 5.9 provides the following new features and enhancements:

CTMULTITOKEN

ProtectToolkit 5.9 includes **ctmultitoken**, a multi-threaded performance testing tool (which will eventually replace the single-threaded CTPerf tool) that allows you to perform basic cryptographic functions on a ProtectServer HSM. Designed as a testing tool for HSM operations and performance, **ctmultitoken** allows you to specify one or more tokens on which to perform or repeat an operation, and returns a summary of the results.

Key Creation From Multiple Components Using PIN Pad Allowed in FIPS Mode

A new mechanism, CKM_PP_LOAD_SECRET_2, allows you to import keys from multiple components using the ProtectServer PIN pad accessory without requiring the **Weak PKCS#11 Mechanisms** flag to be set. These operations are now supported in FIPS mode.

MIBs for SNMP Logging Enhancements

ProtectToolkit 5.9 includes Management Information Base files (MIBs) that enable you to retrieve information about the ProtectServer Network HSM via SNMP.

New TUAK and KECCAK Mechanisms

ProtectToolkit 5.9 includes new mechanisms for using the TUAK and KECCAK cryptographic algorithms, used for 5G mobile ethernet systems.

New PSESH Commands Display HSM Information and Allow Audit Log Cleanup

New PSESH commands allow the following functions:

- **audit log clear**: allows the **audit** user to delete all current audit logs on the HSM.
- **syslog cleanup**: allows the **admin** user to create a .tar archive of all audit logs currently on the HSM, and delete them.
- **hsm show** displays information about the appliance image/HSM firmware versions, slot information, and admin token information.

New in Firmware 5.06.00

Firmware 5.06.00 supports the latest features from release 5.9, bug fixes as described in "Addressed Issues" on page 10, and recent changes to FIPS restrictions.

Firmware 5.06.01 Latest Candidate for FIPS Certification

New ProtectServer firmware 5.06.01 is the latest candidate for FIPS certification.

Advisory Notes

Support Ended For Some Authentication Features

Firmware 5.06.00 removes support for the following features:

- Auth challenge response (**CT_Gen_AUTH_Response** and **CT_GetAuthChallenge**)
- Temporary PINs (**CT_GetTmpPin**)

Support Ended For Legacy Serial Smart Card Readers

Firmware 5.06.00 removes support for the following legacy serial smart card readers:

- OMNI 3111
- GCR410
- PE122

> DUMB

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.

Uninstall Previous PTK Client Software on Windows 10 Systems

If you previously installed the ProtectServer PCIe Access Provider software on a host workstation running Windows 10, uninstall any previous client software and the driver. You must also manually delete all LunaK4-related files in the **C:\Windows** directory before installing PTK 5.8.

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 5.9 *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 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 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 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 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 ProtectServer PCIe HSM, remove the card from the computer for a few minutes and then re-insert it. For the 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 Group 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=ProtectToolkit-C, PKCS #11 v2.10/2.20

M=ProtectToolkit-M, MS CSP 2.0 with CNG

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

> **NOTE** Do not upgrade to ProtectToolkit 5.9 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	10	64-bit	C/M/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	Server 2019	64-bit	C/M/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	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

Operating System		OS type	64-bit PTK	64-bit PTK supported hardware	32-bit PTK	32-bit PTK supported hardware
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
5.06.01	Network HSM, Network HSM Plus, PCIe HSM	Pending
5.06.00	Network HSM, Network HSM Plus, PCIe HSM	No
5.05.00	Network HSM, Network HSM Plus, PCIe HSM	No
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

Firmware Version	Available Platforms	FIPS Level 3 Certified
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 ProtectServer Network HSM, Network HSM Plus, and PCIe HSM ship with firmware version 5.04.00. Download and install firmware 5.06.00 to use all the latest features. If you require FIPS certification, 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 ProtectToolkit 5.9:

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, Solaris	> Java Runtime Environment (JRE) 6.x, 7.x, or 8.x

NOTE The older (minor) versions of Java 7 or Java 8 could cause issues with the SAFENET java library (**jprov_sfnt.jar**). Thales Group recommends updating Java 7/8 to the latest version.

Supported Server Hardware

The 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 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 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 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-5010	M	**Problem:** When running psesh:> **sysconf appliance factory**, the network configuration (hostname and IP address) are not reset. **Workaround:** Run the following commands to complete the factory reset procedure: > psesh:>**network interface delete** to delete the IP address. > psesh:>**network hostname** <hostname> to set a new host name for the appliance.
PSR-3414	M	**Problem:** When a new PCI driver is installed on Windows using the **PTKpcihsmK6.msi** package, the driver file (**LunaK4.sys**) is not updated automatically. **Workaround:** Use the following procedure to allow the Device Manager to recognize the new driver: 1. Disable the Luna PCI device in the Device Manager. 2. Copy **LunaK4.sys** manually from the installation directory to **System32/drivers**. 3. Enable the Luna PCI device in the Device Manager.
PSR-3219	M	**Problem:** Pressing **Cancel** on the legacy Verifone 1000SE PIN pad halts the HSM. **Workaround:** Do not press **Cancel** when entering keys. Upgrade to a newer PIN pad.

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-3368	L	**Problem:** While installing the PCI access provider, driver insert code is displayed on the console.
		`if ! ( insmod $VKDLONG vip_comm_mode=$VIP_COMM_MODE ignore_k6_pci_ext=1 2>&1 ) ; then`
		`Starting vkd (via systemctl):`
		Workaround: This can be safely ignored.

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-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-3011	L	**Problem:** When using software-only mode on 64-bit AIX and HP-UX operating systems, token initialization fails. **Resolved:** Fixed in PTK 5.9.
PSR-3007	L	**Problem:** DSA key generation fails for 4096-bit keys. DSA parameter (`dsa_param`) key generation fails for 2048, 3072, and 4096-bit keys. **Resolved:** Fixed in PTK 5.9.

Revision History

Revision A: 09 December 2019

> Initial Release

Revision B: 20 February 2020

> Correction in "New Features and Enhancements" on page 2: Key creation from multiple components in FIPS mode is supported using the ProtectServer PIN pad accessory only.

Revision C: 21 September 2020

> Correction in "Supported Platforms" on page 5: Added Windows Server 2019 to the list of supported client platforms.

Revision D: 03 November 2020

> Added to "Supported Firmware" on page 7: New ProtectServer firmware 5.06.01 is the latest candidate for FIPS certification.

Revision E: 07 April 2021

> Added to "Known Issues" on page 9: PSR-5010 is a known issue in PTK 5.9.

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).