SafeNet ProtectServer/ProtectToolkit 5.2

CUSTOMER RELEASE NOTES

Issue Date: 09 December 2019

Document Part Number: 007-007171-011 Rev. M

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 3
- SafeNet ProtectToolkit Software 3

Release Description 3
- Support for Legacy PSI-E HSMs 3

New Features and Enhancements 4
- PSESH Command Shell on the SafeNet ProtectServer Network HSM 4
- Appliance Software Version Updates 4
- New USB Card Reader 4
- IPv6 Addressing Support on the SafeNet ProtectServer Network HSM 4
- Support for HP-UX 5
- Support 131-A transition (Deprecate DES2 keys) 5

Advisory Notes 5
- HA/WLD Limitations 5
- GCC Tree-Vectorize Error 5
- Run ctconf -t on First Install of HSM 5
- Use Tamper to Recover From an Unresponsive State 5
- Loading an FM Causes Halt and Reset 5

Compatibility and Upgrade Information 6
- Supported Platforms 6
- Supported Firmware 6
- FIPS Status 7
- New in Firmware 5.00.05 7
- New in Firmware 5.00.04 7
- New in Firmware 3.20.12 8
- New in Firmware 3.20.11 8
- New in Firmware 3.20.10 8
- Required Third-Party Software 8
- Supported Server Hardware 9

Known and Addressed Issues 9

Known Issues 9
Addressed Issues 10
Support Contacts 13

Product Description

SafeNet ProtectToolkit is Thales'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 ProtectToolkit Software

As in previous releases, 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)

> **NOTE** SafeNet ProtectToolkit 5.2 is not tested or supported on legacy PSG HSMs.

Release Description

SafeNet ProtectToolkit 5.2 extends the functionality and utility of the SafeNet ProtectServer HSMs. SafeNet ProtectToolkit 5.2 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 ProtectToolkit 5.2 if you are using the legacy PSG HSM.

Support for Legacy PSI-E HSMs

PSI-E with SafeNet ProtectToolkit 5.2 supports all the same functionality as the SafeNet ProtectServer PCIe HSM with SafeNet ProtectToolkit 5.2, 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.

New Features and Enhancements

This release provides the following new features and enhancements:

PSESH Command Shell on the SafeNet ProtectServer Network HSM

New release 5.2 (or later) SafeNet ProtectServer Network HSM appliances shipped from the factory now provide a command shell (PSESH). You can use PSESH to configure the appliance as the **admin** or **pseoperator** user. Appliance configuration using **root** and Linux commands is no longer required. Refer to the *SafeNet ProtectServer Network HSM Installation and Configuration Guide* for a detailed description of how to access and use PSESH to configure the appliance.

> **NOTE** For security reasons, the PSESH command shell is available only on new Release 5.2 (or later) SafeNet ProtectServer Network HSMs shipped from the factory. You cannot install it as an upgrade on an existing appliance.

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*

New USB Card Reader

A new USB card reader is available that provides a direct data and power connection to the USB port on the HSM. The legacy card reader that uses USB for data and PS/2 for power (or USB via a PS/2 to USB adapter) continues to be supported.

IPv6 Addressing Support on the SafeNet ProtectServer Network HSM

The SafeNet ProtectServer Network HSM appliance now supports IPv6 addressing. IPv6 support is implemented as a dual stack, allowing the appliance to support both IPv4 and IPv6 simultaneously. That is, you can configure both IPv4 and IPv6 addresses on the eth0 and eth1 interfaces. Refer to the *SafeNet ProtectServer Network HSM Installation and Configuration Guide* for more information.

Support for HP-UX

The SafeNet ProtectToolkit 5.2 software is supported on the HP-UX operating system. See "Supported Platforms" on the next page for more information.

Support 131-A transition (Deprecate DES2 keys)

The 5.00.04 firmware does not allow use of DES2 for encryption, signing, and MACing operations in FIPS mode.

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 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, see "Support Contacts" on page 13.

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

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
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
5.00.06	Network HSM, PCIe HSM	No

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

New in Firmware 5.00.05

Firmware 5.00.05 addresses the following issues. See "Addressed Issues" on page 10 for details.

- PSR-1117
- PSR-1133
- PSR-1424
- PSR-1427

New in Firmware 5.00.04

Firmware 5.00.04 supports the latest features, including the following:

- DES2 deprecated in FIPS mode
- support for the following mechanisms:
  - CKM_RSA_PKCS_PSS
  - CKM_SHA_RSA_PKCS_PSS
  - CKM_SHA224_RSA_PKCS_PSS

- CKM_SHA256_RSA_PKCS_PSS
- CKM_SHA384_RSA_PKCS_PSS
- CKM_SHA512_RSA_PKCS_PSS
- CKM_DES3_CMAC
- CKM_DES3_CMAC_GENERAL
- CKM_AES_CMAC
- CKM_AES_CMAC_GENERAL

Firmware 5.00.04 also provides many bug fixes, as outlined in "Addressed Issues" on page 10.

New in Firmware 3.20.12

Firmware 3.20.12 removes support for legacy smart card drivers (GCR410, PE122, DUMB), and the following features:

> Auth challenge response (**CT_Gen_AUTH_Response** and **CT_GetAuthChallenge**)

> Temporary PINs (**CT_GetTmpPin**)

Thales recommends updating legacy PSE and PSI-E HSMs to firmware 3.20.12, for the latest security updates.

New in Firmware 3.20.11

Firmware 3.20.11 includes bug and vulnerability fixes.

New in Firmware 3.20.10

Firmware 3.20.10 addresses the following issues. See "Addressed Issues" on page 10 for details.

> PSR-1117

> PSR-1133

> PSR-1315

> PSR-1424

Required Third-Party Software

You must install the following third-party software before installing SafeNet ProtectToolkit 5.2:

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, Solaris	> Java Runtime Environment (JRE) 6.x, 7.x, or 8.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-541	M	**Problem:** If you attempt to export a key to a smart card using the **KMU** utility when there is no smart card attached, no error message is displayed. **Workaround:** Ensure that a smart card reader, with a smart card inserted, is attached to the HSM before attempting to perform a key export.
PSR-809	M	**Problem:** PTK-M is not available for Windows 32 bit. **Workaround:** Develop with KSP.
PSR-953	M	**Problem:** Firmware upgrade via **gtcadmin** fails with the error code `0x80000384`, and the HSM is left in a tampered state. **Workaround:** Upgrade firmware using **ctconf**.

Issue	Severity	Synopsis
PSR-1081	M	**Problem:** If you update the firmware on a SafeNet ProtectServer Network HSM, the HSM halts with the error `Could not verify firmware image: 0x5, general error.` Despite the error, the firmware successfully updates. **Workaround:** Reset the HSM using the command **hsmreset**.
PSR-1100	M	**Problem:** If you run **ctfm** to install an FM in an AIX environment, the HSM halts with the error `could not verify Functionality Module image: error 0x5, general error`. Despite the error, the FM successfully installs. **Workaround:** Reset the HSM using the command **hsmreset**.

PSR-1169	M	**Problem:** When performing an MofN backup using the USB card reader, you are prompted twice to insert the next smart card, as follows:
		`Please wait while data is being written to smart card.......`
		`Done.`
		`Please insert the NEXT smart card (Press ENTER to continue).......`
		`Please insert the NEXT smart card (Press ENTER to continue).......`
		Workaround: You must press ENTER twice after inserting the next smart card to initiate the backup operation.

PSR-951	L	**Problem:** The ctconf temperature reading does not function with legacy K5 cards. Therefore, the temperature displayed on the legacy PSE and PSI-E HSMs is 0 Celsius, which is the default value. **Workaround:** None.

Addressed Issues

The following table lists the issues addressed in this release.

Issue	Severity	Synopsis
PSR-1125	H	**Problem:** libcthsm does not work on AIX, affecting HA and WLD. **Resolution:** Fixed in PTK 5.2.
PSR-1127	H	**Problem:** In PTK 5.1 with the SafeNet ProtectServer PCIe HSM, the netserver port is not listening although the Etnetserver service is running correctly. **Resolution:** Fixed in PTK 5.2.
PSR-1131	H	**Problem:** When using JCPROV, the application throws the following exception: `Caused by: java.lang.NoClassDefFoundError: safenet/jcprov/params/CK_RSA_PKCS_PSS_PARAMS` **Resolution:** Fixed in PTK 5.2.
PSR-1132	H	**Problem:** Unable to backup wrapper key (AES 256) to smart card (SafeNet ProtectServer PCIe and Network HSMs only). **Resolution:** Fixed in firmware 5.00.04.

Issue	Severity	Synopsis
PSR-1144	H	**Problem:** On the SafeNet ProtectServer Network HSM and legacy PSE appliance, the NIC stops responding over the network and replies only after the reboot of the appliance. However, the console of the HSM is accessible and hsmstate works fine on the HSM console but not over the network. That is, the appliance is active but not responding over the network. **Resolution:** Fixed in PTK 5.2.
PSR-1315	H	**Problem:** Smart card reader detection is not consistent on the PSI-E and PSE HSMs when using **ctconf –q** or **hsmreset**. **Resolution:** Fixed in firmware 3.20.10.
PSR-1422	H	**Problem:** Decryption with invalid data using Mechanism CKM_RSA_PKCS_OAEP causes E0 in HA Mode **Resolution:** Fixed in firmware 5.00.04.
PSR-1427	H	**Problem:** Verification with AES_CMAC and AES_CMA_GENERAL always fails with Signature Invalid. **Resolution:** Fixed in firmware 5.00.05.
PSR-35	M	**Problem:** Token replication fails after slot deletion. **Resolution:** Fixed in PTK 5.2.
PSR-957	M	**Problem:** C_getInfo() shows Software Only when querying a physical SafeNet ProtectServer PCIe HSM. **Resolution:** Fixed in firmware 5.00.03 and higher.
PSR-1111	M	**Problem:** Memory leak on the SafeNet ProtectServer PCIe and Network HSMs after using CM_Initialize/CM_Finalize to open/close a session. The memory used to open/close this session will not be cleaned up on the card, which can be viewed using **ctconf -v**. The memory does get cleared up after using hsmreset or physically powering down the card, but hsmreset from the remote client may fail with error: `hsmreset: cannot issue the reset command (0x0000000d)` The memory lost on the card per iteration is very low, but could become an issue if the HSM is in production for a long period of time without a reset. **Resolution:** Fixed in firmware 5.00.04.
PSR-1117	M	**Problem:** HSM goes in halted state when attempting to use ctcert to import a certificate (.pem file) that contains special characters, such as " =, , ,=,= " **Resolution:** Fixed in firmware 5.00.05 and 3.20.10.

Issue	Severity	Synopsis
PSR-1129	M	**Problem:** Certificates generated on the SafeNet ProtectServer PCIe and Network HSMs with EC Key and CKM_ECDSA_SHAx (Except SHA1) mechanism have incorrect OID in Signature Algorithm Tag. This behaviour applies to CKM_ECDSA_SHA224, CKM_ECDSA_SHA256, CKM_ECDSA_SHA384, and CKM_ECDSA_SHA512 Only CKM_ECDSA_SHA1 results in a certificate with the correct OID. **Resolution:** Fixed in firmware 5.00.04.
PSR-1133	M	**Problem:** RSA_PKCS Mechanism accepting input data of more than k-11 bytes **Resolution:** Fixed in firmware 5.00.05 and 3.20.10.
PSR-1424	M	**Problem:** ECDH key derivation causes a 128 byte memory leak. **Resolution:** Fixed in firmware 5.00.05 and 3.20.10.
PSR-1794	M	**Problem:** Serial port does not allow login access. **Resolution:** Tech note TE2661 released, instructing users to add an entry for **ttyS0** in the **/etc/securetty** file. The issue will be fixed in PTK 5.3.
PSR-772	L	**Problem:** Custom FMs fail to run in emulation mode, although they run successfully on the HSM. **Resolution:** Fixed in PTK 5.2. You can now successfully run all custom FMs in emulation mode.

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).