SafeNet ProtectServer/ProtectToolkit 5.4

CUSTOMER RELEASE NOTES

Issue Date: 29 March 2019

Document Part Number: 007-007171-014 Rev. F

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

Contents

Product Description

SafeNet ProtectToolkit is Gemalto'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

ProtectServer 5.01.03 firmware provides bug and vulnerability fixes. It supports all the functionality of SafeNet ProtectToolkit 5.4. See "New in Firmware 5.01.03" on page 9 for more information.

SafeNet ProtectToolkit 5.4 extends the functionality and utility of SafeNet ProtectServer HSMs. SafeNet ProtectToolkit 5.4 is compatible with SafeNet ProtectServer Network HSM, Network HSM Plus, and PCIe HSM.

New Features and Enhancements

Release 5.4 provides the following new features and enhancements:

SafeNet ProtectServer Network HSM Plus

The new SafeNet ProtectServer Network HSM Plus provides an upgraded hardware enclosure for the K6 cryptographic engine. Upgraded hardware features include:

- Intel® Pentium® CPU G6950 @ 2.80GHz
- 2 GB RAM

- 250 GB HDD
- Dual redundant power supplies
- Improved fan system with 3 removable fan units and cleanable dust filter

Appliance Software Version Updates

Gemalto 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 Gemalto 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*

Audit Logging

ProtectServer now supports secure audit logging, managed by an Auditor, a role separate from the Admin SO. Logs are stored on the HSM and wrapped off securely to the appliance, where the Auditor can transfer them to a client workstation for verification. All logs are encrypted using a deterministically-generated Audit Key, ensuring that the Auditor is the only user who can view them.

Multiple Custom FMs

Starting with SafeNet ProtectToolkit release 5.4, you can upload multiple custom FMs to an HSM and use them simultaneously. Only one PKCS#11 patched FM can be loaded and used at a time. If a patched FM is already loaded, it is overwritten by the new FM.

Appliance Root Access Removed

To improve the security of SafeNet ProtectServer Network HSM, superuser login access is no longer available on the appliance. All appliance administration tasks are now performed through the PSE Shell (PSESH).

Windows Server 2016 Support

Release 5.4 adds support for client workstations running Windows Server 2016. See "Supported Platforms" on page 7 for details.

Milenage Algorithm

The Milenage cryptographic algorithm is now available on ProtectServer for Mobile 3G Network-related applications.

BIP32 Algorithm and secp256k1 Named Curve Support

The BIP32 cryptographic algorithm and secp256k1 named curve are now available on ProtectServer. This adds ProtectServer support for applications related to hierarchical deterministic wallets, used in Bitcoin and Blockchain transactions.

Factory Reset Network HSM Appliance Settings

The admin user can now reset all appliance account passwords, SNMP settings, and network settings to their factory defaults by executing the PSESH command **sysconf appliance factory**.

New SMS Mode ADH2 Uses SHA-512

The ProtectServer Client software now uses enhanced Anonymous Diffie-Hellman secure messaging protocol (ADH2), utilizing SHA-512-based MAC, as the default mode. This mode is only available when using SafeNet ProtectToolkit 5.4 with firmware version 5.01.00 or newer. If you are using an earlier firmware version with SafeNet ProtectToolkit 5.4, you must set the configuration item ET_PTKC_SMS_MODE=ADH to use standard ADH.

Automatic Log Rotation Available On New SafeNet ProtectServer Network HSMs

The **syslog** service is now configurable in PSESH to allow automatic log rotations. See the *SafeNet ProtectServer Network HSM Installation/Configuration Guide* or run **syslog help** in PSESH for the proper command syntax.

Lockout After 3 Failed Remote Login Attempts

To improve the security of remote SSH connection to the SafeNet ProtectServer Network HSM and Network HSM Plus, three consecutive failed remote login attempts will now result in the appliance being locked out for ten minutes.

Advisory Notes

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.

Firmware 5.01.xx Not Compatible With Older Client Software

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

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

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 Gemalto Technical Support ("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.

Legacy PSI-E HSMs

PSI-E with SafeNet ProtectToolkit 5.4 supports all the same functionality as the SafeNet ProtectServer PCIe HSM with SafeNet ProtectToolkit5.4, 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 FIPS Restrictions in Release 5.4

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 following changes now apply when running in FIPS mode:

- New Diffie-Hellman keys must be a minimum of 2048 bits
- CKM_DH_PKCS_DERIVE cannot be used with existing Diffie-Hellman keys smaller than 2048 bits
- The following mechanisms cannot be used for wrapping with DES3 keys:
  - CKM_DES3_CBC
  - CKM_DES3_CBC_PAD
  - CKM_DES3_ECB
  - CKM_DES3_ECB_PAD
  - CKM_WRAPKEY_DES3_CBC
  - CKM_WRAPKEY_DES3_ECB
  - CKM_WRAPKEYBLOB_DES3_CBC
- The following mechanisms cannot be used for wrapping with AES keys:
  - CKM_AES_CBC
  - CKM_AES_ECB
  - CKM_AES_CBC_PAD
  - CKM_WRAPKEY_AES_CBC
  - CKM_WRAPKEYBLOB_AES_CBC

Firmware 5.01.02 Additional FIPS Mode Restrictions

In addition to the restrictions listed above, the following new FIPS Mode restrictions apply to firmware version 5.01.02, the latest FIPS-certified firmware:

- Only CKM_AES_KW, CKM_AES_KWP and CKM_TDEA_TKW are available for key wrapping in FIPS Mode. All other AES/DES3 wrapping mechanisms are unavailable.
- The following DES3 mechanisms are disabled in FIPS Mode:
  - CKM_DES3_MAC
  - CKM_DES3_MAC_GENERAL
  - CKM_DES3_X919_MAC
  - CKM_DES3_X919_MAC_GENERAL
  - CKM_DES3_RETAIL_CFB_MAC

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 5.4 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	All platforms	C/J	Network HSM (Plus), PSE
	Server 2012 R2	64-bit	C/M/J	All platforms	C/J	Network HSM (Plus), PSE
	Server 2008 (R1 and R2)	64-bit	C/M/J	All platforms	C/J	Network HSM (Plus), PSE
	7	32-bit	-	-	C/J (KSP support)	All platforms
	7	64-bit	C/M/J	All platforms	C/J	Network HSM (Plus), PSE
Linux	RHEL 6	32-bit	-	-	C/J	All platforms
	RHEL 6	64-bit	C/J	All platforms	C/J	Network HSM (Plus), PSE
	RHEL 7	64-bit	C/J	All except PSI-E (K5)	C/J	Network HSM (Plus), PSE
	SUSE12	64-bit	C/J	All except PSI-E (K5)	C/J	Network HSM (Plus), PSE
AIX	6.1	64-bit	C/J	Network HSM (Plus), PSE	C/J	Network HSM (Plus), PSE
	7.1	64-bit	C/J	Network HSM (Plus), PSE	C/J	Network HSM (Plus), PSE
	7.2	64-bit	C/J	Network HSM (Plus), PSE	C/J	Network HSM (Plus), PSE
Solaris	10 (SPARC, x86) 11 (SPARC, x86)	64-bit	C/J	Network HSM (Plus), PSE	C/J	Network HSM (Plus), PSE
HP-UX	11	64-bit	C/J	Network HSM (Plus), PSE	C/J	Network HSM (Plus), PSE

Supported Firmware

Firmware Version	Available Platforms	FIPS Level 3 Certified
5.01.03	Network HSM, Network HSM Plus, PCIe HSM	Certification Pending
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

Firmware Version	Available Platforms	FIPS Level 3 Certified
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 5.01.00. If you require FIPS certification immediately, you can download and install firmware 5.01.02.

FIPS Status

The latest FIPS-certified firmware version is 5.01.02. 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 5.01.03

Bug and vulnerability fixes. This firmware version contains all features from release 5.4.

New in Firmware 5.01.02

Bug fixes; FIPS Level 3 ceritified. This firmware version contains all features from release 5.4.

New in Firmware 5.01.01

Firmware 5.01.01 provides bug fixes as outlined in "Addressed Issues" on page 11. This firmware supports all the latest features from release 5.4.

New in Firmware 5.01.00

Firmware 5.01.00 supports the latest features described above, including support for the following mechanisms:

- CKM_MILENAGE_SIGN
- CKM_MILENAGE_DERIVE
- CKM_BIP32_MASTER_DERIVE
- CKM_BIP32_CHILD_DERIVE
- CKM_AES_KW
- CKM_AES_KWP
- TDEA_TKW
- WRAPKEY_AES_KWP

Firmware 5.01.00 also provides bug fixes.

New in Firmware 5.00.08

Bug fixes. This firmware version contains all features from release 5.3.

Required Third-Party Software

You must install the following third-party software before installing SafeNet ProtectToolkit 5.4:

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-2123	M	**Problem**: On Solaris x86, **ctconf –v** and **ctconf –g** commands report some debug information. **Workaround**: This information can be ignored.
PSR-2117	M	**Problem**: On Windows systems hosting a SafeNet ProtectServer PCIe HSM, the Device Manager shows two entries for the ProtectServer card. **Workaround**: The extra entry can be ignored or removed from the Device Manager.
PSR-2083	M	**Problem**: With firmware 5.01.xx installed, the KMU utility does not perform backup. **Workaround**: Use the command-line utility **ctkmu** to backup cryptographic material.
PSR-953	M	**Problem**: Firmware upgrades through **gctAdmin** appear to fail with error code 384, but the upgrade actually succeeds. The HSM must then be reset. **Workaround**: Reset the HSM after upgrading the firmware; the error can be safely ignored. Alternatively, use the command **ctconf –g** to upgrade the HSM firmware.
PSR-2119	L	**Problem**: The serial port on SafeNet ProtectServer Network HSM or SafeNet ProtectServer Network HSM Plus becomes unresponsive. **Workaround**: Disconnect and re-connect the provided DB9-to-USB cable and start a new serial session.

Addressed Issues

The following table lists the issues addressed in this release.

Issue	Severity	Synopsis
PSR-2097	H	**Problems**: Issues related to card readers. a. When retrieving the LMK using a USB card reader, inserting a 2nd card returns an error, requiring **hsmreset**. b. When a USB reader card is inserted, the FM crashes. c. If a card is inserted incorrectly in a serial card reader, the session between the FM and 0 slot is closed. **Resolution**: Fixed in firmware 5.01.01.
PSR-2042	H	**Problem**: When an empty USB smart card reader is connected to an HSM configured for High Availability, applications return an error (Session Handle Invalid). **Resolution**: Fixed in firmware 5.01.01.
PSR-1939	M	**Problem**: When deleting an FM from the HSM using **ctfm d**, the HSM goes into a halted state. **Resolution**: Fixed in release 5.4.
PSR-1963	M	**Problem**: Continuous execution of **ctconf –v** may result in memory reported as “UNAVAILABLE” even though the HSM will continue to operate normally. **Resolution**: Fixed in firmware 5.00.08.

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. **Resolution**: Fixed in release 5.4.
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. **Resolution**: Fixed in release 5.4.
PSR-1913	L	**Problem**: When SafeNet ProtectToolkit-C Runtime is installed on Unix systems, **setvars.sh** cannot be sourced to configure environment variables. **Workaround**: Fixed in release 5.4; sourcing **setvars.sh** is necessary on Linux platforms only.

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 Gemalto Customer Support.

Gemalto 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 Gemalto 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.gemalto.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 Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@gemalto.com.