SafeNet ProtectServer/ProtectToolkit 5.5

CUSTOMER RELEASE NOTES

Issue Date: 31 July 2018

Document Part Number: 007-007171-016 Rev. C

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

SafeNet ProtectToolkit 5.5 extends the functionality and utility of SafeNet ProtectServer HSMs. SafeNet ProtectToolkit 5.5 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. The SafeNet ProtectToolkit 5.5 product documentation lists the old processor under Technical Specifications. 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 5.00.02.

New Features and Enhancements

Release 5.5 provides the following new features and enhancements:

Key Management Utility (KMU) Backup

The Key Management Utility (KMU) can now be used as a FIPS approved mechanism to backup keys, certificate objects, and other PKCS#11 objects. The keys, certificate objects, and other PKCS#11 objects can be backed-up to a smart card or the local file system. All of the PKCS#11 attributes for any key/object, including the security attributes, are backed up along with the key/object's value.

Key Component Entry via Verifone VX805 PIN Pad

ProtectServer 5.5 adds support for the Verifone PIN pad model VX805. The current PIN pad model PP1000se is still supported.

ctbrowse Support for RSA-PSS Algorithms

ProtectServer 5.5 introduces **ctbrowse** support for RSA-PSS signature generation. RSA-PSS can be used as a mechanism for certificate signing, provided the signing key/private key (used to sign the certificate) is RSA.

Support for AES-OFB Algorithms

The AES-OFB cryptographic algorithms are now available on ProtectServer. This adds ProtectServer support for the AES-OFB block cipher and stream cipher. You can now use AES-OFB for encrypting and decrypting, and wrapping and unwrapping.

Support for PKCS#11 v2.20 Compliant AES Algorithms

AES algorithms compliant with PKCS#11 v2.20 are now available on ProtectServer. This adds ProtectServer support for AES symmetric block cipher, encryption and decryption, multi-part MAC, and multi-part verify. ProtectServer 5.5 introduces the following AES key derivation mechanism:

- CKM_AES_CBC_ENCRYPT_DATA

Support for PKCS#11 v.2.20 Compliant DES/DES3 Algorithms

DES/DES3 algorithms compliant with PKCS#11 v2.20 are now available on ProtectServer. The DES/DES3 mechanisms released with previous versions of ProtectServer are now PKCS#11 v2.20 compliant. This adds ProtectServer support for DES/DES3 symmetric block cipher, encryption and decryption, multi-part MAC, and multi-part verify. ProtectServer 5.5 introduces the following DES/DES3 key derivation mechanisms:

- CKM_DES_ECB_ENCRYPT_DATA
- CKM_DES_CBC_ENCRYPT_DATA
- CKM_DES3_ECB_ENCRYPT_DATA
- CKM_DES3_CBC_ENCRYPT_DATA

Support for SHA256 with ECDSA GBCS

ProtectServer 5.5 introduces support for the SHA256 with ECDSA GBCS signing algorithm. You can now use SHA256 with ECDSA GBCS as a signing algorithm within ProtectServer.

Curve25519

The named curve Curve25519 is now available on ProtectServer. You can now use Curve25519 for key derivation on ECDH operations.

Advisory Notes

Previously Released Versions of Windows Installer Trigger Anti-Virus Software

Binaries within the SafeNet ProtectToolkit 5.4 and previously released versions of the Windows installer are being flagged as malware by anti-virus software. Previously released versions of Windows Installer are still usable however they may conflict with your anti-virus software.

Firmware 5.01.xx and Newer Versions are 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 5.5 *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 (see "Support Contacts" on page 12).

Legacy PSI-E HSMs

PSI-E with SafeNet ProtectToolkit 5.5 supports all the same functionality as the SafeNet ProtectServer PCIe HSM with SafeNet ProtectToolkit5.5, 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 5.5

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 5.5 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

Operating System		OS type	64-bit PTK	64-bit PTK supported hardware	32-bit PTK	32-bit PTK supported hardware
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
5.02.00	Network HSM, Network HSM Plus, PCIe HSM	No
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 5.01.02.

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 5.02.00

Firmware 5.02.00 provides bug fixes as outlined in "Addressed Issues" on page 10. This firmware supports the latest features from release 5.5. Firmware 5.02.00 introduces support for the following mechanisms:

- CKM_AES_CBC_ENCRYPT_DATA

- CKM_DES_CBC_ENCRYPT_DATA
- CMK_DES_ECB_ENCRYPT_DATA
- CKM_DES3_CBC_ENCRYPT_DATA
- CKM_DES3_ECB_ENCRYPT_DATA
- CKM_AES_OFB
- CKM_ECDSA_GBCS_SHA256

New in Firmware 5.01.02

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

Required Third-Party Software

You must install the following third-party software before installing SafeNet ProtectToolkit 5.5:

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.

Severity Classification	Definition
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-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-2025	L	**Problem**: When ProtectServer PCIe (K6) is installed on HP DL360 Gen9, the server may restart when the shutdown command is input. This happens only on HP BIOS versions later than v2.00_12-27-2015. **Workaround**: Disable the ProtectServer PCIe HSM before server shutdown or downgrade the server BIOS to v2.00_12_27-2017.

PSR-2211	L	**Problem**: The FM-SDK automated cross-compiler build script fails on Windows operating systems.
		Workaround: Open the **cross.cmd** file in a text editor and replace the following line:
		`mingw-get install mingw32-base mingw32-gcc-g++ mingw-developer-toolkit mpc-dev mpfr-dev gmp -dev`
		with
		`mingw-get install mingw32-base "mingw32-gcc-g++<6" mingw-developer-toolkit mpc-dev mpfr-dev "gmp-dev<6`

Addressed Issues

The following table lists the issues addressed in this release.

Issue	Severity	Synopsis
PSR-2159	H	**Problem**: Restore operation fails when using the multi-custodian method. **Resolution**: Fixed in release 5.5
PSR-2123	M	**Problem**: On Solaris x86, **ctconf –v** and **ctconf –g** commands report some debug information. **Resolution**: Fixed in release 5.5.
PSR-2117	M	**Problem**: On Windows systems hosting a SafeNet ProtectServer PCIe HSM, the Device Manager shows two entries for the ProtectServer card. **Resolution**: Fixed in release 5.5.
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. **Resolution**: Fixed in release 5.5

Issue	Severity	Synopsis
PSR-2083	M	**Problem**: With firmware 5.01.xx installed, the KMU utility does not perform backup. **Resolution**: Fixed in release 5.5.
PSR-2027	M	**Problem**: Generic secret key generation for large key sizes using CKM_GENERIC_SECRET_KEY_GEN causes firmware crash. **Resolution**: Fixed in release 5.5.

Revision History

Revision A: 11 December 2017

> Initial Release

Revision B: 19 March 2018

> Added to "Release Description" on page 3:

- Upgraded Intel® Atom™ CPU E3827 processor for SafeNet ProtectServer Network HSM

> Added to "Advisory Notes" on page 5:

- Firmware 5.01.02 -- Firmware 5.01.02 Additional FIPS Mode Restrictions

> Added to "Supported Firmware" on page 8:

- Firmware 5.01.02 -- candidate for FIPS certification

Revision C: 31 July 2018

> Added to "Supported Firmware" on page 8:

- Firmware 5.01.02 -- 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 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.