PTK 4.0 with Firmware 3.00.03 Customer Release Notes

Document #: 007171-004Revision A

Release Notes Issued on: 2008/11/17

Updated: 2009/11/17

Product Description

ProtectToolkit is SafeNet's PKCS #11 V 2.10 compliant, API product. The distribution supports the following hardware components:

- ProtectServer Internal (PSI-E) – Intelligent cryptographic adapter (PCIe bus)
- ProtectServer External – Networked appliance containing current version of PTK-C and PS firmware
- ProtectServer Gold – legacy intelligent cryptographic adapter (PCI bus)

The distribution includes the following software components:

- PTK-C – Toolkit for PKCS #11 and C Language API calls
- PTK-J – API support for Java
- PTK-M – Microsoft CAPI and CNG support

Version Summary

Component	Version
PTK-C	4.00.00
PSG and PSI-E firmware	3.00.03
PSe	4.0
PTK-J	4.00.00
PTK-M	4.00.00

New Features and Enhancements

Ptk-C Version	Reason for Update
4.00	• PSI-E (ProtectServer Internal for PCI-E slots) short-

	form-factor adapter card supported • Bug fixes
3.33	• Update firmware to meet FIPS validation standards
3.32	• Updated firmware to meet FIPS validation standards • Support for RoHS-compliant peripherals • Support for European passport project • Safenet rebranding
3.28.00	• implements requirement for minimum 4-character password, as requested by FIPS auditors
3.27.00	• Added support for Siemens CardOS V4.3 Smartcards
<previous>	• (See release notes accompanying previous releases.)

Scope

This version is released for general distribution. Please see Advisory Notes and Known Issues for limitations and restrictions.

Summary of Release Support

PTK-C Release Support by Platforms

OS/Platform	**Ptk-C Version**	**Ptk-C Version**
	3.33	**4.0**
Windows 2003	√	√
Windows NT	√	
Windows 2008 Server	√	√
Solaris 9 (32-bit)	√	√
Solaris 10 (32-bit)	√	√
Solaris 9 and 10 (64-bit)	√	√
Linux - Red Hat 8 (kernel 2.4.x)	√	
Linux – Red Hat Enterprise Server 3 (kernel 2.4.x)		
Linux - Red Hat Enterprise Server 4 and 5 (kernel 2.6.x) – 32 bit	√	√

Linux - Red Hat Enterprise Server 4 and 5 (kernel 2.6.x) – 64 bit	√	√
Linux SuSe 9 – 32 bit		√
Linux SuSe 9 – 64 bit		√
Linux SuSe 10 – 32 bit	√	√
Linux SuSe 10 – 64 bit		√
AIX 5.3 (32-bit)	√	√*
AIX 5.3 (64-bit)	√	√*
AIX 6.1		√*
HP-UX 11i (32-bit)	√	
HP-UX 11i (64-bit)	√	

* Not supported with PSI-E at this time

Advisory Notes

Run "ctconf -t" on first install of card: The first time you install any of:
PSI-E
PSI
PSG
and before running any other command, synchronize the card clock with the machine clock by running "ctconf -t".
Also, initialize the user token, as there are a couple of performance tests that are skipped if the user token is not initialized.

SafeNet KSP for CNG: Configuration instructions for KSP (our interface to Microsoft CNG) were incorrect in the Ptk-M manual. Please see the end of this Customer Release Notes document for the corrected KSP configuration instructions, which will also be incorporated into the next-release Ptk-M manual.

Solaris 9 for SPARC: On Solaris 9 for SPARC it is possible that the operating system will assign the driver "**cpu**" to the ProtectServer cryptographic hardware adapter. In this case it will appear in the output from "**prtconf –D**" and the SafeNet device driver will install but will not attach. The following error messages will result:

devfsadm: driver failed to attach: e8k

Warning: Driver (e8k) successfully added to system but
failed to attach

In this case, try the following:

1. After the installation, reboot the computer and see if the driver has attached. If it has then the **hsmstate**(1) utility will work.

2. If (1) fails then uninstall the driver (see the Uninstallation section below) and remove the protectserver cryptographic hardware adapter. Now re-boot and re-install the PCI HSM Access Provider package without the card in the computer.

Shut down, re-install the card and re-boot. See if the **hsmstate**(1) utility works.

3. If (2) fails then ensure that you have the most up-to-date patch for Solaris 9 and re-attempt 2.

If you are unable to apply the most up-to-date patch and/or still unable to successfully add the driver to the system, contact SafeNet technical support and request the "PTK 4.0 patch driver for Solaris 9." This driver removes a dependency present in the older versions of the Solaris 9 kernel.

Memory reduction on PSI: The newer PSI-E cards have – and report - 128MB of onboard memory (as designed), compared to 512MB on the older PSG card. This difference has no operational impact.

PSI-E if in doubt, tamper: If the PSI-E card displays an un-useful or non-responsive state that does not resolve itself after a system reboot, try "tampering" the card by removing it from the computer for a few minutes and then re-inserting it. If the card does not return to normal operation, contact SafeNet Customer Support.

Windows 2003 and 2008 Note – By default, Windows 2003 and 2008 server will block the ETNETSERVER package from sending information to the client. If you are using these operating systems as a server, make sure you either make the "HSM messenger service" or "Local Area Connection" an exception for the firewall.

Resolved Issues

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

Issues resolved in this release

Issue#	Severity	Synopsis
74996	M	Unix version of Network access provider terminates if HSM not listening
71618	C	PTK 4.0 - Firmware port - add ARIA support

Issue#	Severity	Synopsis
75826/71120	C	PTK 4.0 - add support for Solaris X86, 32 and 64-bit
71103	M	Problems creating intermediate CA certificate
71037	M	driver for PSG included with PTKM installation
70466	M	Incompatibility with BouncyCastle provider
70329	M	Add RSA OAEP support to PTK C ctkmu and ctbrowse
68763	C	PTK 4.0 - add new Operating System support for AIX 6.0 and 6.1
67946	C	PTK 4.0 - port host driver onto non-Windows OSs
67299	M	PTK C SDK Unix Install package installs unwanted stub library
66447	C	PTK 4.0 - porting work (other than firmware) - Java 1.6 support
66430	C	PTK 4.0 - Software Emulator Port - add ARIA support
65187	H	PTKM: SSL is not working on Windows
64261	C	logging error (AIX only) in Net Client Access Provider - see also MKS 60997
63004	H	The cryptoki2.lib library file is missing from the Win64 SDK release. This file is necessary for linking 64-bit programs.
59516	M	ctperf fails to run in high-memory Linux64 systems.
58869	H	Linux64 fails to update firmware.
40035	M	Import ECC Parameters should be available in GUI KMU
37679	M	WLD settings need to be in 'Eracom' folder
29746	M	Cannot create generic secret key from components in KMU GUI

Known Issues and Workarounds

This is a list of the issues known at time of release:

Issue	Priority	Synopsis
(80808) Driver on	M	**Problem:** If you try to load the driver on a SuSE

Issue	Priority	Synopsis
SuSE won't compile		system, compilation will fail: rpm -U pci_hsm_access_provider/ETpcihsm-4.00.00-1.i386.rpm make -C /lib/modules/2.6.13-15-smp/source SUBDIRS=/opt/ETpcihsm/src modules make[1]: Entering directory `/usr/src/linux-2.6.13-15' CC [M] /opt/ETpcihsm/src/e8k_main.o /opt/ETpcihsm/src/e8k_main.c: In function 'e8k_ioctl': /opt/ETpcihsm/src/e8k_main.c:1588: warning: cast to pointer from integer of different size CC [M] /opt/ETpcihsm/src/e8k_linux.o /opt/ETpcihsm/src/e8k_linux.c: In function 'e8k_cleanup_module': /opt/ETpcihsm/src/e8k_linux.c:864: error: implicit declaration of function 'class_simple_device_remove' /opt/ETpcihsm/src/e8k_linux.c:917: error: implicit declaration of function 'class_simple_destroy' /opt/ETpcihsm/src/e8k_linux.c: In function 'e8k_init_module': /opt/ETpcihsm/src/e8k_linux.c:1049: error: implicit declaration of function 'class_simple_create' /opt/ETpcihsm/src/e8k_linux.c:1049: warning: assignment makes pointer from integer without a cast /opt/ETpcihsm/src/e8k_linux.c:1058: error: implicit declaration of function 'class_simple_device_add' make[2]: *** [/opt/ETpcihsm/src/e8k_linux.o] Error 1 make[1]: *** [_module_/opt/ETpcihsm/src] Error 2 make[1]: Leaving directory `/usr/src/linux-2.6.13-15' make: *** [e8k.ko] Error 2 ETpcihsm: compile failed. Please see /opt/ETpcihsm/README for further instructions. error: %post(ETpcihsm-4.00.00-1) scriptlet failed, exit status 1. **Workaround:** After the driver fails, go to /opt/ETpcihsm/src and open e8k_linux.c, and edit the lines (NOTE: these have changed since Ptk 3.32) 92, 115, 863, 916, 1044 that contain: #if LINUX_VERSION_CODE <= KERNEL_VERSION(2,6,16)

Issue	Priority	Synopsis
		to this: #if LINUX_VERSION_CODE <= KERNEL_VERSION(2,6,12) and re-compile with "make clean add"
(80813) Driver fails to attach in Solaris 9 install	H	**Problem:** When you try to install the PTK 4.0 driver for a PSG, you get a "failed to attach" message and the PSG will not work. **Workaround:** See the Advisory note for Solaris 9 for SPARC on page 1 of these Release Notes. Contact customer support for patch.
(80542) ctident does not recognize PSI serial number	M	**Problem:** When you are generating identity key pairs or trust relationships with the 'ctident' tool, it does not recognize a PSI device using its serial number. A workaround for this is to use the device numbers instead of serial numbers (example: "ctident trust 0 1"). However any user following the PTKC administration manual will use serial numbers. Cryptoki Version = 2.10 Manufacturer = Safenet, Inc. aa (Slot 0) AdminToken (400885) (Slot 1) aa (Slot 2) AdminToken (135791) (Slot 3) X:\PTK4.0>ctident gen sn:135791 ProtectToolkit C HSM Identity Key Management Utility $Revision: 1.1.1.1 $ Copyright (c) Safenet, Inc. 2009 No device exists with serial number 135791 X:\PTK4.0>ctident trust sn:135791 sn:400885 ProtectToolkit C HSM Identity Key Management Utility $Revision: 1.1.1.1 $ Copyright (c) Safenet, Inc. 2009 No device exists with serial number 135791. **Workaround:** Use device numbers instead of serial numbers (until this is fixed, ignore the suggested practice in the Ptk-C Administration Manual).
(80355) creating key on PSI with	M	**Problem:** Trying to create a key with a non-standard key size can take a really long time to

Issue	Priority	Synopsis
non-standard key size will cause system to hang and put HSM in bad state		complete (about 6 -10 minutes depending on the size requested) and will subsequently put the HSM in a "Halted" state. Performing an hsmreset takes the HSM out of this state. Note that the key IS created. This happens only on a PSI. With a PSG the key is created in a normal amount of time, and continues to operate in a responsive state. The problem occurs when trying to generate RSA keys with non-standard sizes >= 2200. Anything less than that and the command immediately fails with a "key size range" error. **Workaround:** Use standard key sizes, if possible.
(80269) csoftware .cryptoki not forward compatible from 32-bitto 64-bit	L	**Problem:** In software mode, the .cryptoki directory manages the software HSM. This directory is not removed when the PTK-C SDK package is removed. The problem described below relates to only AIX, SPARC and x86 Solaris (presumably to HP-UX as well, though it's not part of this release). If you initialize software mode in 32 -bit, then switch your env paths to 64 -bit, cttools will fail (error shown below). However, if you initialize software in 64 -bit you can then operate in either 32 -bit or 64 -bit software. **Workaround:** If you do init in 32 -bit and wish to switch to 64 -bit, the only solution (at this time) would be to "tamper" your software HSM by deleting $HOME/.cryptoki.
(80086) PTKJ samples have bad directory structure in Windows	L	**Problem:** The directory structure for the PTKJ samples in Windows has changed - they used to be in the directory \eracom_tech\ptkj\samples\<samplename>, now they are simply in the directory \samples\<samplename>. This creates a problem as the "package" line in all the samples is "package eracom_tech.ptkj.samples.<samplename>. So if you try to run the samples in their current directory, you will get a "bad name" runtime error. **Workaround:** Workaround for this would be either

Issue	Priority	Synopsis
		to create the missing directories and place the appropriate file in there, or to simply comment out the "package" line.
(80050) SDK needs util.mak in samples dir	M	**Problem:** Trying to compile samples in Windows generates an error: D:\Program Files\SafeNet\Protect Toolkit C SDK\samples\copyobj>nmake Microsoft (R) Program Maintenance Utility Version 6.00.8168.0 Copyright (C) Microsoft Corp 1988-1998. All rights reserved. makefile(2) : fatal error U1052: file '..\util.mak' not found Stop. The makefile calls for ..\util.mak, which is not present in the current build of the SDK. **Workaround:** Contact Customer Support for a util.mak file.
(80013) registering java provider disables some jprovdemo functions	M	**Problem:** jprovdemo will work normally if default install of PTK-J is used. If, however, you register the java provider (add jprov.jar to the java "ext" dir, and add the Eracom provider to the java.security list in the java security dir) then all attempts to generate random secret keys will fail without error. Simply, nothing happens when the generate button is pressed. **Workaround:** Use jprovdemo only on non-production computer(s) where you have not registered the SafeNet Eracom provider.
(79722) "Use PED" in KspConfig	M	**Problem:** When assigning slots with the KspConfig utility, there is a "Use PED" checkbox underneath the password entry text box. As there is not currently a PED for the PTK product, this checkbox should be removed. Note: checking this box when entering the password will give a "bad password" error message if checked, even with the correct password.. **Workaround:** Ignore "Use PED"; it is not a real

Issue	Priority	Synopsis
		option for PTK – it is used with other SafeNet products. Do not check the box.
(79518) Windows install of ETcprt should warn if device driver not installed	M	**Problem:** Previous versions of PTK would give you a warning if you tried to install PTKC Runtime (ETcprt) before you installed the device driver (pcihsm or nethsm). Version 4.00 does not give this warning - ETcprt can be installed without a DD with no complaint - until you try to run a command, of course. This also happens when you install the SDK in hardware mode. **Workaround:** Be aware that the driver must be installed first, before you install Etpcihsm or Etnethsm (on Windows).
(79339) PSI does not report serial number with 'ctstat'	M	**Problem:** The PSI does not report its serial number with 'ctstat', where a PSG does. Here's output from a PSG: [root@ka ~]# ctstat -s0 ProtectToolkit C Status Utility $Revision: 1.1.1.2 $ Copyright (c) Safenet, Inc. 2009 Slot ID 0 Description : ProtectServer Gold:52751 Manufacturer : SafeNet Inc. Hardware Version : 66.00 Firmware Version : 3.00 Token for Slot ID 0 Label : aaa Manufacturer : SafeNet Inc. Model : PSG:PL600 Serial Number : 400885:52751 Hardware Version : 66.00 Firmware Version : 3.00 And here's output from a PSI: ProtectToolkit C Status Utility $Revision: 1.1.1.2 $ Copyright (c) Safenet, Inc. 2009 Slot ID 0 Description : ProtectServer K5:70620 Manufacturer : SafeNet Inc. Hardware Version : 65.00 Firmware Version : 3.00 Token for Slot ID 0 Label :

Issue	Priority	Synopsis
		Manufacturer : SafeNet Inc. Model : K5:PL600 Serial Number : :70620 Hardware Version : 65.00 Firmware Version : 3.00 **Workaround:** n/a
(79049) ctkmu does not set CKA_ID when importing keys	M	**Problem:** The CKA_ID attribute is set when generating a key on the HSM. However, when a key is imported it is not set and this field is blank. CTKMU should have the ability to set this attribute when importing keys. **Workaround:** On Windows, use ctbrowse. On other systems you would need a custom utility to set the attribute until this problem is fixed.
(78282) SafeNet PCI HSM uninstall on Windows 2003 32 bit	L	**Problem:** When we uninstall SafeNet PCI HSM uninstall on Windows 2003 32 bit as the last SafeNet application the following is left behind: C:\Program Files\SafeNet\PCI HSM\bin\ethsm.dll The uninstall is deleting the folder on Windows2003 64 bit and on Windows 2008 32 and 64 bit. **Workaround:** Delete the entire C:\Program Files\SafeNet folder after the uninstall of SafeNet PCI HSM uninstall on Windows 2003 32 bit **only** if it the last SafeNet software being uninstalled..
(77742) Clean up loose files in Win64 SDK	M	**Problem:** The Win64 SDK has duplicate files where there shouldn't be any. Leaving them in place could affect operation and registering applications, though this has not been found in testing. The following files are found under C:\Program Files\SafeNet\Protect Toolkit C SDK\ and should be removed: - ber.lib (duplicate of C:\Program Files\SafeNet\Protect Toolkit C SDK\lib\ber.lib) - cryptoki.dll and cryptoki.dll.sig (should only be found in C:\Program Files\SafeNet\Protect Toolkit C SDK\bin under extToken, hsm, logger, and sw - fcrypt.exe (duplicate of C:\Program Files\SafeNet\Protect Toolkit C SDK\bin\fcrypt.exe) - x509.lib (duplicate of C:\Program Files\SafeNet\Protect Toolkit C SDK\lib\x509.lib) - x962.lib (C:\Program Files\SafeNet\Protect Toolkit C SDK\lib\x962.lib) **Workaround:** Files can be ignored. Manually

Issue	Priority	Synopsis
		remove the indicated files if desired – not considered necessary.
(77493) Support of ChipDrive card reader fot PSG/K5e	M	**Problem:** Chip Drive card reader does not work on release 4.00. **Workaround:** Use the supported OmniKey card reader, or wait until next release for ChipDrive reader support.
(77334) bad attribute with 'ctkmu c' will generate incorrect error message	M	**Problem:** Supplying a bad attribute for 'ctkmu c' will generate the wrong error message - it generates the error message intended for a bad attribute for 'ctkmu idp': [root@ka ~]# ctkmu c -tdes -ntest -aQ ProtectToolkit C Key Management Utility Revision: 3.33.2 Copyright (c) Safenet, Inc. 2009 ctkmu: Invalid attributes specified with -a<attribute> option. ctkmu: Attribute 'Q' not appropriate for Domain Parameter Valid attributes are - P and M **Workaround:** n/a
(77254) Permission for ETpcihsm driver gets reset on reboot on RHEL 4	M	Permission for ETpcihsm driver gets reset on reboot on RHEL 4 OS with non-root login /dev/e8k0 has read write permissions only at root level as detailed below: [tester@ott1-titan ~]$ ls -l /dev/e8k* crw------- 1 root wheel 254, 0 Aug 10 15:55 /dev/e8k0 crw-rw-rw- 1 root wheel 254, 1 Aug 10 15:55 /dev/e8k1 crw-rw-rw- 1 root wheel 254, 2 Aug 10 15:55 /dev/e8k2 crw-rw-rw- 1 root wheel 254, 3 Aug 10 15:55 /dev/e8k3 crw-rw-rw- 1 root wheel 254, 4 Aug 10 15:55 /dev/e8k4 crw-rw-rw- 1 root wheel 254, 5 Aug 10 15:55 /dev/e8k5 **Workaround:** Set permissions to 644
(77232) tampered PSIe card requires 2nd power cycle to function	H	**Problem:** PSIe card will be unusable if installed into computer when zeroized, which will happen in 1 of 3 circumstances:

Issue	Priority	Synopsis
		- new card installed into computer - manually tampered and moved card - transport mode set to none and card is moved If any of these 3 are done, hsmstate will show the card to be tampered. Hsmreset will not complete and, therefore, not return card to normal operation. The only solution to get the card operational is to power-cycle the computer. Transport mode set to continuous or single shot will work as expected. **Workaround:** Cycle the computer power.
(76711) jcprov does not declare paramter CK_MAC_GENERAL_ PARAMS	M	**Problem:** There is defect in our jcprov (java native interface) for the PTKC. It does not specify/declare the parameter CK_MAC_GENERAL_PARAMS which is used in conjunction with mechanisms such as CKM_DES3_MAC_GENERAL and CKM_AES_MAC_GENERAL. **Workaround:** see workaround in MACgen.java demo at the end of this Release Note.
(76675) PSIe driver install requires reboot on Win32/64, PSG does not	M	**Problem:** The PCI driver install, as it finishes, has a pop-up asking the user to reboot the system when installation completes. A reboot is required if a PSIe is installed as running (for example) hsmstate returns a message indicating that the HSM is in a power off state with no key material. **Workaround:** Reboot. Applies only to PSI-E.
(59882) 'ctstat' conflicts with name of Solaris 10 utility	L	**Problem:** There is a Solaris 10 utility called 'ctstat', which happens to be the name of a PTK-C utility. This can be a problem if the user has PTK-C tools in his PATH. **Workaround:** If you intend to have your PTK-C ctstat in the PATH, make sure you have /opt/PTK/bin listed before /usr/bin in the PATH.

Issue	Priority	Synopsis
(37609) Windows firewall settings block etnetserver	L	**Problem:** The default firewall settings on Windows 2003 and 2008 block "HSM messenger service" which prevents etnetserver from sending data to the client. This is not immediately apparent when etnetserver is installed and the user clicks "Yes" to setting etnetserver as a system service. Only when you manually run etnetserver does Windows server alert you that it is blocking the HSM messenger service. **Workaround:** The user needs to set his/her firewall settings correctly. This is noted in the advisory section at the top of this document.
(36976) OmniKey smartcard reader issues on software emulator	M	**Problem:** The OmniKey smartcard reader and the Verifone PIN pad reader do not work in software emulation mode. **Workaround:** None. To be addressed in a future release.

Publications

The publications associated with this release are:

Documentation CD

- 009812-001_ptk_4-0_quickstart_guide_rev-a.pdf
- 800230-003 071409.pdf
- 800230-003 071409.txt
- 002861-005_ptkc_installation_guide_rev-a.pdf
- 002924-004_psi_installation_manual-rev-a.pdf
- 006731-003_hsm_access_provider_install_guide_rev-a.pdf
- 006734-001pkcs11v2-10.pdf
- 007474-004_ps_e_installation_guide_rev-a.pdf
- 007568-003_updt_ptk_and_fw_rev-a.pdf
- 008393-002_ptk_c_administration_manual_rev-a.pdf
- 008394-002_ptkc_kmu_key-management_util_user-gd_rev-a.pdf
- 008395-002_ptk-c_sdk_user_manual_rev-a.pdf
- 008396-003_ptk_c_programmers_manual_rev-a.pdf
- 002855-004_ptk-j_installation_guide_rev-a.pdf
- 007556-002_ptk_j_reference_manual_rev-a.pdf
- 008398-001_ptkj_jca_jce_api_overview_rev_b.pdf
- 008399-001_ptkj_jca_jce_api_tutorial_rev_b.pdf
- 002863-005_ptkm_user_manual_rev-a.pdf
- 007568-003_updt_ptk_and_fw_rev-a.pdf

MACGen.java for Known Issue 76711

```
/*
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
 */

/**
 *
 * @author Nsrivastava
 */
import eracom_tech.jcprov.*;
import eracom_tech.jcprov.constants.*;


public class MACGen
{
    private static long slotID = 0;
    private static String pin = "123456";
    private static String keyName = "test_des3";
    private static String plain_data = "This is the data to sign. " +
                                       "This is the data to sign. " +
                                       "This is the data to sign. ";

    public static void main(String[] args)
    {
        CK_SESSION_HANDLE session = new CK_SESSION_HANDLE();
        CK_RV rv = new CK_RV();
      CK_ATTRIBUTE[] template =
      {
        new CK_ATTRIBUTE(CKA.LABEL,keyName.getBytes()),
        new CK_ATTRIBUTE(CKA.KEY_TYPE,CKK.DES3),
        new CK_ATTRIBUTE(CKA.TOKEN,CK_BBOOL.TRUE),
      };
      LongRef objectCount = new LongRef();
      CK_OBJECT_HANDLE[] hObjects = {new CK_OBJECT_HANDLE()};

      Long mech_Param = new Long(8);
      CK_MECHANISM mech = new CK_MECHANISM(CKM.DES3_MAC_GENERAL, mech_Param);

      byte signature[] = new byte[8];
      LongRef signatureLen = new LongRef(signature.length);

      try
      {
        rv = CryptokiEx.C_Initialize(new CK_C_INITIALIZE_ARGS(CKF.OS_LOCKING_OK|
```


```
CKF.LIBRARY_CANT_CREATE_OS_THREADS));
        System.out.println("C_Initialize returned : " + rv.intValue());

        rv = CryptokiEx.C_OpenSession(slotID, CKF.RW_SESSION|CKF.SERIAL_SESSION, null, null, session);
        System.out.println("C_OpenSession returned : " + rv.intValue());

        rv = CryptokiEx.C_Login(session, CKU.USER, pin.getBytes(), pin.length());
        System.out.println("C_Login returned : " + rv.intValue());

        rv = CryptokiEx.C_FindObjectsInit(session, template, template.length);
        System.out.println("C_FindObjectsInit returned : " + rv.intValue());

        rv = CryptokiEx.C_FindObjects(session, hObjects, hObjects.length, objectCount);
        if(rv.intValue() == 0 && objectCount.value > 0)
        {
           System.out.println("C_FindObjects returned: " + rv.intValue());
           System.out.println("Number of objects found: " + objectCount.value);
        }
        else
        {
           System.out.println("C_FindObjects returned: " + rv.intValue());
           System.out.println("NO objects found: ");

        }

        rv = CryptokiEx.C_FindObjectsFinal(session);
        System.out.println("C_FindObjectsFinal returned : " + rv.intValue());

        rv = CryptokiEx.C_SignInit(session, mech, hObjects[0]);
        System.out.println("C_SignInit returned : " + rv.intValue());

        rv = CryptokiEx.C_Sign(session, plain_data.getBytes(), plain_data.length(), signature, signatureLen);
        System.out.println("C_Sign returned : " + rv.intValue());

        System.out.println("PlainText:" + plain_data);
        System.out.println("Hex dump of signature: " + byteArrayToHexString(signature));

        rv = CryptokiEx.C_Logout(session);
        System.out.println("C_Logout returned : " + rv.intValue());

        rv = CryptokiEx.C_CloseSession(session);
        System.out.println("C_CloseSession returned : " + rv.intValue());

        rv = CryptokiEx.C_Finalize(null);
        System.out.println("C_Finalize returned : " + rv.intValue());
    }
    catch (CKR_Exception ex)
```

```
    {
        ex.getMessage();
    }
}

static String byteArrayToHexString(byte in[])
{
        byte ch = 0x00;
        int i = 0;
        if (in == null || in.length <= 0)
        {
                return null;
        }
    String pseudo[] = {"0", "1", "2","3", "4", "5", "6", "7", "8","9", "A", "B", "C", "D", "E", "F"};
        StringBuffer out = new StringBuffer(in.length * 2);
        while (i < in.length)
        {
        ch = (byte) (in[i] & 0xF0); // Strip off high nibble
        ch = (byte) (ch >>> 4);     // shift the bits down
        ch = (byte) (ch & 0x0F);    // must do this is high order bit is on!
        out.append(pseudo[ (int) ch]); // convert the nibble to a String Character
        ch = (byte) (in[i] & 0x0F); // Strip off low nibble
        out.append(pseudo[ (int) ch]); // convert the nibble to a String Character
        i++;
        }
        String rslt = new String(out);
```

KSP Installation

CNG is Microsoft's cryptographic application programming environment (API) replacing the Windows cryptoAPI (CAPI).

CNG stands for Cryptography Next Generation and is applicable to Windows Vista and Windows Server 2008. CNG adds new algorithms along with additional flexibility and functionality, compared with the old API.

Just as SafeNet provides our CSP for applications running in older Windows crypto environments (and JSP for Java), we offer KSP to allow your Vista or Server 2008 client applications to make use of the SafeNet HSM.

To install KSP:

- go to the Ptk-M directory on the CD (or tar),
- open the Win32 or Win64 directory (as appropriate to your system)
- open the CNG directory

- launch the CNG.msi installer.

KSP Configuration Tool

The KSP registration tool KspConfig.exe registers HSM slots for use with CNG. It secures the Password for each HSM slot such that only the user for which the Password was secured is able to un-secure it.

You must already have performed the appliance and HSM configuration steps as described elsewhere in the Ptk-M User Manual. Continue with KSP Configuration, below.

KSP (not CSP) is required in order to use ProtectServer and Protect Toolkit with Microsoft's CNG API.

Only Administrator or members of the Administrators group are to run "KspConfig.exe".
KSP can be used by any application that acquires the context of the KSP.
All users who login and use the applications that acquired the context have access to the KSP.

KspConfig.exe is a simple GUI application that registers HSM slots with CNG.

When you start the program, open the "SafeNet KSP Config" heading, and double-click "Register HSM Slots", then several fields appear in the right-hand pane of the program window. If you have properly configured your ProtectServer, then some of the fields are already populated, including a drop-down list of available slots.

You can then choose to register any of the available slots.

In general, we recommend that you Register By Slot Label (rather than by Slot Number).

1. Go to C:\Program Files\SafeNet\CNG\SafeNet and launch KspConfig.exe (the KSP configuration wizard).
2. In the left-hand pane (tree view) double-click "Register Or View Security Library"
3. In the right-hand pane, browse to the library C:\Program Files\SafeNet\ProtectToolkit M\hsm\cryptoki.dll and click [Register]
4. When the success message appears, click [OK]
5. Return to the left-hand pane and double-click "Register HSM Slots", and click [Next]
6. In the "Slot Password" field, type in the password for the indicated slot.

   To the right of the window, clickthe [Register Slot] button

   to register the slot for Domain/User. A success message appears.
7. Return to the "Domain" pull-down list and select "NT AUTHORITY", supply the password for the slot being registered, and again click Register Slot] to complete theKSP configuration

Once you have the slots registered, you can begin using your client application to perform crypto operations in your HSM Partitions.