

Luna PCI-E 5.0.0 CRN

Document #: 007-011328-001 Rev F

Note Issued on: 2012-05-29



Product Description

SafeNet Luna PCI-E is a hardware cryptographic module providing cryptographic acceleration, hardware key management, and multiple configuration profiles.

Two models of Luna PCI-E are available – password authenticated and PED authenticated - in two performance variants, the Luna PCI-E-1700 or PCI-E-7000 which are capable of 1700 and 7000 (RSA 1024-bit) signings per second respectively , and are otherwise functionally identical.

The most up-to-date version of this Customer Release Notes document is always at:

http://www.securedbysafenet.com/releasenotes/luna/007-011328-001_crn_luna_pci_5-0.pdf

Component Versions

Component	Version
Luna PCI-E firmware	6.2.1
Luna Library (libcryptoki) cryptoki v2.2.0	5.0.0
Lunacm utility	2.3.3
Luna PCI-E 5 Client	5.0
Luna PCI-E 5 driver vkd	5.0.0

Luna Remote Backup HSM	1.0
Luna PED firmware	2.4.0

Battery Switch and Tamper

Previously, customers could encounter a problem with Luna PCI-E if their use-case model is :

- configure the HSM card at a central location, including installing keys and certificates,
- ship the card (not installed) on to its ultimate destination,
- end-user installs in workstation or server of their choice with HSM already populated.

Removing the HSM from the configuring computer caused the HSM to detect a tamper and to clear the Master Tamper Key, repeatedly. This repeated action wore down the non-rechargeable battery. Sliding the battery switch to the disengaged position saved the battery but immediately decommissioned the HSM, destroying the installed objects. Therefore the only way to ship a populated original Luna PCI-E HSM was to ship it inside a computer. This option remains useful in OEM situations where our customers include Luna PCI-E (K6 HSM) as part of an appliance that they sell or lease to their end-customers, where they would want the HSM to tamper if removed from the appliance.

The latest Luna PCI-E card now disables the tamper-on-removal feature. This version can be populated with cryptographic objects, set to Secure Transport Mode, removed from the computer, and stored or shipped without running down the battery. The eventual consumer/customer installs the HSM into a workstation or server of their choice, with all cryptographic objects preserved. With this version of the Luna PCI-E product the battery switch should always remain in the "on" or engaged position.

In summary, Luna PCI-E (the K6 HSM) is now available in two versions, one specifically intended for permanent use in an appliance, and one for general use (tamper-on-removal disabled).

The former, identified by **PART NUMBER 808-000052-001 AND MODEL NUMBER VBD-05-0101** , should have its battery slider switch in the "disengaged" (toward the battery) position while it is being stored and handled, and then must have its battery slider switch moved to the "engaged" (away from the battery) position immediately before installation in your OEM HSM appliance.

The latter, identified by **PART NUMBER 808-000055-001 AND MODEL NUMBER VBD-05-0103** , should have its battery slider switch left in the "engaged" (away from the battery) position.

Luna PCI-E Variant	Battery Engaged	Battery Disengaged
Tamper-on-removal enabled	Objects preserved when Luna PCI-E is not installed in server – BATTERY is rapidly DIScharging! DO NOT attempt populated storage or shipment (with or without Secure Transport Mode)	HSM is decommissioned – all objects rendered unrecoverable
Tamper-on-removal disabled	Objects preserved when Luna PCI-E is not installed in server – Battery is not threatened. Secure Transport Mode is possible.	HSM is decommissioned – all objects rendered unrecoverable

Maximum Asymmetric Performance Needs 25-to-30 Threads

Luna PCI-E 5 has achieved 7000 RSA 1024-bit signings per second, under laboratory conditions, when driven by a multi-threaded application running at least 25 threads on a high-performance server. Additional simultaneous threads are required on less powerful host computers to achieve best performance.

JVM Support

A reference to Java and IBM in the Help might be interpreted to suggest that IBM JVM and the AIX platform are supported in the first Luna PCI-E release. This is not the case.

1. Some ECC-related code introduced in Luna PCI-E 5.0 Luna JSP has a dependency on certain Java classes that exist only in the SUN and OpenJDK JVMs; AND
2. WebSphere uses the IBM JVM; THEREFORE
3. Any application using WebSphere, ECC and the Luna PCI-E 5.0 JSP will break.

A potential fix internalizes certain OpenJDK classes within the Luna provider, thus removing the dependency on a specific JVM. WebSphere and ECC do not currently work with Luna PCI-E 5.0. If this is an issue for you, contact Technical Support.

New Features and Enhancements

Luna PCI-E Version	Reason for Update
5.0	<ul style="list-style-type: none"> • HA (for load balancing on same server) • Secure Transport Mode – protects against tampering while the HSM is in transit • PKI Keys and objects can be migrated from legacy Luna HSMs • Remote Management (Remote PED operation and Remote Backup HSM) • Object storage capacity onboard (2476 RSA 2048 keys) • Support for RSA 8192-bit keys • High Performance ECC • expanded OS support

Server Compatibility

SafeNet tests HSM products on a selection of commonly used servers. We are unable to test on all possible host systems. A lock-up issue related to a bridge component used in Luna PCI-E was detected on some servers at installation of the driver.

Servers tested successfully

*x86 and x64-based Servers (Windows 2003 R2 64,** Windows 2008R2, RedHat Enterprise Linux 5.5 (64),and Intel Solaris 10u9*

Dell T610	- Single card in any of slots 1, 2, or 5. Passes 3-card test.* Slots 3 and 4 fail.
IBM x3650 M2	- Single card in any of slots 1, 2, or 3. Passes 3-card test.* Slot 4 no detect.
Dell R710	- Single card in any of slots 1, 2, 3, or 4. Passes 3-card test.*
HP DL 380 G5	- Single card in any of slots 1, 2, or 3. Passes 3-card test.*
Dell R610	- Single card in any of slots 1, or 2. Passes 2-card test.
HP DL 380 G2 AMD-based	- Single card in any of slots 1, 2, or 3. Passes 3-card test.*
HP DL 380 G7	- Single card in any of slots 1, 2, or 3. Passes 3-card test.*
Cisco UCS C210 M1 server	- Single card in any of slots 1, 2, or 3. Passes 3-card test
Fujitsu Primergy RX 200 S6	- The Luna PCI-E HSM card is not detected in either PCI-e slot.

* On system boot, with 3 Luna HSM cards installed, system might see PCIe training error. If this happens, reboot. Once PCIe training succeeds, system is stable with 3 Luna PCI-E 5.x HSMs.

** One exception was noted for Windows 2003 R2 64-bit, where Luna PCI-E 5 failed in all slots, passed as indicated on all other servers..

Other servers

HP Integrity rx 2660 Intel IA (running HP-UX i11 v2 or v3) - Single card in any of slots 1, or 2. Passes 2-card test.*

Fujitsu SUN Sparc M4000 (running SUN Solaris 10 Sparc) - Single card in slot 1, only. Kernel panic crash in slots 2, 3, or 4.

* On system boot, with 3 Luna HSM cards installed, system might see PCIe training error. If this happens, reboot. Once PCIe training succeeds, system is stable with 3 Luna PCI-E 5.x HSMs.

Migration of Key Material

If you need to migrate key material from other Luna HSM products to Luna PCI-E 5.x, contact SafeNet Technical Support for the Migration instruction document.

KCDSA is Optional

Luna PCI-E 5.x is normally shipped without KCDSA installed. If you require KCDSA mechanism support, an installable capability update is available for purchase. Contact SafeNet Technical Support. Instructions for applying an upgrade are below.

How to Apply an Advanced Configuration Upgrade

If you have purchased a capability upgrade from SafeNet, you should have received the upgrade CUF (capability update file) and the authcode file. The filename convention is <prefix><part #>_<sales order number>. <extension>, and is applicable to all Luna HSMs whose serial numbers are included in your purchase order.

<prefix> is caupdateK3, in most cases.

<part number> is the 900-level price list part number – it begins with “9xx-”.

<sales order number> is a numeric value generated by our order-tracking system, and is unique for every order.

<extension> is one of “txt”, “auth”, “CUF”, or “spkg”, depending upon the part ordered.

Here are instructions to install the upgrade.

You must be logged in with administrator rights.

1. Save the .CUF and authcode files on your computer, in an accessible folder.
2. Open a command prompt window or console session.
3. Go to the Luna software directory.
4. Run lunacm.
5. Log into the HSM as SO.
lunacm:>hsm login
6. Run the update, providing the full file paths to the .CUF file and the authcode.txt file
hsm updateCap -cuf <path_to_update_file> -authcode <path-to_authcode_file>

EXAMPLE

```
lunacm:> hsm updateCap -cuf caupdateK3900-87654321_12345.CUF -authcode
caupdateK3900-87654321_12345.txt
      Capability update passed.
```

```
Command Result : No Error
lunacm:>
```

To verify that the upgrade has been installed, run `hsm showinfo` and check the list below “License Count” for the new capability.

Supported Platforms and API

Luna PCI-E with 32-bit API

OS	32-bit driver	64-bit driver	PKCS#11 2.2.0	CAPI 2.0	CNG	Java 1.6	OpenSSL 0.9.8n
Windows 2003 Enterprise (x86)							
Windows 2003 Enterprise (x86_64)							
Windows Server 2008 R2 Enterprise (x86_64)							
Windows 7 Enterprise (x86)							
Windows 7 Enterprise (x86_64)							

OS	32-bit driver	64-bit driver	PKCS#11 2.2.0	CAPI 2.0	CNG	Java 1.6	OpenSSL 0.9.8n
Red Hat Enterprise Linux 5.5 (x86)							
Red Hat Enterprise Linux 5.5 (x86_64)							
Red Hat Enterprise Linux 6.0 (x86)							
Red Hat Enterprise Linux 6.0 (x86_64)							
Fedora Core10 (x86)							
Fedora Core 10 (x86_64)							
Suse Enterprise Linux 10 SP4 (x86)							
Suse Enterprise Linux 10 SP4 (x86_64)							
Debian 5.0 (x86)							
Intel Solaris 10 (x86)							
Intel Solaris 10 (x86_64)							
Sun Solaris 10 64-bit Sparc							
HP-Itanium 11i V2, V3 64bit							

Luna PCI-E with 64-bit API

OS	32-bit driver	64-bit driver	PKCS#11 2.2.0	CAPI 2.0	CNG	Java 1.6	OpenSSL 0.9.8n
Windows 2003 Enterprise (x86_64)							

OS	32-bit driver	64-bit driver	PKCS#11 2.2.0	CAPI 2.0	CNG	Java 1.6	OpenSSL 0.9.8n
Windows Server 2008 R2 Enterprise (x86_64)							
Windows 7 Enterprise (x86_64)							
Red Hat Enterprise Linux 5.5 (x86_64)							
Red Hat Enterprise Linux 6.0 (x86_64)							
Fedora Core 10 (2.6K) (x86_64)							
Suse Enterprise Linux 10 SP4 (x86_64)							
Debian 5.0 (x86_64)							
Intel Solaris 10 (x86_64)							
Sun Solaris 10 64-bit Sparc							
HP-Itanium 11i V2, V3 64-bit							

(RHEL 6.0 – when 32-bit client is installed on 64-bit OS, lunacm fails to find shared object; install the "libstdc++-4.4.6-3.el6.i686.rpm 32-bit package on 64-bit OS from RHEL6 packages.)

If you encounter problems getting Luna PCI-E 5 to work in your server:

FIRST update your systems with the latest firmware and OS patches from your vendors,

THEN, look on [C3](#) for the latest list of tested platforms, or contact Technical Support if your platform is not on their most current list.

Known Issues

The issues in this table have not been addressed in this release.

Issue	Priority	Synopsis
140070 – Multitoken utility has cosmetic	L	Problem: "Multitoken2 mode rsassign" has been replaced with "multitoken2 mode rsasigver". Although tool works

Issue	Priority	Synopsis
bug in the notes section		as expected, the notes section still says to run the tool with the old syntax (rsassign instead of rsasigver). Workaround: Use “mode rsasigver” instead
135511 – lunacm unable to read information from the K6	M	Problem: Intermittent issue where lunacm reported that it was not able to read information from the HSM. Workaround: Use vreset to get the HSM responding again.
131388 – Using lunacm, the Luna Remote Backup HSM cannot be placed in transport mode	L	Problem: The lunacm command "srk t" is available when addressing a K6 HSM, but not when addressing a G5 HSM such as the Luna Remote Backup HSM. Workaround: Use CKDemo utility to set the Backup HSM into transport mode.
128432 – Both Java5 and java6 not working on HPUX Itanium V2 and V3	M	Problem: Both Java5 and java6 not working on HPUX Itanium V2 and V3 Workaround: Install the PA-RISC version of Java6 instead of the IA64 version – this is able to load the 32-bit libLunaAPI successfully.
128389 – FW6 for PCI needs to be updated to support X9.31 with SHA2 signatures and FIPS 186-3 RSA key generation	H	Problem: FW6 for PCI needs to be updated to support X9.31 with SHA2 signatures and FIPS 186-3 RSA key generation Workaround: None.
127007 – HSM should be able to use certificate objects as keys for increased performance	H	Problem: Performance declines in cases where a write operation occurs. Some round trips to the HSM could be saved in java usage of certificate objects. Because the HSM cannot verify / encrypt using a certificate object we create a public key object to perform the operation. Creating these objects can be slow especially in an HA group. Workaround: N/A
124719 – The function GetConfigurationEntry () in the ChrystokiConfiguration class does not work properly.	M	Problem: The function GetConfigurationEntry() in the ChrystokiConfiguration class does not work properly. This function is used on linux and Unix system to parse the .conf file. If your conf file contains the following

Issue	Priority	Synopsis
		<pre>Chrystoki2 = { LibUNIX64=/dummy; LibUNIX=/usr/lib/libCryptoki2.so; }</pre> <p>GetConfigurationEntry() will incorrectly try to use the LibUNIX64 entry because it only tries to match "LibUNIX" and ignores the rest.</p> <p>This function should be more specific when it is comparing strings.</p> <p>Workaround: Use one or the other entry in .conf file, or adjust the order of the entries so that the desired entry is found first.</p>
123776 – HSM allows login as two different user types simultaneously	H	<p>Problem: The HSM currently allows you to log in as both the CRYPTO_OFFICER and CRYPTO_USER (regular and limited users) simultaneously, in the same session. This leads to some confusion as to who is actually logged in, and may be counter to the PKCS11 spec.</p> <p>Workaround: Manually limit logins.</p>
121689 – Block two-key 3DES as an offered service	H	<p>Problem: To comply with the NIST Key Management Guidelines in SP 800-57, Luna firmware must block 2-key TDES from being offered as a service to calling applications when the module is in FIPS-approved mode.</p> <p>NOTE: NIST has extended the deadline for this to 2013.</p> <p>Workaround: Do not use 2-key Triple DES in your applications.</p>
121682 – Block signing and hashing services based on strength	H	<p>Problem: To comply with the NIST Key Management Guidelines in SP 800-57, Luna firmware must block the following operations from being offered as a service to calling applications when the module is in FIPS-approved mode.</p> <ul style="list-style-type: none"> · SHA-1 as a digest function and when used in digital signature generation, · RSA digital signature generation with modulus size less than 2048 · ECDSA digital signature generation and ECDH with curve order less than 224 · DSA digital signature generation and Diffie-Hellman with N less than 224 & L less than 2048 <p>Firmware can continue to offer signature verification services for all currently approved algorithms post-2010. SHA-1 can continue to be used for HMAC and in NIST-approved or accepted PRNG and key management</p>

Issue	Priority	Synopsis
		<p>techniques (e.g., TLS).</p> <p>Workaround: Avoid using the indicated operations.</p>
120405 – setlegacy domain does not accept default domain in ckdemo	L	<p>Problem: During key migration testing from PCM to PCI5.0, it was found that there is no way to input default which is an empty string for setlegacydomain in ckdemo. In this case, there is no way to do key migration with ckdemo if PCM PW-Auth was using default domain.</p> <p>Workaround: Use lunacm.</p>
119352 – Tamper event for K6 should be in the logs	M	<p>Problem: A tamper event occurs when a Luna PCI-E (K6) card is removed from a server but the event is not recorded in the logs (messages or event viewer). The only way currently to know if the tamper event occurred is to view the dual port output.</p> <p>If SRK is enabled, and a K6 card is removed from the server and later reinserted, the SRV must be restored from the SRK before the HSM can be used again. Without the tamper event in the logs, there is chance the customer might think the card is faulty when they reinsert the card and their application is unable to talk the HSM.</p> <p>Workaround: Maintain awareness of SRK status and tamper status (has the HSM card been removed from a server slot). Verify in the dual port output, in case of doubt.</p>
117029 - PCI5.0: need document or online help to indicate newly added -PKCS8 option for cmu importkey command	M	<p>Problem: Recently supporting pkcs#8 format has been added in cmu importkey command and an new option "PKCS8" must be specified, however there is nowhere to tell the user this.</p> <p>Example:</p> <pre>[admin@localhost bin]# ./cmu importkey -slot=1 -password=userpin -in pkcs8.cer -keyalg RSA -PKCS8 ...Autogenerating a 3DES key for unwrapping -> Handle (52) ...The key was sucessfully unwrapped onto the token -> Handle(53) [admin@localhost bin]#</pre> <p>Workaround:</p>
116976 – cmu generatekeypair for DSA not accept subprime in interaction mode	M	<p>Problem: cmu generatekeypair for DSA not accept subprime in interaction mode while it has been accepted in command line mode.</p> <p>Workaround: Use command-line mode.</p>
111546 – adding/removing a member to an HA	L	<p>Problem: Cannot add/remove a member from an HA group using the serial number of the HSM.</p> <pre>lunacm:> ha r -se 753951 -g myHA -p userpin</pre>

Issue	Priority	Synopsis
group using HSM serial number is broken		<p>Error: Failed to open a user session on slot 0. Command Result : 0x3 (CKR_SLOT_ID_INVALID) lunacm:></p> <p>Workaround: Add/remove with the slot number. lunacm:>ha r -slot 3 -group myHA -password userpin Member 753951 successfully removed from group myHA. New group configuration is:</p> <p>HA Group Label: myHA HA Group Number: 150031 Group Members: 150024, 150031 Needs sync: no</p> <p>Command Result : No Error lunacm:></p>
111091 – Key Migration from K5 to K6: with K5 card kernel panics on Solaris 10 sparc	M	<p>Problem: A Luna PCI 3 (K5e) HSM card is inserted into a Solaris 10 SPARC server where Luna PCI-E 5.0 (K6) is installed. The driver installs. When lunacm is run, the result is a kernel panic and the system shuts down immediately.</p> <p>Workaround: If possible, use a Linux or Windows computer for the migration. The Luna PCI-E (K6) with the migrated material can then be installed into the Solaris 10 SPARC server for ongoing operation (without a co-installed K5e).</p>
110818 – Timeout sometimes occurs during remote backup with append option	M	<p>Problem: During appended remote backup, sometimes got timeout (depending on operator speed) when attempting to re-size a partition on the backup HSM. Looks like this: lunacm:>partition backup backup -slot remote -hostname 172.20.11.130 -port 2222 -debug -partition backuppartition1 -append The partition backuppartition1 will be resized. recv(): timed-out setContainerSize_Client(): failed to read cmd result (-110)</p> <p>Error: failed to resize partition backuppartition1 on remote device. Command Result : 0x5 (CKR_GENERAL_ERROR) lunacm:></p> <p>Workaround: Specify a longer commandtimeout setting when issuing the remote backup command from lunacm.</p>

Issue	Priority	Synopsis
		<p>Here is a workaround example specifying -ct as 20 seconds:</p> <pre>lunacm:>partition backup backup -slot remote -hostname 172.20.11.130 -port 2222 -partition backuppartition1 -append -commandtimeout 20</pre> <p>The partition backuppartition1 will be resized. Verifying that all objects can be backed up... 4 objects will be backed up. 17 objects will not be backed up because they are duplicates. Backing up objects... Cloned object 43 to partition backuppartition1 (new handle 256). Cloned object 44 to partition backuppartition1 (new handle 257). Cloned object 47 to partition backuppartition1 (new handle 260). Cloned object 48 to partition backuppartition1 (new handle 261). Backup Complete. 4 objects have been backed up to partition backuppartition1 on remote device. Command Result : No Error lunacm:></p>
107862 – driver errors when clearing full partition on HSM	M	<p>Problem: After filling up a partition with small key objects (88 byte AES keys), and clearing the partition using the par clear command, these errors appear in syslog.</p> <pre>n 7 16:45:10 harvey kernel: ERR: viper0: _rx: user rsp buf 2 small rxhdr cmd=00, msb(00000035) lsb(0000009c) rxoffset(000035a0) dataleft(00000040) Jan 7 16:45:10 harvey kernel: ERR: viper0: _rx: too small user's response buffer, cmd=0x16(?), size (00006b40) > rxmaxsize (00004408) Jan 7 16:45:10 harvey kernel: ERR: viper0: _rx: user rsp buf 2 small cmd=0x16(?), rxcount(000035a0) rxoffset (000035a0) insize (00000040) blksize (0000359c) Jan 7 16:45:11 harvey kernel: ERR: viper0: _rx: user rsp buf 2 small rxhdr cmd=00, msb(00000035) lsb(0000009c) rxoffset(00006b40) dataleft(00000040)</pre> <p>Workaround: The driver and HSM card are still working so the reported errors don't appear to have consequences - ignore.</p>
107776 – RSA with MGF1 is missing from	M	<p>Problem: During performance testing on jMultitoken, we found RSA with MGF1 algorithms were missing from jMultitoken cross all supported clients. We don't support</p>

Issue	Priority	Synopsis
jMultitoken		<p>RSA with MGF1 for small key sizes (256 and 512), but the HSM does support key size 1024 and larger.</p> <p>Workaround: None.</p>
105873 – lunacm command syntax summary not consistent	L	<p>Problem: The command syntax summary that is presented when the user types a lunacm command followed by "?" is not consistent for all lunacm commands.</p> <p>Workaround: None.</p>
105218 – Handling of PEDid parameter is inconsistent or confusing	L	<p>Problem: Currently, whether an application uses the remote or the local PED is determined by the existence of the PEDid=[0 1] parameter in the 'Luna' section of Crystoki.conf. If this parameter does not exist, applications will always try to use the local PED, even if one is not attached. There is currently no way of setting this through any of the applications (lunacm or ckdemo), so the user must manually edit this file - not a preferred method.</p> <p>Lunacm, ckdemo, and multitoken all allow the user to specify the PED id, either on the command line or via a menu selection, but this works only for one specific session in the given application.</p> <p>Also, commands initrpv and deleterpv are executed only on a locally-attached PED. However, the applications which invoke these functions will simply use whatever PED id is currently specified for that session (or the default from Crystoki.conf). So these commands might incorrectly attempt to invoke a remote ped..</p> <p>Workaround: Modify the configuration file, or specify at the command line for each instance.</p>
104893 – should hide PED command when password based configuration has been used	L	<p>Problem: Some lunacm commands are hidden if they are not applicable (example: the "srk" command is not presented if no external MTK capability is enabled), but others are not. For consistent user interface, we should present only commands and options that can be used in the current situation and with current configuration.</p> <p>Workaround: None.</p>

Addressed Issues

This is the first release of this product. Therefore, there were no previously existing issues to record here.

Information is subject to change without notice. Copyright 2009-2012. All rights reserved.

Luna and the SafeNet logos are registered trademarks of SafeNet Inc.

Document created: 2011-10-21

Document last updated: 2012-05-29

007-011328-001 Rev F