THE
DATA
PROTECTION
COMPANY

SafeNet Customer Support Contacts:
Web: hhttp://support.safenet-inc.com
Email: support@safenet-inc.com

Luna SA 4.4.0

CUSTOMER RELEASE NOTES

Document part number: 007-010090-001 Revision B
Release notes issued on: 11 November 2011

Note The most up-to-date version of this document is available at the following location: http://www.securedbysafenet.com/releasenotes/luna/crn_luna_sa_4-4.pdf

Product description

SafeNet Luna SA is a network-attached hardware security appliance providing cryptographic acceleration, hardware key management, and multiple configuration profiles.

Component versions

Note Luna SA 4.4.0 does not support legacy 2U appliances. Luna SA 4.3.2 is the last release to suppport the 2U appliance. Do not attempt to upgrade 2U Luna SA appliances to release 4.4.0. The outcome would not be a tested or supported configuration. Release 4.4.0 applies to the current, RoHS-compliant 1U Luna SA only.

Component	1U
HSM:	K5
Card Reader	USB
HSM Firmware:	4.6.1 or 4.6.8 (see Note 1)
G3 Backup Token	4.5.3, 4.6.8, or 4.8.1 (see Note 2)
G4 Backup Token	4.5.3, 4.6.8, or 4.8.1 (see Note 2)
Luna CA4 Token	4.6.8
Luna PCM KE Token	4.6.8
PED Workstation software (requires Remote PED) [optional]	1.0
PED I migration	1.14
PED I	1.12
PED II	2.0.2
IKey (for PED II)	1000

Note 1

You can use backup tokens at firmware 4.5.3 with Luna SA at firmware 4.6.8 or 4.8.1, provided you do not use the ARIA cipher (which was not supported in 4.5.3). However, we generally recommend that you update to token firmware 4.8.1.

Note 2

Appliance software 4.4.0 requires installed HSM firmware 4.6.8 or 4.8.1. Both firmware versions are FIPS-validated.

Software upgrade paths

The following table lists the upgrade paths for 1U Luna SA appliances running release 4.2.0 or higher software.

Component	From Version	Directly To Version
Client software	4.2.0, 4.3.0	4.4.0
Appliance software	4.2.0, 4.2.3, 4.2.5, 4.3.2	4.4.0
HSM firmware	4.6.1*, 4.6.7, 4.6.8*	4.8.1 (4.6.8*)

If your Luna SA equipment is at any other starting point, please refer to the Luna SA 4.2 CRN and update instructions in order to bring your system to that approved (tested and supported) starting point before you begin the upgrade to Luna SA 4.4.0 and firmware 4.6.8 or 4.8.1. Otherwise, contact SafeNet Customer Support.

Legacy 2U models of Luna SA (with the orange front-panel-cover) are not supported for this release. Do not attempt to update the old 2U models. For FIPS compliance, Luna SA 4.3.2 and firmware 4.6.8 were your last stop.

Firmware upgrade paths

The tables below present your upgrade options depending on whether you start with a brand-new Luna SA 4.4.0 appliance or you start with an older version and install the 4.4.0 update.

Luna SA 4.4.0 ITEM	[Previously] Installed Software	Supported (new) System Software	Included firmware	Installed firmware	Supported firmware
New appliance (from factory)	4.4.0	4.4.0	4.6.8 with optional 4.8.1	4.6.8	4.6.8 or 4.8.1
Update package	4.2.0, 4.2.3, 4.2.5, 4.3.2	4.4.0	4.8.1 option only	4.6.1, 4.6.7, 4.6.8	4.6.8 or 4.8.1

New systems are shipped with firmware 4.6.8 installed and with [optional] firmware 4.8.1 already in the “waiting area” on the appliance. New features like Remote PED require firmware 4.8.1. You can keep firmware 4.6.8 if you don’t want Remote PED. You cannot keep an earlier firmware (such as 4.6.1) and use software 4.4.0 at all.

In general, if update software includes firmware, then that firmware displaces whatever firmware package is in the appliance’s “waiting area”. Therefore, it is possible to have installed HSM firmware of one version and optional/waiting firmware of another version. It is not possible to have more than one optional/waiting version.

Update 4.4.0 software includes ONLY the [optional] 4.8.1 firmware, which it loads into the “waiting area”. So after you install the upgrade appliance software your HSM firmware is whatever version it was before the update and the optional firmware in the appliance’s waiting area is 4.8.1 only.

Upgrade path for firmware 4.6.8

Start	Intermediate via s/w update 4.3.2	End
4.6.1	4.6.8	4.6.8

Upgrade path for firmware 4.8.1

Start	End
4.6.1 or 4.6.7 or 4.6.8	4.8.1

Luna SA 4 hardware refresh

Due to end-of-life or near end-of-life conditions on several components, a new hardware variant of the Luna SA 4 platform was released in July 2011. As a result of the hardware refresh, you must use new part numbers when ordering the Luna SA 4 product. The old part numbers are no longer valid. For more information, see "Hardware revisions and part numbers" below.

The hardware refresh has introduced some minor changes to the operational behavior of the product, as described in the following sections:

SNMP enabled by default

SNMP is enabled by default on the hardware-refresh platform.

Support added for gigabit Ethernet

The Ethernet ports now support 10 Mbps, 100 Mbps, and 1000 Mbps link speeds.

New network LED behavior

The following table describes the behavior of the network status LEDs on the hardware-refresh platform.

LED color	LED state	Ethernet link and activity
Green	Blinking	100 Mbps or 1000 Mbps link speed
	Steady on	Link established. Communication activity not detected.

Hardware revisions and part numbers

SafeNet may occasionally make minor changes to the hardware components used to manufacture the appliance for cost or availability reasons. For example, if the supply of one the original components used to manufacture the appliance becomes limited, the original component may be replaced with an equivalent, but more widely available component. Although these minor hardware changes do not affect how the appliance behaves or operates, any hardware change triggers a change in the product revision. A product may go through several hardware revisions during its lifecycle. Note, however, that for any given part number, all revisions of that part number are functionally equivalent. For example, there is no operational difference between revisions B and D of part number 808-000043-001.

In general, the following rules apply:

- If the hardware change does not affect how the product behaves or operates, the part number remains the same. Only the revision is changed.
- If the hardware change affects how the appliance behaves or operates, the hardware is assigned a new part number.

Notes about this release

Luna SP

Luna SP is a special implementation that resides on a base Luna SA system. Versions of Luna SP older than 2.0.4 are not compatible with Luna SA 4.4.0. If you intend to update the underlying Luna SA platform to 4.4.0, then you must also update Luna SP to at least version 2.0.4.

SafeNet phasing out MD5 in Luna HSM products

MD5 and SHA-1 digest algorithms have seen widespread use for the past decade or more, but are beginning to show their age. Due to advancing technology, exploits against these algorithms that were once considered theoretical are now becoming feasible in certain circumstances. In particular, a practical exploit of MD5 vulnerabilities that would allow an attacker to create a bogus document with a MD5 digest matching that of a legitimate document has recently been demonstrated and published. There has been no demonstrated equivalent exploit of SHA-1 yet. It is likely, however, that researchers will be working to find such an exploit over the next several months. As a result, SafeNet has adopted the goal of emplacing SHA-256 as the default digest standard for our HSM client and appliance software, starting with the Luna SA 4.4 release.

MD5 has been used as the digest function in the Luna client and appliance software for digital signature and authentication purposes. MD5 has **never** been used within the HSM firmware, for reasons of FIPS 140-2 compliance.

Due to existing standards and technology limitations, it is currently not possible to adopt SHA-256 throughout the Luna product software. Therefore, in the short to medium term, SHA-1 will replace MD5 as the digest used for all client and appliance signature and authentication purposes. The intention is to replace SHA-1 with SHA-256 as standards are updated and as technology allows, with the goal to complete this replacement within twelve months.

SafeNet recommends that customers review their use of certificates from their own and trusted third-party sources, and consider renewing or replacing certificates that were created using MD5. This recommendation includes a revisit of the Java keystore for Java 1.6.0_11 (the latest version at the time of writing) and earlier. If customers are using Java 1.6.0_11 or earlier versions, be aware many of the supplied certificates use MD5withRSA. SafeNet also suggests that customers consider eliminating the use of the MD5 digest in their own application software, taking into mind any compatibility considerations.

Help in Linux

If the Help links do not appear to work, try renaming the /Content directory to /content.

SNMP security changes

The SNMP security requirements have been strengthened in this release as follows:

- support for SNMP v2c has been removed. Only SNMP v3 is now supported.
- support for the MD5 authentication protocol has been removed. Only SHA is now supported.
- support for the DES privacy protocol has been removed. Only AES is now supported.

When executing the **sysconf snmp** command, the **-authProtocol** and **-privProtocol** parameters default to SHA and AES, respectively, so that the following commands are equivalent:

- sysconf snmp user a -secname myname -authpassword mypwd -privpassword mypwd -authpro SHA -privpro AES
- sysconf snmp user a -secname myname -authpassword mypwd -privpassword mypwd

New features and enhancements

Luna SA Version	Reason for Update
4.4	• PKI Bundles – supports the use of Luna PCM CA4 tokens via the front-panel card reader – appears as a removable HSM Partition. • Enhanced (secure/trusted) NTP – ability to authenticate and use trusted NTP sources. • Remote PED Management - securely present PED Key authentication to a remotely located HSM. • HA AutoRecovery – recovery by HA group members is now automatic. • Upgrade of Card-reader Firmware – new commands added. • Remote System Logging – to a UNIX/Linux system that supports the service. • Named Administrative User Accounts – appliance ‘admin” can now create named users and assign administrative roles to them (admin, operator, monitor). • MD5 is no longer supported, for security reasons.
4.3	• Support for Brainpool algorithms • Support for ARIA block cipher • Itanium platform • Various fixes (see the Addressed Issues section, below, and the two patch releases 4.2.2 and 4.2.3)
4.2.3 (patch)	• Adds to JCA the ability to sign certificates with SHA2 algorithms (sha224withRSA, sha256withRSA, sha384withRSA, and sha512withRSA)
4.2.2 (patch)	• Fixes to client software to improve handling of condition where Luna SA appliance(s) become unavailable (disconnection) and client continues to seek valid slot
4.2	• Support of 800 NTLS connections per second • Client/SDK and 32/64-bit libraries combined on one distribution CD (or tar) • Support for Microsoft Cryptographic Next Generation (CNG) key storage provider • HSM is validated to FIPS 140-2 level 3 • Discontinued support for: — JRE 1.3, — Windows 2000, — Solaris 8, — RH Linux Enterprise 3 (kernel 2.4.x), — AIX 5.1 and — AIX 5.2 • Various fixes (see the Addressed Issues section of the Luna SA 4.2.0 Customer Release Notes)

Luna SA Version	Reason for Update
4.1	• Enhanced MIB Support • NTLS performance improvement • Fix to token backup issue (from patch 4.0.2 release) • Fix to Public Key authentication bug • New f/w 4.6.1 to meet FIPS validation • Added Windows 2003 64-bit library support • Officially added AIX 5.3 64-bit library support • Updated SSH • Tested with SP 2.0 • Additional configurations for Key Export (RA) with 20 partitions/80 objects each

Versions older than 4.1.0 are listed in a similar table in previous editions of Luna SA Customer Release Notes.

Summary of release support

Luna SA 4.4.0 Client software

O/S & version	O/S kernel	32-bit library	64-bit library
Win2003	32	X	
Win2003	64	X	X
Win 2008 Server	32	X	
Win 2008 Server	64		X
Solaris 9 SPARC	32	X	
Solaris 9 SPARC	64	X	X
Solaris 10 SPARC	64	X	X
Solaris 10 x86	32		
Solaris 10 x86	64		
RH Ent 4 2.6.x	32	X	
RH Ent 4 2.6.x	64	X	X
RH Ent 5 2.6.x	32	X	
RH Ent 5 2.6.x	64	X	X
AIX 5.3	32	X	
AIX 5.3	64	X	X
HP-UX 11i (11.11) PA-RISC	64	X	X
HP-UX 11i V2 (11.23) Itanium	64	X	X

API support - 32-bit client

OS	PKCS #11 v2.01/2.20	MS CSP 2.0	Java 1.4.x/1.5.x	OpenSSL 0.9.8e
Win2003	X	X	X	
Win2008	X	X	X	
Solaris 9 SPARC	X		X	X
Solaris 10 SPARC	X		X	X
Solaris 10 x86	X		X	X
Ent 4 2.6.x	X		X	X
Ent 5 2.6.x	X		X	X
HP-UX 11i PA-RISC	X		X	
AIX 5.3	X		X	

API support - 64-bit client

OS	PKCS #11 v 2.01 64-bit	MS CSP 2.0	Java 1.5.x/1.6.x 64 bit	OpenSSL 0.9.8e	CNG
Win2003	X	X	X		
Windows 2008 Server	X		X		X
Solaris 9 SPARC	X		X		
Solaris 10 SPARC	X		X		
Solaris 10 x86					
Ent 4 2.6.x	X		X		
Ent 5 2.6.x	X		X		
AIX 5.3	X		X		
HP-UX 11i PA-RISC					
HP-UX 11i Itanium	X		X		

Remote PED Server OS Support

OS	Driver	App
Win2003 Standard / Enterprise	32/64	32*
Windows Vista	32/64	32*
Windows XP Professional	32	32*

* 32-bit app will run on 64-bit OS

Firmware versions

Supported firmware versions

HSM/Token	Luna SA Version										
	3.0	**3.0.1**	**3.1.0**	**3.2.0**	**3.2.3** **3.2.4**	**3.3.0**	**4.0**	**4.1** **4.2**	**4.3.0**	**4.3.2**	**4.4.0**
Luna SA KeyCard firmware	4.2.1	4.2.4	4.1.0 or 4.4.0	4.1.0 or 4.5.1	4.1.0 or 4.5.2	4.1.0 or 4.5.3	4.5.3 or 4.6.0	4.5.3 or 4.6.1	4.6.7	4.6.8	4.6.8 or 4.8.1
Luna SA (G3 and G4) Backup Token firmware	4.2.1	4.2.4	4.1.0 or 4.4.0	4.1.0 or 4.5.1	4.1.0 or 4.5.2	4.1.0 or 4.5.3	4.5.3	4.5.3	4.6.7 or 4.5.3	4.6.8 or 4.5.3	4.8.1 or 4.6.8 or 4.5.3

CD contents and compatibility

Contents of Luna SA distribution CDs

Client Software, SDK, and Documentation (32-bit and 64-bit) [CD# 700-00187-xxx]	Luna SA Appliance Software [CD# 700-00188-xxx]
Libraries and utilities required for any computer that is to be a Luna SA Client, connecting to a Luna SA appliance. Additional application interfaces for integration of Luna SA with third- party applications. Documents for the user and administrator. Logging utility. Code samples for software developers.	Luna SA appliance software. HSM and token firmware update code.

Software Version Compatibility by Luna SA Release

Luna SA Release	Client software version [CD#]	Software Development Kit version [CD#]	Luna SA Appliance s\w version [CD#]
4.4.0	4.4.0 (32-and 64-bit) [700-00187-003]	[combined into client CD]	4.4.0 [700-00188-003]
4.3.0	4.3.0 (32-and 64-bit) [700-00187-002]	[combined into client CD]	4.3.0 [700-00188-002]
4.2.0	4.2.0 (32-and 64-bit) [700-00187-001]	[combined into client CD]	4.2.0 [700-00188-001]
4.1.0	4.1.0 (32-bit) [900506-037 Rev B] 4.1.0 (64-bit) [006901-002]	4.1.0 (32-bit) [900536-037] 4.1.0 (64-bit) [006903-002]	4.1.0 [900552-038]
Versions older than 4.1.0 are listed in a similar table in previous editions of Luna SA Customer Release Notes.			

Known issues

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

Priority	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

Issue	Priority	Synopsis
(71997) [docs] miscellaneous Luna SA 4.4 doc errors	L	**Problem:** In "B - Administration & Maintenance - Remote PED - using", the link to "Initialize the HSM" is broken. When you click on Syslog - Remotehost commands in the "D - Reference" section, there is a blank entry in the TOC called "New Entry". Not all the commands associated with the "token pcmvisibility" section are accounted for in the Reference section. "ChangePin", "Clone", "listDeployed", and "ResetPin" are all missing pages. **Workaround:** Missing commands are shown in the lush syntax display if you type the command followed by “?”.. To be addressed in a future release.
(71997) [docs] User role list in docs needs to be updated for new commands	L	**Problem:** The user role list (user_accounts_and_privileges.htm) needs to be updated for the new commands included with Luna SA 4.4 (token pcmvisibility, syslog remotehost, etc.). **Workaround:** N/A To be addressed in a future release.
(71996) [docs] Should be section on setting up remote logging	L	**Problem:** There is no specific section in the help on remote logging. It is mentioned in the "Major Changes" section of the help and the commands are listed in the reference section, but there should be a section in "B - Administration & Maintenance" on how to set it up. **Workaround:** N/A To be addressed in a future release.
(71024) can't list public keys for created users	L	**Problem:** lunash:>sysconf setAdmin publickey list User must be admin, monitor or operator Command Result : 65535 (Luna Shell execution) Functionality is otherwise OK! **Workaround:** N/A To be addressed in a future release.

Issue	Priority	Synopsis
(69852) ugly error when attempting to start NTLS with no key/cert generated	L	**Problem:** NOTICE: The NTLS service must be restarted for new settings to take effect. If you are sure that you wish to restart NTLS, then type 'proceed', otherwise ty pe 'quit' > proceed Proceeding... Restarting NTLS service... Stopping ntls: [OK] Error opening Certificate /usr/lunasa/vts/server/server.pem 30136:error:02001002:system library:fopen:No such file or directory:bss_file.c:2 78:fopen('/usr/lunasa/vts/server/server.pem','r') 30136:error:20074002:BIO routines:FILE_CTRL:system lib:bss_file.c:280: unable to load certificate **Workaround:** ALWAYS generate the server certificate BEFORE attempting to start NTLS. Improved handling to be addressed in a future release.
(68674) error handling in sysconf drift commands	L	**Problem:** There are some issues with the way handles incorrect user values with the "sysconf drift" commands. When supplying "sysconf drift start", "sysconf drift stop", or "sysconf drift init" without any arguments, you will not get the standard lunash list of options (it should tell you to supply the -c argument): [merlot101] lunash:&gt;sysconf d start The format of the given time is invalid. Exiting. Command Result : 65535 (Luna Shell execution) When you have the drift meaurement started, and you fail to supply the -c argument for "sysconf drift start", the error message will not supply the time: [merlot101] lunash>sysconf d start Time drift measurements was already started on . Use the 'sysconf drift reset' command to restart them. Command Result : 65535 (Luna Shell execution) [merlot101] lunash> When you input invalid characters (not numbers) for the -c option (in start, stop, or init), it will report each bad character on its own line, which is cumbersome. It should report the argument on one line as "token not recognized" or something like that. [merlot101] lunash:&gt;sysconf d start -c AAAAAAA Syntax Error: currentprecisetime parameter AAAAAAA for option -currentprecisetime contains invalid character 'A' Syntax Error: currentprecisetime parameter AAAAAAA for option -currentprecisetime contains invalid character 'A' Syntax Error: currentprecisetime parameter AAAAAAA for option -currentprecisetime contains invalid character 'A' Syntax Error: currentprecisetime parameter AAAAAAA for option -…. Etc. **Workaround:** N/A To be addressed in a future release.
(68296) Can't see CSP on Win 2003 64-bit	H	**Problem:** Problem with CSP with a 64 -bit install of Luna SA Software on a 64 -bit Windows 2003 Enterprise machine. The test machines were not populating the 'Luna' entries in the 64 -bit key folders: HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > Defaults > Provider However the 32 bit folder: HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > Microsoft > Cryptography > Defaults > Provider was being populated. The above folder was being deleted and re-added with un-installation and re-installation. No logging was taking place even after the register.exe command was run. **Workaround:** You must have Windows .NET framework (version 2.0 or higher) installed/enabled to use the CSP/KSP/CNG on Windows 2003 64-bit. To be addressed in a future release.

Issue	Priority	Synopsis
(68121) HPUX PA-RISC uninstall can't find SDK or JSP uninstall scripts	L	**Problem:** The Luna SA client's uninstall script can't invoke the SDK or jsp component uninstall scripts. Easy workaround, just run those scripts within the SDK or javasp directories. ======= 02/25/09 11:41:20 EST END swremove SESSION (non-interactive) (jobid=moe-1523) Uninstalled lunaconf Would you like to uninstall the Luna JSP for Luna SA? (y/n) y sh: unin_jsp.sh: not found. Would you like to uninstall the SDK for Luna SA? (y/n) y sh: unin_sdk.sh: not found. **Workaround:** Run those scripts within the SDK or javasp directories. To be addressed in a future release.
(65291) incompatiblites between Luna SA kernel & ntpd 4.2.4 cause error messages	L	**Problem:** Odd entries in the NTP log. It seems that they are the result of running newer versions of NTP on old kernels. Some of the messages seen are: 29 Dec 13:18:07 ntpd[14713]: getaddrinfo: "::1" invalid host address, ignored 29 Dec 22:28:37 ntpd[14713]: kernel time sync error 0001 29 Dec 23:02:46 ntpd[14713]: kernel time sync error 0001 29 Dec 23:17:11 ntpd[14713]: offset -0.010709 sec freq -77.465 ppm error 0.003272 poll 10 Despite these errors, the time seems to be accurate. **Workaround:** ignore To be addressed in a future release.
(64704) HSM zeroize de-assigns PKI bundles partitions from clients	L	**Problem:** When the HSM gets zeroized, all partitions get de-assigned from all clients in the ntls database. This is correct behaviour because the HSM zeroizing means all partitions are gone. However, any PKI bundles tokens assigned to the client also get de-assigned. This is incorrect behaviour because those tokens are independent of the HSM and are still present even if the K5 gets zeroized. **Workaround:** N/A To be addressed in a future release.
(64662) debug output in CMU	L	**Problem:** If you type C:\Program Files\LunaSA>cmu -? the first line of the command list is spurious output. nExitCode returned was =0 Certificate Management Utility V1.3 ? - Display this list certify - Create a certificate from a PKCS #10 certificate request delete - Delete an object on an HSM export - Export an X.509 certificate from an HSM to a file generatekeypair - Generate an asymmetric key pair on an HSM getattribute - Retrieve readable attribute(s) from an object on an HSM import - Import an X.509 certificate onto an HSM list - Locate and list sets of objects on an HSM requestcertificate - Create a PKCS #10 certificate request

Issue	Priority	Synopsis
(64313) some lush commands cause an hsm reset and thus will close remote PED connection	M	**Problem:** Several lunash commands result in a vreset. A side effect of this is the closure of any remote PED connection. They are: hsm factoryreset (also erases RPV - a new one must be created before a remote PED connection can be opened) hsm update capability hsm debug mode set recovering the admin account **Workaround:** n/a Working as designed. Documented in Help. No further action.
(64225) misleading message on unregistered client trying to connect to ntls	L	**Problem:** Logging when trying to connect an unregistered client to an SA the final error is a bit misleading - it implies the client connected successfully and then disconnected. Dec 3 08:51:05 viper18 vtsd: Client address trying to connect is 172.20.11.71 Dec 3 08:51:05 viper18 vtsd: Error message is : error:14094412:SSL routines:SSL3_READ_BYTES:sslv3 alert bad certificate Dec 3 08:51:05 viper18 vtsd: Error during SSL accept (0) Dec 3 08:51:07 viper18 vtsd: NTLA client has disconnected. In this case something more appropriate like "Unknown NTLA client 172.20.11.71 failed to connect" would be better. Or even nothing. **Workaround:** None. Unregistered clients cannot actually connect, even briefly. To be addressed in a future release.
(64112) token PED commands fail while there is an active PED server connection	M	**Problem:** Luna SA 4.4 does not support remote PED for commications with backup and or PKI bundles tokens. However, if you have a remote PED server connection open for administering the K5, any command issued to PKI bundles or the backup tokens while that connection is active will fail. You must close your remote PED connection before they can be successful. It would be more convenient if token commands were sent directly to a local PED. **Workaround:** Close Remote PED connection before issuing commands to backup or PKI tokens. To be addressed in a future release.
(64106) PED prompt originating from client not propagated to remote PED	M	**Problem:** In some instances a client can cause a PED prompt to the Luna SA. One of those is a login against a partition that does not have activation enabled. This will cause a PED prompt on the Luna SA. The Activate MofN API call, which can also be called from the client, causes a green key PED prompt. If the Luna SA in question is connected to a remote PED, these client PED prompts will NOT be sent to the remote PED. They time out and return an error. **Workaround:** None. If your preference is to have PED prompts on every login (no Activation), then you currently cannot use Remote PED. To be addressed in a future release.
(63973) Dual lib entries in Chrystoki.conf prevent sample code from running in Sol x86 64-bit	L	**Problem:** The ckdemo sample included with x86 Sol 64 -bit will compile, but when run it attempts to look for /usr/lunasa/lib/libCryptoki2.so instead of libCryptoki2_64.so. This is because the first lib entry in the Chrystoki.conf file is LibUNIX and not LibUNIX64 (LibUNIX64 is the second entry). Commenting or deleting the 32 lib line will correct this and produces no side effect to other apps. Other apps also run without error without any changes to Crystoki.conf. **Workaround:** Remove the 32-bit entry from Chrystoki.conf To be addressed in a future release.

Issue	Priority	Synopsis
(63957) PED server takes ~20 seconds before it detects it's disconnected from PED	L	**Problem:** If you start your PED server with your PED in remote mode, then switch the PED to local mode - the PED disconnects from the PED server. But repeated "pedserver -m show" commands still show a connection to the PED, for about 20 seconds. Then it will show disconnected. It should show "disconnected" as soon as the PED is put into local mode. Similarly, when you switch back from local to remote PED mode on the PED, it takes about 20 seconds before the PED server shows that it's connected. **Workaround:** None – just wait the 20 seconds To be addressed in a future release.
(63874) multitoken -p (packet size) doesn't seem to do anything	L	**Problem:** Tried using the -p option to sign different packet sizes with rsa signature mechanisms. But multitoken always returned the same performance no matter what packet size we specified, which doesn't seem correct. We also notice the same thing on symmetric operations. C:\Program Files\LunaSA&gt;multitoken2 -mode aesenc -key 192 -p 1000000 -s 1,1,1,1,1,1,1 Initializing library...Finished Initializing ...done. This program will not initialize the tokens. You will be prompted for authentication data for the tokens in the following slots: slot 1 Do you wish to continue? Enter 'y' or 'n': y Constructing thread objects. Logging in to tokens... slot 1... Enter password: userpin Creating test threads. Press ENTER to terminate testing. AES ECB encryption, KBytes/second: 0 1 2 3 4 5 6 | total ----- ----- ----- ----- ----- ----- ----- | ----- 127.6 114.8 114.8 127.6 127.6 102.0 114.8 | 829.1 **Workaround:** None To be addressed in a future release.
(63734) HA - Client can't detect failure on idle appliance	H	**Problem:** Current HA client design is such that only a member partition that is doing work can be detected when it fails. For example, running multitoken against an HA slot - all members are "active" and sharing in the signing, so if one of them fails it's detected immediately. This detection is used to trigger the automatic recovery. If for some reason, one of the members is NOT doing any signing (for example, it's not in synch) - then if it fails, the client will NOT detect this. This might become significant for customers who wish to use RA tokens (or partitions) in HA mode – supported beginning in Luna SA 4.4.0 via the ability to turn HA group member synchronization off. In this scenario, a customer wants an HA RA member to be generating keypairs and wrapping them off, while the other member(s) do nothing (since synchronization is turned off). BUT the customer wants the application to fail over to one of the other HA members if the partition doing the wrapping fails. This works. HOWEVER, if the other HA member(s) have failed in the meantime, this will never be detected. **Workaround:** None To be addressed in a future release.

Issue	Priority	Synopsis
(63527) Signing against HA group of RA tokens generates errors in Java	M	Problem: I can run multitoken signing against an HA group of RA tokens, as long as synchronization is turned off. That way, it doesn't attempt to clone the keys over & just signs on the primary. When I run the same test on jMultitoken, I get: Exception on generating key pair: com.chrysalis.crypto.LunaCryptokiException:function 'C_GenerateKeyPair' returns 0x8000000b Possibly the library is handling session objects differently than token objects jMulitoken (and our JCA/JCE in general) uses session objects, multitoken uses token objects Workaround: (see above) To be addressed in a future release.
(62575) CNG should be installed under main LunaSA pat	L	**Problem:** Current CNG install path is: C:\Program Files\SAFENET\<files> To keep things together and organized, install path should be: C:\Program Files\LunaSA\CNG\<files> **Workaround:** N/A To be addressed in a future release.
(39873) CNG/KSP Machine Owned Keys Need To Be Visible By Multiple Machines In Server 2008 Cluster	H	**Problem:** Can’t use Luna SA 4.4.0 and KSP with Windows Server 2008 Cluster. When a key pair is created by CertServices on Server 2008, the key pairs are created as machine owned keys making them visible only to the Server 2008 machine where they were generated from. This is by design and should continue to behave in this manner. However, if the CertServices application is within a Windows cluster, then the keys must be made visible to the other machines in the cluster. The ksputil intended to make the keys visible does not work. Bug was fixed too late in SA 4.4 product quality release cycle. **Workaround:** Contact SafeNet for a patch release that fixes ksputil and allows you to use Windows Server Clustering with Luna SA 4.4.0 Patch to be included in a future release.
(33641) windows install script should have option to install KSP	L	**Problem:** There should be an option in the main install script in windows to install KSP in the same way you install JSP and CSP. This would be more convenient than running a separate executable after the main install is finished. **Workaround:** Run separate installation as currently instructed. To be addressed in a future release.
(31353) Signing context is terminated if we pass small buffer in C_Sign() API	H	**Problem:** Pass buffer of smaller length than expected in the C_Sign() . An error message is returned "Buffer too small" and terminates the Signing context. 1. C_Initialise() 2. C_OpenSession() 3. C_FindObjectInit()---for finding the private key 4. C_FinObjects() 5. C_SignInit()---pass the required mechnism 6. C_Sign()---with buffer of smaller length than expected. Observed:An error message "Buffer too small" is displayed and Signing context is deleted. Next call to C_Sign() does not work. Expected: An error message should be displayed " Buffer too small" but proper length should be returned in the length field. And subsequent call to C_Sign() shoudl work without calling C_SignInit(). **Workaround:** Avoid passing wrong size content to C_Sign() To be addressed in a future release.

Issue	Priority	Synopsis
(27667) K5 restore - LUNA_RET_SM_ACCESS_DOES_NOT_VALIDATE	M	**Problem:** When performing a restore/backup commands from a second shell can corrupt process During a restore on K5 lunaSP device the error LUNA_RET_SM_ACCESS_DOES_NOT_VALIDATE was returned. To reproduce: 1. partition restore comamnd start when backup start it take long long time to restore object (3-4 time slower than in K3). 2. open a new shell (over ssh) on the same box 3. partition showContents during restore showcontents will work perfectly but all object from backup after issuing the command will fail to restore. Object "CertificateTest_TESTKEY7_TSTAPP_113DDEA470263AF0" (handle 49) cloned to handle 165 on target Object "PublicKeyTest_LOCENC KEY_LOCENC_D8D7579A29F9FA1D" (handle 52) cloned to handle 168 on target Object "CertificateTest_LOCENC KEY_LOCENC_D8D7579A29F9FA1D" (handle 53) cloned to handle 169 on target Object "StaticKeyTest_TINT1_SIC_0000000000000001" (handle 54) cloned to handle 170 on target Object "StaticKeyTest_TINT2_SIC_0000000000000002" (handle 55) cloned to handle 171 on target Object "StaticKeyTest_TINT3_SIC_0000000000000003" (handle 56) cloned to handle 172 on target Object "StaticKeyTest_TINT32_SIC_0000000000000003" (handle 57) cloned to handle 173 on target Object "StaticKeyTest_TINT4_SIC_0000000000000004" (handle 58) cloned to handle 174 on target Object "StaticKeyTest_TINT42_SIC_0000000000000004" (handle 59) cloned to handle 175 on target Object "PrivateKeyTest_TESTKEY1_TSTAPP_C4DADD48C5A849E3" (handle 60) cloned to handle 176 on target Object "PublicKeyProd_SNB0_SIC_90DCEB7EBC54F247" (handle 61) cloned to handle 177 on target Object "CertificateProd_SNB0_SIC_90DCEB7EBC54F247" (handle 62) cloned to handle 178 on target... etc. **Workaround:** Avoid issuing commands from two shell connections. To be addressed in a future release.

Addressed issues

Issue	Priority	Synopsis
(65702) All usage of MD5 must be discontinued immediately	C	**Problem:** MD5 has been found to subject to an easily exploitable flaw which allows collisions to be found that permit modified data to be signed in place of the legitimate data. MD5 is currently used as the digest algorithm in the certificates generated for appliances and clients. Because of the proven exploitation, the use of MD5 must be discontinued immediately. The digest algorithm must now be set as SHA-256. SHA-1 is also no longer acceptable for certificates used in our products because it also has known flaws and it is only a matter of time before the successful exploitation in MD5 is replicated with SHA-1. Note that despite what the SW component shows above, this applies to both appliance and client. **Fixed.**
(63280) Admin password recovery will also reset the monitor and operator password	L	**Problem:** Admin password recovery will also reset the monitor and operator password. **Fixed.**
(63157) Monitor and operator accounts rendered useless after admin password recovery	C	**Problem:** When you recover the admin password with the blue key, it seems as though the monitor and operator accounts become unreachable afterwards. After the admin password is recovered with the blue key, you will not be able to access monitor or operator with the passwords you previously set. Setting the password for these accounts with "user password <monitor/operator>" will give a success message, but you will still not be able to log into these accounts with the password "chrysalis". **Fixed.**
(58380) Require SO authentication prior to setting/modifying the time	H	**Problem:** A Customer requires that the SO be authenticated prior to being able to set the time. If the SO is logged in, the operation should be fine. If the SO isn’t logged in, the operation should fail. **Fixed.**
(67871) Cannot import cert exported from windows	M	**Problem:** When you export a cert PFX file as outlined in the help section "B - Administration & Maintenance - Preparing a PKCS12 Key", you will find that the "cmu importkey" function will give an error when you try to import it onto the HSM. **Fixed.** Added code in cmu to locate the begin block in the pem file in case it is not at the beginning of the file.
(67870) 64-bit cmu will not import keys	M	**Problem:** In the 64 -bit client (both windows and linux), the cmu utility will not import keys that the 32 -bit version will. It will always fail with the error "**Unmapped error: '0x150'. (Check 'Cryptoki.h' for a literal value.)>" **Fixed.**
(41685) No way to set “always ask mofn” option when cloning mofn to another SA	L	**Problem:** The customer was configuring an HA group consisting of members with a shared MofN secret. To share the MofN secret you must initialize the destination member without mofn, then clone the MofN over using a backup token. But because "always ask mofn" is an option you set on HSM init, and only selectable when init'ing with MofN, they could not set this on the destination. So, their primary group member had "always ask mofn" set - but the other member(s) could not have this option. We could (if feasible) add an "always ask mofn" swith to the hsm restore command, to allow the customer to configure this when cloning MofN to the destination. **Fixed.**

Issue	Priority	Synopsis
(39025) cklog and Chrystoki.conf issues on AIX 64	M	**Problem:** Attempted to enable cklog on an AIX 64 machine. The Chrystoki.conf had the following: LibAIX64 = /usr/lunasa/lib//libCryptoki2.so;libcklog2.so; The Sample_Chrystoki.conf contained (CKLog2 section) LibUNIX=/usr/lib/libCryptoki2.so; In the end, for it to work, both entries had to be changed to LibUNIX64. **Fixed.** Samples Chrystoki.conf entries corrected.
(34338) No way to tell if HA recover command needs to be issued	H	**Problem:** If an HA group is actively running and loses a member for some reason (network loss, etc.), there is no way that member can tell you that you need to issue a "vtl haAdmin recover" command. "vtl haAdmin status" will tell you that the device is "up" regardless if it is working in the group or not. **Fixed.**
(32936) Lush help is missing ntls bind “all” option	L	**Problem:** Lush help for ntls bind does not show anything about the “ntls bind all” option. **Fixed.**
(27457) hsm login on tampered/crashed FIPS3 based SA prompts for plaintext password	C	**Problem:** This is a well known problem. Tamper or otherwise crash your FIPS3 HSM in any Luna SA, and when you do an hsm -login, you'll be presented with what appears to be a FIPS2 password prompt. Of course the FIPS2 login fails, but this has been baffling behaviour for many customers over the years. The login should fail immediately with something to the effect of "Cannot communicate with HSM!" rather than default to a FIPS2 based login. **Fixed.**

Disclaimer

Although we have attempted to make this document as complete, accurate, and useful as possible, we cannot guarantee it contents. Errors or omissions will be corrected, as they are identified, in succeeding releases of the product.