Contact Customer Support:
http://safenet-inc.com/support
support@safenet-inc.com

Luna G5 1.2 Customer Release Notes

Document #: 007-011301-001 Revision C

Release Notes Issued on: 2010/12/17

Product Description

SafeNet Luna G5 is a USB attached hardware security module providing cryptographic acceleration, hardware key management, and multiple configuration profiles.

Component Versions

Component	version
HSM:	G5
HSM Firmware:	6.0.8
PED II	2.4.0-3
IKey	1000
Client	1.2

This is a new product and has not yet been submitted for FIPS 140-2 or Common Criteria EAL evaluations.

To follow when Luna products are FIPS validated, you can check from time to time at the NIST website: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm or http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.
You may also contact SafeNet Customer Support at support@safenet-inc.com.

SRK and MTK

Everything in the Luna G5 is encrypted with the MTK (master tamper key). In addition, two “splits” of that key are maintained in the HSM. If the MTK is deleted by a tamper or related event (like battery removal) the tamper light comes on, and the HSM contents are unavailable, unusable.

If your Luna G5 is password authenticated, or is PED authenticated but with no purple PED Key created, then as soon as the power is cycled, the HSM gathers the splits from their internal locations and reconstitutes the MTK. The HSM and all its objects can be decrypted and are once more usable. The tamper light goes off.

If your Luna G5 is PED authenticated, and you **have** enabled an external split, then one of the MTK splits is no longer available inside the HSM. It is stored externally on the SRK (secure recovery key), the purple PED Key. An event that destroys the MTK can now be recovered only with the SRK recover command and the correct purple PED Key presented via Luna PED. The tamper light stays on until you perform the recover operation.

Separately, the SRK (purple PED Key) is used to recover from Secure Transport Mode (which also destroys the MTK).

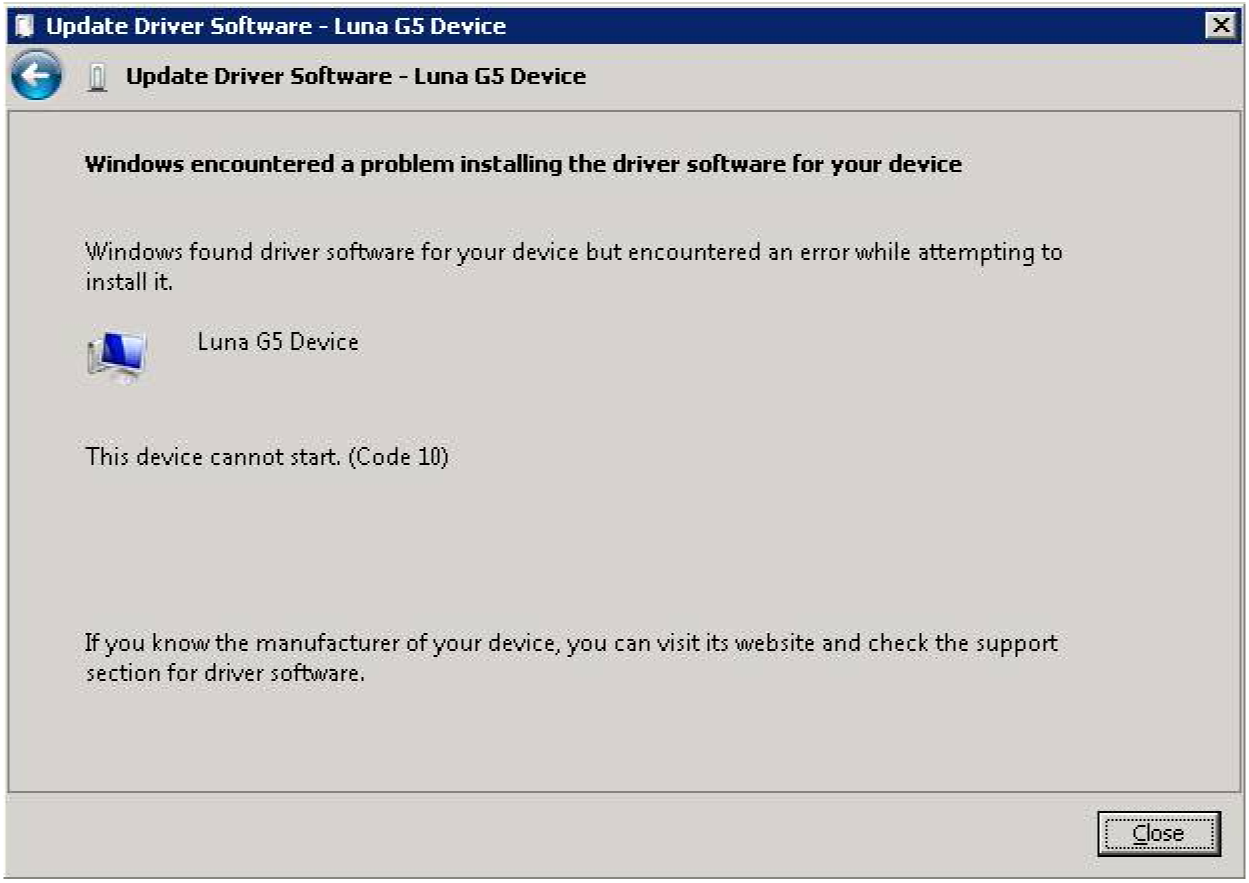
8192-bit RSA keys not supported for first release

Luna G5 can generate 8192-bit RSA keys, but their use is not supported for this release.

Incorrect error message when installing Windows driver

When first installing or updating the Luna G5 driver in Windows Device Manager – a status window reports “Windows found driver software for your device but encountered an error while attempting to install it”. This applies to Windows only. Other operating systems are not affected.

Ignore the error message. After the install/update of the driver, perform a power-cycle of the Luna G5 and it works properly with Windows – the driver is properly installed.


Update Driver Software - Luna G5 Device
Update Driver Software - Luna G5 Device
Close

Windows encountered a problem installing the driver software for your device

Windows found driver software for your device but encountered an error while attempting to install it.

Luna G5 Device

This device cannot start. (Code 10)

If you know the manufacturer of your device, you can visit its website and check the support section for driver software.

Delay slightly when connecting multiple Luna G5 HSMs

Multiple Luna G5 HSMs can be connected to a single computer. If you connect two or more simultaneously to a Windows computer, the driver might not discover both/all of them. After connecting each unit, wait 20 seconds before connecting another. This allows the driver to be ready for the next USB connection.

On Linux machines, you can connect multiple Luna G5 HSMs simultaneously if you wish. Depending on the state of the system, it might take a few seconds for all to be recognized, but in a matter of seconds they all become visible and ready to use.

Upgrade Paths

This is the first generally distributed release of the product (1.0 and 1.1 had controlled distribution). No upgrades exist yet.

Lunacm utility retains unused commands

The version of the lunacm utility shipped with Luna G5 is enhanced for Luna G5, but retains some commands that are used with other Luna products. For Luna G5, lunacm has the “haGroup” commands – use those for HA.

Ignore the lunacm “hsm hainit” and “hsm halogin” commands.

Ignore the lunacm “partition hainit” and “partition halogin” commands.

Linux uninstall does not include full path

For Linux, do not run the uninstall script from the software CD (or tar ball, if you downloaded) - the uninstaller expects to be invoked from the working installed directory, not from the CD. The script will be fixed in the next release to work from anywhere on your system.

jMultitoken has a few issues that could cause confusion

If you are using the jMultitoken demonstration utility, be aware of the following:

- Perform any operation that does not use digest or curve (ie., RSA or DSA), run it, then stop it. Digest and curve drop-boxes are now selectable and any value can be chosen for an op. that does not support either. No error occurs when this is run, though the curve and digest are ignored.
- DSA has a 2048 -bit option, though it only supports 512 and 1024. When this is selected and run, an error occurs. The 2048 option should be removed.
- Depending on the Digest chosen, RSAwithDigest (SHAx) might not support 256 -bit or 512 -bit keys. An error is generated. If the algorithm/digest does not support a given key size, it should not be an option.
- ECC (NOT ECCwithDigest) has the same problem as listed above: run an operation, stop it, then Key Size and Digest are selectable. These are ignored, and no error is generated, but results could be confused with ECCwithDigest.

Summary of Release Support

Luna G5 1.0 Client software:

O/S & version	O/S kernel	32-bit library	64-bit library
Windows 2008 Server R2	64		X
RH Enterprise 5 2.6.18	32	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

Red Hat Enterprise 5 2.6.18	X		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**
Windows 2008 Server R2	X		X		X

Firmware Versions

Supported Firmware Versions

	Luna G5 Version
	1.0
Luna G5 HSM firmware	6.0.0

CD Contents and Compatibility

Contents of Luna G5 Distribution CDs

Client Software and SDK 32-bit and 64-bit [CD# 700-010335-xxx]	**Luna G5 Customer Documentation [CD# 700-010336-xxx]**
Drivers, libraries and utilities required for any computer that is to connect to a Luna G5 HSM. Additional application interfaces for integration of Luna G5 with third- party applications. Logging utility. Code samples for software developers.	Luna G5 Documents for the user and administrator (QuickStart Guide, Help, readme.txt).

Software Version Compatibility by Luna SA Release

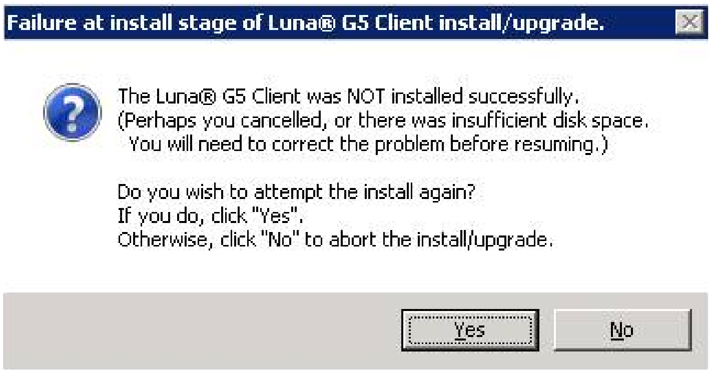
Luna G5 Release	**Client Software version [CD#]**	**Luna G5 Documentation [CD#]**
1.2.0	1.2 (32-and 64-bit) [700-010335-003]	1.0 [700-010336-001] (unchanged)

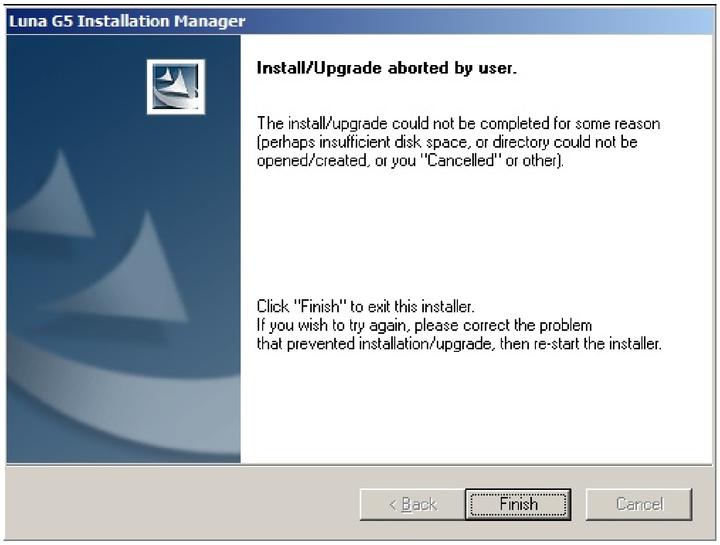
1.0.0	1.0 (32-and 64-bit) [700-010335-001]	1.0 [700-010336-001]

Known Issues

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

Issue	Priority	Synopsis
(104178) "Safely remove hardware does not remove G5 from host system	M	**Problem:** On Windows XP 32 bit, the "Safely remove hardware" wizard removes the Luna G5 device but the G5 resets itself and reappears (within 5 sec). On USB disconnect, the Luna G5 should self-reset, which it does. This is an important failsafe measure to avoid having to send a human out to a remote/secure facility merely to power-cycle a mis-behaving G5. But in MS Windows "safe removal", the host also drops the USB link, causing a disconnect condition at the G5, which then self-resets, confusing MS Windows. **Workaround:** Power-off the Luna G5 and then disconnect it from the host computer.
(99275) "haGroup haOnly -disable" not functional	M	**Problem:** With Luna G5s in High Availability Group you can run "haGroup haOnly –enable" to configure "HA Only" mode, but once "HAOnly" mode is established, lunacm does not allow disabling or exit from "HAOnly" mode. **Workaround:** Edit the configuration file (Chrystoki.ini or chrystoki.conf) to remove the line "HAonly = 1;".
(99270) Code 10 error while updating G5 Driver on Win 2008 64-bit	M	**Problem:** On first installing or updating the Luna G5 driver in Windows Device Manager – a window pops up reporting "Windows found driver software for your device but encountered an error while attempting to install it". Windows only. Other operating systems are not affected. **Workaround:** Ignore the error message. After the install/update of the driver, power-cycle the Luna G5 and it works properly with Windows.
(97845) G5: killing unresponsive lunacm causes hsm reboot	M	**Problem:** The hsm reboots if you try to ungracefully kill lunacm when it is not responding because the system is busy generating large keys. **Workaround:** None.
(95860) Luna G5 HA virtual slot not visible in lunacm	M	**Problem:** The Luna G5 virtual slot is not shown by the show slot list command in lunacm. The virtual slot ID can still be seen in lunadiag or in ckdemo. **Workaround:** Restart lunacm to see the virtual slot. Or if you are a developer, use C_GetSlotInfo and parse the Slot Description to find which slot is the virtual slot.
(95016) lunacm can't	M	**Problem:** Cloning fails with -

Issue	Priority	Synopsis
clone objects from old firmware version (Key Migration Issue)		Error = 0x54 while getting OUID for object handle 6, slot 1. No objects were cloned. The problem is that firmware 4.x (the legacy token HSMs) does not support OUIDs, used by newer versions of lunacm and newer HSM firmware. Attempting to migrate keys from firmware 4 HSMs to firmware 6 HSMs (Luna G5, K6) with lunacm fails. **Workaround:** It is possible to use ckdemo for the migration task, or for a developer to create a migration application using the Luna API.
(82593) Windows driver problem when two Luna G5 units connected simultaneously	H	**Problem:** When 2 (or more) Luna G5s are connected at the same time to a Windows system, all but one of them remain unusable.. **Workaround:** Connect one unit, wait for it to be fully recognized by the host system (20 seconds), and then connect the next unit.
(82205) cklog when file exceeds 2GB, applications like lunacm exit	H	**Problem:** On Linux 32bit - when cklog file in /tmp reaches 2GB, applications like lunacm will exit with file size exceeded. The file needs to be removed or renamed to restore functionality. **Workaround:** Cklog function is off by default. Turn it on if instructed by SafeNet Customer Support. If you switch cklog on, track it and keep the file size below 2GB.
(81986) installing linux32 driver with 2 devices attached might confuse driver	M	**Problem:** Linux32 system with 2 Luna G5s attached. Driver (and software) install without error. However, could not start lunacm or access Luna G5s through other utilities as neither Luna G5 could be detected. The driver was showing as running, but showed both Luna G5s running under the same instance. **Workaround:** USB disconnect/reconnect the second Luna G5. If that is insufficient, try disconnecting and reconnecting both.
(80788) G5 Windows 64-bit install finishes before it starts	M	**Problem:** Installing from the CD in a Windows 64-bit computer results in an error message "Failure at install stage of Luna G5 Client install"  Failure at install stage of Luna® G5 Client install/upgrade. The Luna® G5 Client was NOT installed successfully. (Perhaps you cancelled, or there was insufficient disk space. You will need to correct the problem before resuming.) Do you wish to attempt the install again? If you do, click "Yes". Otherwise, click "No" to abort the install/upgrade. The message is misleading.

Issue	Priority	Synopsis
		Workaround: When asked if you wish to attempt the install again, or click [No] to abort, click [No]. Then the installer presents a “could not be completed...” message:  **Install/Upgrade aborted by user.** The install/upgrade could not be completed for some reason (perhaps insufficient disk space, or directory could not be opened/created, or you "Cancelled" or other). Click "Finish" to exit this installer. If you wish to try again, please correct the problem that prevented installation/upgrade, then re-start the installer. Click [Finish]. The installation resumes and completes. Alternatively, copy the contents of the Windows 64-bit installer directory from the Luna CD to your hard disk, and Setup.exe from there – the error does not occur.
(80669) Unplugging/plugging back in G5 will eventually fails to reset it correctly	M	**Problem:** Repeatedly disconnecting and reconnecting the USB cable between Luna G5 and your computer can put the Luna G5 into an "undefined" state that shows in lunacm as firmware 0.0 and "undefined" mode. **Workaround:** Power-cycle the Luna G5, waiting 30 seconds before reconnecting the power cord.
(80371) "hsm showinfo" doesn't show enough info if SRK is zeroized	L	**Problem:** When the G5's SRK is zeroized, not much can be done with it - and only certain information is query-able. "hsm showinfo" in this state quits almost immediately: lunacm:> hsm si HSM Label -> no label HSM Manufacturer -> Safenet, Inc. HSM Model -> G5 Base HSM Serial Number -> 655123 Token Flags -> CKF_RNG CKF_LOGIN_REQUIRED CKF_RESTORE_KEY_NOT_NEEDED CKF_PROTECTED_AUTHENTICATION_PATH Firmware Version -> 6.0.0 Command Result : 0x80000026 (CKR_MTK_ZEROIZED) lunacm:> "hsm si" should be modified to show all that it is allowed to when the HSM is in this state. **Workaround:** Power-cycle the Luna G5, waiting 30 seconds before reconnecting the power cord.

Issue	Priority	Synopsis
(80363) Can't regenerate SRK when Luna G5 is zeroized	L	**Problem:** In this case, if SRK generate is not permitted in the zeroized state, it should error out immediately with "srk_zeroized", and not present a PED prompt and then device error. lunacm:> srk generate Please attend to the PED. SRK failed to regenerate. Command Result : 0x30 (CKR_DEVICE_ERROR) **Workaround:** None.
(80017) HA Login/HA Init LunaCM commands	M	**Problem:** Luna CM has HA Init and HA Login commands. They are not used with Luna G5 and should be removed/obscured when lunacm is used with Luna G5. hainit hai High Availability Initialize HSM halogin hal High Availability Login **Workaround:** Ignore the hainit and halogin commands in the lunacm hsm and partition menus. Use the lunacm hagroup commands instead.
(79918) Luna G5 -USB compliance regarding host-controller reset	L	**Problem:** When the host controller issues a reset, the Luna G5 does a deep reset, rebooting itself. However, usb compliance requires the device to come back in a short time (on the order of a hundred milliseconds). The entire reboot process takes a lot longer than this. **Workaround:** None.
(79716) Documentation: SO user loses their login state by setting appid	M	**Problem:** When you set an APPID in lunacm, the SO loses login state. **Workaround:** This behavior for LunaCM is expected. LunaCM behaves differently than ckdemo because ckdemo lets the user manage the sessions. With lunaCM, the sessions are all handled internally. When an appID is set in lunaCM, it explicitly closes the existing session, forcing you to open a new session, and as a result, re-login.
(79124) Windows install lacks Microsoft Windows Logo (for Driver) certification	L	**Problem:** The Windows driver might not yet have received the Windows Logo (formerly WHQL) certification at release time, and therefore would cause an error message to appear during the installation. **Workaround:** Ignore the message and trust/accept the driver to permit it to be installed.

Addressed Issues

Issue	Priority	Synopsis
(84992) Secure	H	**Problem:** Luna G5 units are shipped from the factory with

Issue	Priority	Synopsis
Transport Mode should be configurable by the customer		SRK external split on purple PED Key. Many customers do not require this extra handling for an HSM that has not yet been used. However, they do want to be able to enable the feature for their own purposes. **Fixed**. Luna G5 HSMs are now shipped STM-capable from the factory, but with no external split (SRK) set. This simplifies delivery handling, but allows customers to turn on (enable) the feature if desired.
(84297) Use SHA-256 or stronger as the digest mechanism in the manufacturing process	H	**Problem:** In order to conform to the NIST key management document, Special Publication 800-57, all certificates and keys used in our internal processes and procedures must be converted to use SHA-256 (or stronger) as the digest mechanism. **Fixed**. Re-certification and increased signature strength have been implemented in 2010.
(80787) Luna G5 PED port is too close to USB port, some devices or connectors might not be able to fit	H	**Problem:** Luna G5 PED port is too close to USB port, some devices or connectors might not be able to fit side-by-side. **Fixed**. Hardware was modified to increase the distance between the two ports.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

Printed in Canada 2010/12/17
007-011301-001 Revision C