SafeNet Luna PCIe HSM 7.0

CUSTOMER RELEASE NOTES

Issue Date: 07 December 2017

Document Part Number: 007-013579-002 Rev. B

The most up-to-date version of this document is posted to the Technical Support Customer Portal at https://supportportal.gemalto.com

Contents

Product Description

The SafeNet Luna PCIe HSM secures your sensitive data and critical applications by storing, protecting and managing your cryptographic keys in a high-assurance, tamper-resistant, low-profile PCIe card that offers market-leading performance. The SafeNet Luna PCIe HSM provides applications with dedicated access to a purpose-built, high-performance cryptographic processor. You can quickly embed this cost-efficient solution directly into your servers and security appliances for FIPS 140-2 validated key security.

The SafeNet Luna PCIe HSM is installed directly into an application server to provide PKCS#11-compliant cryptographic services.

Release Description

SafeNet Luna PCIe HSM 7.0 is the first release of Gemalto's next-generation SafeNet Luna PCIe HSM. It includes a new cryptographic module that provides performance gains that are 10x faster than the previous version. Functionality is equivalent to SafeNet Luna PCIe HSM 6.x, with significant improvements as detailed in "New Features and Enhancements" below.

New Features and Enhancements

This section highlights what's new in SafeNet Luna PCIe HSM 7.0.

Low-Profile Card

The SafeNet Luna PCIe HSM 7.0 is smaller than its predecessors and can be installed in a half-height PCIe slot.

Partition Security Officer

All application partitions now have a Partition Security Officer (PSO) role that is completely distinct from the HSM Security Officer (HSM SO) role. In this security model, the HSM SO is responsible only for initializing the HSM, setting HSM-level security policies, and creating and deleting partitions. After creating the partitions, the HSM SO has no access to the contents of the partitions. Partitions are owned by the PSO, who is responsible for initializing the partition, setting the partition-level security policies and initializing the cryptographic roles on the partition. This model permits a complete separation of roles on the HSM.

Best-in-Class Performance

SafeNet Luna PCIe HSM 7.0 provides cryptographic performance that is 10x faster than the release 5.x and 6.x SafeNet Luna HSMs.

Industry-Leading Security

SafeNet Luna PCIe HSM7.0 provides enhanced environmental failure protection and tamper resistance.

Improved Random Number Generation

The performance of SafeNet Luna PCIe HSM 7.0's AES-256 CTR DRBG random number generation is significantly increased from previous versions. The RNG is fully compliant with the latest entropy standards:

- SP800-90B
- SP800-90C

- BSI DRG.4

New Cryptographic Mechanism Support

SafeNet Luna PCIe HSM 7.0 adds support for the following cryptographic algorithms:

- SP800-108 HMAC (RSA & ECC)
- SP800-38F (KWP)
- Curve 25519
- AES-XTS - disk encryption standard

Increased Key Storage Capacity

SafeNet Luna PCIe HSM 7.0 provides up to 32 MB of cryptographic object storage (depending on the model).

Secure Transport Mode Redesigned

Secure Transport Mode (STM) in SafeNet Luna PCIe HSM 7.0 provides a simple, secure method for shipping an HSM to a new location and verifying its integrity upon receipt. When the HSM SO enables STM, it locks the HSM and its contents, and records the current configuration as a pair of unique strings. When the HSM is recovered from STM, the unique strings are redisplayed. If the strings match, the HSM has not been tampered or modified during transport.

Note: All SafeNet Luna PCIe HSMs are shipped from the factory in STM, and you are provided with the STM verification strings as part of the shipping materials. You must recover the HSM from STM before it can be initialized. The integrity check is optional - you can still recover from STM if the strings do not match.

External Power Supply for SafeNet Luna Backup HSM

The SafeNet Luna Backup HSM ships with an external power supply.

Advisory Notes

This section highlights important issues you should be aware of before deploying this release.

PED Upgrade Needed for Currently-Owned PEDs

If you have older PEDs that you intend to use with SafeNet Luna HSM 7.0 or later, you must upgrade to firmware 2.7.1 (or newer). The upgrade and accompanying documentation (007-012337-003_PED_upgrade_2-7-1-5.pdf) are available from the Gemalto Support Portal.

New USB-powered PED

Gemalto is pleased to announce the availability of SafeNet Luna HSM Pin Entry Device (PED) v2.8. The v2.8 PED contains new hardware that enables the PED to be USB-powered; there is no longer a requirement for an external DC power Adapter. PED v2.8 is functionally equivalent to your existing (pre-generation) PEDs and is compatible with HSM versions, 5.x, 6.x, and 7.x.

PED v2.8 ships with firmware 2.8.0. Note that you cannot upgrade existing PEDs to the 2.8.0 version; existing PEDs continue to need a separate DC power adapter for remote PED and upgrade use. The model number on the manufacturer's label identifies the refreshed PED: PED-06-0001.

To use the new USB-powered PED

1. Ensure the SafeNet Luna HSM Client software is installed on the Windows computer that will act as the PED Server to your SafeNet Luna HSM. Installing the Remote PED component of the SafeNet Luna HSM Client installs the required driver.
2. Connect the PED to the computer where you installed the Remote PED component of the SafeNet Luna client using the USB micro connector on the PED and a USB socket on your computer.
3. After you connect the PED to the host computer, it will take 30 to 60 seconds for initial boot-up, during which time a series of messages are displayed, as listed below:

   BOOT V.1.1.0-1

   CORE V.3.0.0-1

   Loading PED...

   Entering...
4. After the boot process is complete, the PED displays **Local PED mode** and the **Awaiting command...** prompt. Your new PED is now ready for use.
5. To enter Remote PED mode, if needed, exit Local PED mode with the "< " key, and from the **Select Mode** menu, select option **7 Remote PED**.

Remote Backup Over IPv6 is Unavailable

Network connections from the SafeNet Luna Client to a Remote Backup Server must use IPv4.

Note: Network connections from the client to the HSMs you want to backup using RBS can use IPv6. Only the connection from the client to the RBS server requires IPv4.

Partition Policy Templates are Unavailable

Partition policy templates are not available in this release.

HA Groups Containing Members From Different Releases

You can configure an HA group containing release 7.0 and release 5/6.x partitions to easily migrate cryptographic objects to the new HSM.

Note: Failover and load-balancing performance during sustained application in a mixed-release HA group has not been fully characterized for all failure scenarios.

SafeNet Luna Backup HSM Firmware Upgrade 6.26.0 Limitations

You can apply firmware upgrade 6.26.0 to your existing SafeNet Luna Backup HSMs to increase their backup storage capacity from 15.5 MB to 32 MB. This allows you to fully back up a SafeNet Luna HSM 7.0 partition that takes advantage of the increased key storage capacity offered in this release.

Before upgrading your SafeNet Luna Backup HSMs to firmware 6.26.0, consider the following limitations:

- If you upgrade your Backup HSM to FW 6.26.0, it is no longer compatible with previous releases of SafeNet Luna HSM.
- If you are migrating from previous releases to SafeNet Luna HSM 7.0, we recommend that you do not upgrade to firmware 6.26.0. Note, however, that your backups will be limited to 15.5 MB. Therefore, if the objects in the partition you want to back up consume more than 15.5 MB, you will need to split the backup into two separate operations.
- If you are using only SafeNet Luna HSM 7.0, we recommend that you upgrade your SafeNet Luna Backup HSMs to firmware 6.26.0.

Deprecated and Discontinued Features

The following features are deprecated or discontinued in this release. If you have been using any of these features, plan for a new configuration and workflow that does not make use of the feature:

- Small form factor (SFF) backup

Compatibility Information

This section lists the supported software and hardware for the HSM.

SafeNet Luna HSM Client

You can install the SafeNet Luna HSM Client 7.0 on the following operating systems:

Operating System	Version	64-bit client	32-bit applications on 64-bit OS	32-bit applications on 32-bit OS
Windows	10	Yes	Yes	No
	2012 R2	Yes	Yes	No
	2016	Yes	Yes	No
Redhat-based Linux (including variants like CentOS and Oracle Enterprise Linux)	6	Yes	Yes	Yes
	7	Yes	Yes	Yes
Ubuntu *	14.04	Yes	No	Yes

* The Linux installer for Luna Client software is compiled as .rpm packages. To install on a Debian-based distribution, such as Ubuntu, "alien" is used to convert the packages. We used "build-essential":

apt-get install build-essential alien

You might need to account for your particular system and any pre-existing dependencies for your other applications.

Remote PED Server

The Remote PED server software is included with the SafeNet Luna HSM client software. You must install the SafeNet Luna HSM client, with the PED server option, on each workstation used to host a remote PED. The Remote PED server software is supported on the following operating systems:

- Windows 10 (64-bit)
- Windows 2012 R2

- Windows 2016

Supported Cryptographic APIs

Applications can perform cryptographic operations using the following APIs:

- PKCS#11 2.20
- Java 7
- Java 8
- OpenSSL
- Microsoft CAPI
- Microsoft CNG

Server Compatibility

The SafeNet Luna PCIe HSM conforms to the PCIe 2.0 standard and requires a PCIe x4 or higher slot. There are no known incompatible servers at this time.

Note: Do not install the SafeNet Luna PCIe HSM into a slot reserved for a dedicated function, such as video. If you do, the host system may not boot successfully.

Known Issues

This section lists the issues known to exist in the product at the time of release. Workarounds are provided where available. The following table lists the defines the severity level assigned to each listed issue.

Table 1: Issue severity definitions

Severity	Classification	Definition
H	High	Reasonable workaround exists.
M	Medium	Medium severity problems.
L	Low	Low severity problems.

Table 2: List of known issues

Issue	Severity	Synopsis
LKX-2632	H	**Problem:** When audit logging is configured on Linux, cryptographic operations will continue even when the external log directory is deleted mid-operation. **Workaround:** None. This is expected behavior on Linux systems.
LKX-2634	M	**Problem:** Cannot back up curve25519 key types to the SafeNet Luna Backup HSM. **Workaround:** Use cloning or HA to back up your curve25519 key types to another SafeNet Luna 7.0 HSM.
LUNA-853	M	**Problem:** On Linux, the SafeNet Luna HSM Client software fails to install to a directory with spaces in its name.

Issue	Severity	Synopsis
		Workaround: Remove spaces from the directory name before installing the Client.
LUNA-264	M	**Problem:** On Linux, non-root users cannot initialize the STC token or create an STC client identity. **Workaround:** Start LunaCM as root with **sudo ./lunacm**.
LUNA-263	M	**Problem:** On Linux, non-root users cannot configure the RBS server. **Workaround:** As root, run the following commands: 1. **chown -R root:hsmusers /usr/safenet/lunaclient/rbs/** 2. **chmod g+w -R usr/safenet/lunaclient/rbs/**
LUNA-262	M	**Problem:** On Linux, non-root users receive error (CKR_DATA_INVALID) when creating an HA group. **Workaround:** Before installing the SafeNet Luna HSM Client software, adjust the ownership of the Chrystoki.conf rpmsave with the command **chown root:hsmusers /etc/Chrystoki.conf**
CPP-3385	M	**Problem:** On Windows, a system crash can occur when you disconnect a SafeNet Luna Backup HSM from the computer while the PedClient service is running. **Workaround:** Stop the PedClient service before disconnecting the Backup HSM. From a command line, run **pedclient mode stop**.
CPP-3151	M	**Problem:** SafeNet Luna HSM Client will not install on Windows 2012 R2. **Workaround:** Ensure that your Windows machine has the Universal C Runtime in Windows (KB2999226) update installed on it. If you do not, obtain it from Microsoft Support. Refer to the *Installation Guide* for details.
CPP-2376	M	**Problem:** On the Backup HSM, the **hsm init** command with the **-iped** option fails after **hsm factoryreset**. **Workaround:** Run the **hsm init** command again. The second attempt should be successful.
CPP-2368	M	**Problem:** The **hagroup list** command returns an error. **Workaround:** Run the **hagroup list** command again. The second attempt should be successful.
CPP-632	M	**Problem:** When using CKdemo with HA groups, an **Attribute type invalid** error is returned. **Workaround:** If you plan to use HA Groups, change your CKdemo settings to use legacy role logins. To do this, select **Role Support** from the **98) Options** in the **OTHERS** menu.
CPP-628, LKX-554	M	**Problem:** Unable to add a member to an HA group if the Partition SO or Crypto Officer is currently logged in to the primary member of the HA group. **Workaround:** Ensure that the Partition SO or Crypto Officer are not logged in to the primary HA member partition when adding a new member.
CPP-626, CPP-624	M	**Problem:** If you zeroize an HSM hosting an HA group member partition, all running cryptographic operations against the HA group fail.

Issue	Severity	Synopsis
		Workaround: Remove any member partition from the HA group before zeroizing the host HSM.
LUNA-266	L	**Problem:** In LunaCM, **clientconfig deleteserver** deregisters the HSM server on the Client, but does not delete the HSM server certificate file from the <LunaClient_dir>**/cert/server** directory. Attempts to re-register the same server with a regenerated certificate fail. **Workaround:** Manually delete the certificate from the **cert/server** directory.
LUNA-188	L	**Problem:** When using RBS to remotely backup a PED-authenticated STC partition greater than 30MB, the default idle timeout setting (30 minutes) may not be long enough to prevent the remote session from disconnecting. **Workaround:** Increase the idle timeout threshold for both PedClient and PedServer to at least 40 minutes (2400 s) before attempting remote backup.
LKX-2812	L	**Problem:** The HSM reports 3072-bit as the maximum allowed key size for the RSA 186-3 mechanisms (CKM_RSA_FIPS_186_3_AUX_PRIME_KEY_PAIR_GEN and CKM_RSA_FIPS_186_3_PRIME_KEY_PAIR_GEN), when it should report 4096-bit. **C_GetMechanismInfo** will report 3072 as the maximum size for these mechanisms. If your application uses **C_GetMechanismInfo** to query the maximum key size, it may prevent 4096 operations from working. **Workaround:** Ignore the reported limit. 4096-length keys will generate successfully.
CPP-3391	L	**Problem:** When trying to run the **HALogin.java** script, a CKR_UNKNOWN error is returned. **Workaround:** None. Do not use the **HALogin.java** sample.
CPP-3387	L	**Problem:** On a new Linux client, the Luna HSM Client uninstaller hangs when a SafeNet Luna Backup HSM is connected to the client machine. **Workaround:** Disconnect the SafeNet Luna Backup HSM from the client before uninstalling.
CPP-2960	L	**Problem:** LunaCM hangs on exit on Windows 2016. **Workaround:** End the LunaCM instance using the Task Manager.
CPP-2925	L	**Problem:** When the **cklog** library is configured, an **error.txt** file containing extraneous messages may be created. **Workaround:** None.
CPP-2576	L	**Problem:** Windows installer does not remove CSP and KSP registry entries for 32-bit setup when the Windows client is uninstalled. **Workaround:** No impact on service; registry entries may be deleted manually.
CPP-2488	L	**Problem:** Version 6.x and 7.x HSM role name abbreviations are not consistent. **Workaround:** Remember to use the full role name when logging in to Luna 6.x partitions.
CPP-2380	L	**Problem:** When running the **MiscCSRCertificateDemo.java** sample, a null pointer exception occurs. **Workaround:** None.

Issue	Severity	Synopsis
CPP-1249	L	**Problem:** Remote backup through TCP/IP via the LunaCM command **partition archive backup -slot remote -hostname** <hostname> **-port** <portnum> is not recognized. **Workaround:** Use RBS to backup partitions remotely.
CPP-932	L	**Problem**: If the configured audit logging directory is not found, the **pedclient** service fails with error **LOGGER_init failed**. **Workaround**: Ensure that the directory you configure for audit logging exists.
CPP-3404	L	**Problem:** CMU may crash or report a memory allocation error when using a non-FIPS signing mechanism in FIPS mode. **Workaround:** Specify a FIPS-approved signing mechanism such as **sha256withRSA**.
CPP-3235	L	**Problem:** In LunaCM, the **partition clone** command fails the first time if the Partition SO is logged in to the target slot. **Workaround:** Run the **partition clone** command again. The second attempt should be successful.

Resolved Issues

This section lists issues that have been resolved for the current release.

Table 3: List of resolved issues

Issue	Severity	Synopsis
LKX-3204	H	**Problem:** Implementations of SSL/TLS 1.1 or earlier receive CKR_DATA_INVALID error when attempting to sign data with CKA_RSA_PKCS. **Fixed:** [Requires firmware 7.0.2]

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

Note: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone. Calls to Gemalto Customer Support are handled on a priority basis.

Region	Telephone number (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Global	+1 410-931-7520
Australia	1800.020.183
China	North: 10800-713-1971 South: 10800-1301-932
France	0800-912-857
Germany	0800-181-6374
India	000.800.100.4290

Region	Telephone number (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Israel	180-931-5798
Italy	800-786-421
Japan	0066 3382 1699
Korea	+82 2 3429 1055
Netherlands	0800.022.2996
New Zealand	0800.440.359
Portugal	800.863.499
Singapore	800.1302.029
Spain	900.938.717
Sweden	020.791.028
Switzerland	0800.564.849
United Kingdom	0800.056.3158
United States	(800) 545-6608

