SafeNet Luna PCIe HSM 7.2

CUSTOMER RELEASE NOTES

Issue Date: 17 August 2018

Document Part Number: 007-013579-004 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 7.2 is a field update release of Gemalto's 7.x SafeNet Luna PCIe HSM. It includes Client software with drivers and tools, and new firmware for the HSM.

Important Notices for SafeNet Luna PCIe HSM 7.2 Release

Please consider the following important information before updating to this release.

SafeNet Luna HSM Firmware Updates

Gemalto has provided two (2) new versions of the SafeNet Luna HSM firmware:

- SafeNet Luna HSM firmware version **7.2.0**, which contains all the latest features and bug fixes
- SafeNet Luna HSM firmware version **7.0.3**, Gemalto's newest FIPS-validated version for Luna 7 HSMs

> **NOTE** Refer to the following sections for more information:
>
> - "Valid Update Paths" on page 6
> - "Recommended Minimum Versions" on page 7
> - "Special Instructions for Installing Firmware 7.0.3 if Your Current Firmware Version is 7.1.0" on page 7

Resolved Issue LKX-3338

Gemalto has identified an issue with asymmetric digest-and-sign, or digest-and-verify mechanisms when the data length exceeds 64KB, for all SHAxxx_RSA_xxx, SHAxxx_DSA and SHAxxx_ECDSA mechanisms.

Please note:

- Simple (i.e. not combined with digest) RSA/ECDSA/DSA sign/verify operations are NOT affected, and work as expected for all HSM models.
- This issue only affects HSMs with standard- and enterprise-level performance (*700 and *750 models). Maximum-performance (*790) models are not affected.

This issue is resolved in both firmware 7.2.0 and 7.0.3.

Gemalto strongly recommends that you update to firmware 7.2.0 or firmware 7.0.3 to avoid this issue in the future.

New Features and Enhancements

SafeNet Luna PCIe HSM 7.2 introduces the following new features and enhancements:

Improved Luna HSM Client

Release 7.2 adds improvements to the Luna HSM Client software:

- **Enhanced Version Compatibility for Luna HSM Client** — Version 7.2 and newer Luna HSM Client can be used with HSMs running Luna 6.2.1 or higher, or any Luna 7 version, without conflict. Luna HSM Client 7.2 and newer versions can coexist in large deployments. You can schedule client roll-outs at your convenience, without need to match versions across your organization. Future HSM features that do not have client-version dependencies will function without issue. See also "Supported Operating Systems" on page 5.
- **Improved Client Installer with User-Defined Install Paths (Windows)** — Luna HSM Client can be installed at user-selected locations (file paths with sufficient space), and installed Client software can be modified without uninstalling and reinstalling.
- **User-Defined Client Install Paths (Linux)** — Linux root-level users can install the Luna HSM Client software to an installation directory of their choice.

Relabel Partitions

The Partition SO can now change the label of an initialized partition. This allows partitions to be created ahead of time and renamed to something more suitable later, when they are allocated for a particular purpose (Requires firmware 7.2.0).

Crypto User Can Clone Public Objects

The Crypto User (CU) role has always been able to create public objects, but not clone them. In HA mode, this would cause the replication and subsequent object creation operations to fail. Firmware 7.2.0 allows the CU to clone public objects, and therefore to perform operations on HA groups without Crypto Officer authentication (Requires firmware 7.2.0).

Auto-Enabled HA Logging

Luna HSM Client now automatically enables HA logging, either when you create the first HA group, or when you update the Luna HSM Client to 7.2 and it detects a previously-configured HA group. If you manually turn HA logging off, logging is not auto-enabled for new HA groups.

SCP03 Encoding

The SCP03 encoding scheme, as defined in NIST SP 800-108, is now supported for Global Platform.

Fixes

Issues addressed in this release are listed in "Resolved Issues" on page 11.

Advisory Notes

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

PED Upgrade Required 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 provide PED authentication for your SafeNet Luna PCIe 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 HSM 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 HSM 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.

Supported Operating Systems

This section lists the supported operating systems for the SafeNet Luna HSM Client and Remote PEDserver.

SafeNet Luna HSM Client

You can install the SafeNet Luna HSM Client 7.2 on the following operating systems:

Operating System	Version	64-bit applications on 64-bit OS	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 HSM 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

If you are using a Docker container or another such microservice to install the Luna Minimal Client on Ubuntu, and your initial client installation was on another supported Linux distribution as listed above, you do not require **alien**. Refer to the product documentation for instructions. You might need to account for your particular system and any pre-existing dependencies for your other applications.

Remote PEDserver

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

- Windows 10 (64-bit)
- Windows 2016
- Windows 2012 R2

Supported Cryptographic APIs

Applications can perform cryptographic operations using the following APIs:

- PKCS#11 2.20
- Java 7/8/9
- 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 might not boot successfully.

Update Considerations and Procedures

Detailed procedures for installing the SafeNet Luna PCIe HSM7.2 software and firmware updates can be found in the product documentation. Before you install any of the updates, consider the following guidelines:

- If it applies to you, refer to "Special Instructions for Installing Firmware 7.0.3 if Your Current Firmware Version is 7.1.0" on the next page.
- Back up all important cryptographic material. Refer to the product documentation for backup procedures.
- Stop all client applications running cryptographic operations on the HSM.
- Use an uninterruptible power supply (UPS) to power your HSM. There is a small chance that a power failure during an update could leave your HSM in an unrecoverable condition.

Valid Update Paths

The following table provides tested paths for updating to the current software/firmware versions.

Component	Directly from version	To version
SafeNet Luna HSM Client software	Any	7.2
SafeNet Luna HSM firmware	7.0.1, 7.0.2, 7.0.3, 7.1.0	7.2.0
	7.0.1, 7.0.2	7.0.3 (FIPS-certified)
SafeNet Backup HSM firmware	6.10.9, 6.26.0	6.27.0
SafeNet Luna PED firmware	2.7.1	N/A
	2.8.0	N/A

FIPS-Validated Firmware Versions

The following firmware versions are all FIPS 140-2, overall level 3, certified per certificate #3205 (https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3205):

- Luna firmware v. 7.0.3 (recommended)
- Luna firmware v. 7.0.2 (see F5 note, below)
- Luna firmware v. 7.0.1

For details on the scope of the FIPS certificate and applicable configurations, please refer to the product Security Policy posted alongside the certificate at the link above.

Recommended Minimum Versions

Generally, Gemalto recommends that you always keep your HSM firmware and client software up to date, to benefit from the latest SafeNet features and bug fixes. If regular updates are not possible or convenient, the following table lists the recommended minimum firmware and software versions for use with SafeNet Luna 7 HSMs. If you are running an earlier version, Gemalto advises upgrading to the version(s) below (or later) to ensure that you have critical bug fixes and security updates.

	Luna HSM Client	Luna HSM Firmware
SafeNet Luna PCIe HSM 7 Minimum Recommended Configuration	7.2	7.2.0
		7.0.3

NOTE Customers who wish to use Luna 7 HSMs with F5 Network BIG-IP 13.1 appliances should follow F5 guidelines for Supported SafeNet client and HSM versions (https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/f5-safenet-hsm-version-interoperability-matrix.html). At the time of this release, F5's supported versions for Luna 7 are Luna HSM Client 7.1 with firmware 7.0.2.

Special Instructions for Installing Firmware 7.0.3 if Your Current Firmware Version is 7.1.0

Firmware 7.0.3 is Gemalto's latest FIPS-certified Luna firmware. If you are using firmware 7.0.1 or 7.0.2, you can proceed with the standard update procedure. If you previously updated to firmware 7.1.0, and you wish to use firmware 7.0.3, follow this procedure to ensure a successful update.

SafeNet Luna PCIe HSM does not allow you to update the firmware from a higher-numbered to a lower-numbered version. Therefore, if you are currently running firmware 7.1.0, you must first perform a firmware rollback.

CAUTION! Firmware rollback is destructive; earlier firmware versions might have older mechanisms and security vulnerabilities that a new version does not. Back up any important materials before rolling back the firmware. This procedure zeroizes the HSM and all cryptographic objects are erased.

To install firmware 7.0.3 on an HSM running firmware 7.1.0:

1. Check the previous firmware version that is available on the HSM. The firmware available for rollback must be 7.0.1 or 7.0.2.

   lunacm:>**hsm showinfo**
2. Back up any important cryptographic objects currently stored on the HSM.
3. Log in as HSM SO.

   lunacm:>**role login -name so**
4. Perform a firmware rollback.

   lunacm:>**hsm rollbackfw**

   LunaCM performs an automatic restart following the rollback procedure.

5. Initialize the HSM and log in as HSM SO.
6. Install the SafeNet Luna HSM firmware 7.0.3 as described in the product documentation.
7. Recreate your application partition and restore the contents from backup.

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 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 in release 7.2

Issue	Severity	Synopsis
LKX-3184	M	**Applies to firmware 7.0.3 only. This issue has been fixed in firmware 7.2.0.** **Problem**: If HSM policy 39: Enable Secure Trusted Channel has been set to **1** (ON) at any time, attempting a firmware rollback will cause the HSM to fail with an error (Unable to communicate with HSM). **Workaround:** None. If you are using STC, or have enabled HSM policy 39 in the past, do not roll back the HSM firmware.
LUNA-7170	M	**Problem:** When installing PCIe HSM 7 drivers from Luna HSM Client software on a host machine with a fresh, non-upgraded version of Windows 10, Windows reports an error with the driver signatures. **Workaround:** Disable Windows 10 driver signature enforcement before installing the Luna HSM Client.
LUNA-3298	M	**Problem:** When installing Backup HSM and/or PED drivers from Luna HSM Client software on a host machine with a fresh, non-upgraded version of Windows 10, Windows reports an error with the driver signatures. **Workaround:**Disable Windows 10 driver signature enforcement before installing the Luna HSM Client.
LUNA-3108	M	**Problem:** If you uninstall Luna HSM Client and reinstall it in a custom directory, HA logging stops working. **Workaround:** Open **crystoki.conf**/**crystoki.ini** and edit `haLogPath =` to match the new client path.
LUNA-3107	M	**Problem:** If you uninstall Luna HSM Client and reinstall it in a custom directory, RBS stops working. **Workaround:** Copy the two certificate files **serverkey.pem** and **server.pem** from the original **rbs** directory to the new **rbs** directory.

Issue	Severity	Synopsis
LUNA-3071	M	**Problem:** When LunaCM is launched in Luna Minimal Client, an unexpected error is displayed (Error: Failed to initialize remote PED support). **Workaround:** Edit Chrystoki.conf/crystoki.ini and remove **Toolsdir** form the **Misc** section.
LUNA-3070	M	**Problem:vtl cklog enable/disable** command not working if LibUNIX and LibUNIX64 are in different folders. **Workaround:** Enable **cklog** manually by editing Chrystoki.conf/Chystoki.ini. Refer to the *SDK Reference Guide* for details.

LUNA-2983	M	**Problem:** CMU Export Public Key - Incorrect formatting of exported key. A public key, exported with command **cmu export -handle** <handle#> **-outputfile** <filename> **-key** has incorrect header and footer text.
		Workaround: Edit the exported public key file, replacing
		`----- BEGIN CERTIFICATE -----` and `----- END CERTIFICATE -----`
		with
		`----- BEGIN PUBLIC KEY -----` and `----- END PUBLIC KEY -----`
		respectively.

LUNA-2646	M	**Problem:** One-step NTLS can fail after installing, uninstalling, and reinstalling the Luna HSM Client on Windows. **Workaround:** Use the multi-step NTLS setup procedure to create a connection to the SafeNet Luna PCIe HSM appliance.
LUNA-2445	M	**Problem:** The default maximum length for HA log files is incorrectly set to 40000 bytes, and misreported in LunaCM as 262144 bytes (the intended minimum). This can lead to many small HA log files being rotated frequently. **Workaround:** Manually set the HA log maximum file size using lunacm:>**hagroup halog -maxlength** <bytes> the first time you configure HA logging.

Table 3: List of known issues from prior releases

Issue	Severity	Synopsis
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-2268	M	**Problem:** The deprecated LunaCM command **hsm reset** can still be run on a PCIe HA slot, causing LunaCM to crash. **Workaround:** If you encounter this crash, restart LunaCM. Use **hsm restart** instead.
LUNA-2261	M	**Problem:** "CKR_DATA_INVALID" on wrap/unwrap with **multitoken** on AIX and Solaris clients. **Workaround:** None.
LUNA-2252	M	**Problem:** Invalid options are displayed on Solaris installer. **Workaround:** Only the SafeNet Luna Network HSM is supported for Solaris; drivers for the PCIe HSM and USB HSM options are not provided at this time. If multiple options appear when installing Luna HSM Client on Solaris, choose Network HSM only.

Issue	Severity	Synopsis
LUNA-2224	M	**Problem:** When you initialize an STC partition by applying a partition policy template, a confusing error (CKR_TOKEN_NOT_PRESENT) is returned. **Workaround:** None.
LUNA-2199	M	**Problem:** LunaCM occasionally freezes in Windows 2016 when a new slot is created or deleted. **Workaround:** End the LunaCM instance with Task Manager and restart LunaCM.
LUNA-1927	M	**Problem:** Unable to add new member to HA group after removing primary member. **Workaround:** Manually delete the serial number of the deleted Network HSM's partition from the "VirtualToken00Members" field in the "Chrystoki.conf" (Linux/UNIX) file or "Crystoki.ini" (Windows) file and then add the new partition to the existing HA group. It is added successfully, and the old entry from the lunacm HA list is also removed.
LUNA-1725	M	**Problem:** In LunaCM, **partition archive restore -replace** does not replace DUPLICATED objects in target partition. **Workaround:** Remove all duplicate objects from the target partition prior to running **partition archive restore -replace**.
LUNA-1592	M	**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-2368	M	**Problem:** The **hagroup list** command returns an error. **Workaround:** Run the **hagroup list** command again. The second attempt should be successful.
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. **Workaround:** Remove any member partition from the HA group before zeroizing the host HSM.
LUNA-2347	L	**Problem:** Deprecated `PartitionPolicyTemplatePath` entry is present in the **MISC** section of **Chrystoki.conf**/**crystoki.ini**. **Workaround:** Ignore. This entry is not used by Luna 7 policy templates.
LUNA-2103	L	**Problem:** If you enter duplicate policies (policies with the same ID) in the partition policy template, the partition will take the last value. **Workaround:** Avoid duplicate policy IDs in partition policy template files.
LUNA-218	L	**Problem:** You cannot add a host or network route using the LunaSH **network route add** command without including the gateway value. **Workaround:** None.
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-2960	L	**Problem:** LunaCM hangs on exit on Windows 2016. **Workaround:** End the LunaCM instance using the Task Manager.

Issue	Severity	Synopsis
CPP-2925	L	**Problem:** When the **cklog** library is configured, an **error.txt** file containing extraneous messages may be created. **Workaround:** None.
CPP-2380	L	**Problem:** When running the **MiscCSRCertificateDemo.java** sample, a null pointer exception occurs. **Workaround:** None.
CPP-1249 LUNA-1681	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.

Resolved Issues

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

Table 4: List of resolved issues

Issue	Severity	Synopsis
LKX-3338	H	**Problem:** On Luna HSM *700 and *750 models, asymmetric digest-and-sign or digest-and-verify mechanisms produce the wrong result when the data length exceeds 64 kB. **Fixed:** Fixed in firmware 7.2.0 and 7.0.3.
LKX-3233 LKX-3201	H	**Problem:** Value for HSM policy 46 (Disable Decommission) cannot be changed. Attempting to change it returns an error (CKR_CONFIG_FAILS_DEPENDENCIES). **Fixed:** Fixed in firmware 7.2.0.
LUNA-2677	M	**Problem:** Unable to change CKA_EXTRACTABLE key attribute via Java (LunaProvider/JSP). **Fixed:** Fixed in Luna HSM Client 7.2.
LUNA-2300	M	**Problem:** Incorrect options displayed in LunaCM when running **hsm init** on SafeNet Luna PCIe HSM slot. **Fixed:** Fixed in Luna HSM Client 7.2.
LUNA-2081	M	**Problem:** Multipart AES_KW operations on non-block-sized-data returns incorrect error code CKR_DEVICE_ERROR. **Fixed:** Fixed in release 7.2.
LUNA-2077	M	**Problem:** On Windows, one-step NTLS is very slow and takes almost four minutes to complete the NTLS connection setup. **Fixed:** One-step NTLS performance has been improved in release 7.2.
LKX-3178	M	**Problem:** When you use an older client, and query partition-level capabilities and policies, the HSM returns incorrect policy numbers. **Fixed:** Fixed in firmware 7.2.0.

Issue	Severity	Synopsis
LKX-3159	M	**Problem:** In LunaCM, **hsm information monitor** incorrectly reports HSM utilization. **Fixed:** Fixed in firmware 7.2.0.
LKX-3042 LKX-2989	L	**Problem:** When partition policy 39: Allow start/end date attributes is enabled, all start dates must be later than January 01, 1970. **Fixed:** Fixed in firmware 7.2.0.

Revision History

Revision A: 07 May 2018

> Initial Release

Revision B: 17 August 2018

> Added to "New Features and Enhancements" on page 3:

- Version 7.2 and newer Luna HSM Client can be used with HSMs running Luna 6.2.1 or higher without conflict.
- The improved Luna HSM Client can be used to create mixed-version HA groups with Luna 6/7 partitions.

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/csm, 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 at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@gemalto.com.