SafeNet Luna PCIe HSM 7.1

CUSTOMER RELEASE NOTES

Issue Date: 23 January 2018

Document Part Number: 007-013579-003 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 7.1 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.

New Features and Enhancements

This section highlights what's new in SafeNet Luna PCIe HSM 7.1.

Policy Templates

The HSM or Partition SO can save a copy of their organization's preferred HSM or partition policy settings to a template. They can then use this template to configure policy settings when initializing other HSMs or partitions.

This can save time and effort when deploying multiple HSMs or partitions. It also ensures consistency across your HSMs and partitions, which helps to simplify future audit and compliance requirements. [Requires HSM firmware 7.1]

Configurable Policies for Export of Private Keys

The Partition SO can use partition policies to control whether or not the private keys in a given partition can be exported off the HSM. The ability to export private keys is particularly useful in use cases such as smart card & identity issuance, secure manufacturing, etc.

This gives organizations the ability to support a wider variety of use cases with their HSM, and also provides Partition SOs with more flexibility overall. [Requires HSM firmware 7.1]

Curve 25519 Available in FIPS Mode

Curve 25519 is now available for use in FIPS mode. [Requires HSM firmware 7.1]

Fixes

A number of items have been addressed for this release, and are listed in the Resolved Issues section of this document.

Advisory Notes

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

CKA_EXTRACTABLE=FALSE on New Private Keys

Private keys now have their CKA_EXTRACTABLE attribute set to FALSE by default when they are created. Your applications must specify a value of **1** (TRUE) for this attribute on private keys you wish to wrap and export in Key Export mode.

A patch for the Luna Java Provider (LunaProvider) on 32-bit and 64-bit Linux client systems is available from the Gemalto Customer Support Portal (DOW0002629).

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 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.

HA Groups Containing Members From Different Releases

You can configure an HA group containing release 7.1 and release 5/6.x partitions to easily migrate cryptographic objects to the new HSM.

NOTE Failover during sustained application in a mixed-release HA group has not been fully characterized for all failure scenarios.

Supported Operating Systems

This section lists the supported operating systems for the SafeNet Luna HSM client and Remote PED server.

SafeNet Luna HSM Client

You can install the SafeNet Luna HSM Client 7.1 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 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 7/8/9
- 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.

Upgrade Paths

Table 1: Upgrade Paths

Component	Directly from version	To version
SafeNet Luna HSM client software	Any	7.1
HSM firmware	7.0.1, 7.0.2	7.1.0
SafeNet Backup HSM firmware	6.10.9, 6.26.0	6.27.0
SafeNet Local PED/Remote PED firmware	2.7.1	N/A
	2.8.0	N/A

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 2: Issue severity definitions

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

Table 3: List of known issues, new for release 7.1

Issue	Severity	Synopsis
LKX-3233 LKX-3201	H	**Problem:** Value for HSM policy 46 (Disable Decommission) cannot be changed. Attempting to change it returns a “fails dependencies” error. **Workaround:**None.
LUNA-2677	M	**Problem:** Private key wrapping in Key Export mode does not work when using the Luna Java provider (LunaProvider). **Workaround:** Download and apply Linux client patch (DOW0002629) from the Gemalto Customer Support Portal. Follow the README instructions to ensure that your Java application sets the appropriate key attributes.
LUNA-2300	M	**Problem:** Incorrect options displayed in LunaCM when running **hsm init** on SafeNet Luna PCIe HSM slot **Workaround:** Ignore. The options to "Initialize a Backup Device with PED-Auth" and "Initialize a Backup Device with PWD-Auth" should appear only for a slot corresponding to a SafeNet Luna Backup HSM that is in un-initialized state.
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 SafeNet Luna HSM on Solaris, choose Network HSM only.
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-2081	M	**Problem:** Multipart AES_KW operations on non-block-sized-data returns incorrect error code CKR_DEVICE_ERROR. **Workaround:** None.
LUNA-1927	M	**Problem:Problem:** HA - Unable to add new member to HA group after removing primary member **Workaround:** Restart LunaCM to update the slot list.
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**.
LKX-3178	M	**Problem:** When you use an older client, and query partition-level capabilities and

Issue	Severity	Synopsis
		policies, the HSM returns incorrect policy numbers **Workaround:** Use the documentation to get the correct policy numbers.
LKX-3159	M	**Problem:** In LunaCM, **hsm information monitor** incorrectly reports HSM utilization **Workaround:** None.
LUNA-2347	L	**Problem:** Extraneous entry for partitionpolicytemplatepath is present in the MISC section of the Chrystoki.conf. **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.
LKX-3042	L	**Problem:** When partition policy 39: Allow start/end date attributes is enabled, all start dates must be later than January 01, 1970. **Workaround:** Ensure that start date attribute is later than January 01, 1970.

Table 4: List of known issues from release 7.0

Issue	Severity	Synopsis
LHSM-18236 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.
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-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-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-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.
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.

Issue	Severity	Synopsis
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.
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.
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.
CPP-2925	L	**Problem:** When the **cklog** library is configured, an **error.txt** file containing extraneous messages may be created. **Workaround:** None.
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 5: List of resolved issues

Issue	Severity	Synopsis
LUNA-853	M	**Problem:** On Linux, the SafeNet Luna HSM Client software fails to install to a directory with spaces in its name. **Fixed**
LUNA-264	M	**Problem:** On Linux, non-root users cannot initialize the STC token or create an STC client identity. **Fixed**
LUNA-263	M	**Problem:** On Linux, non-root users cannot configure the RBS server. **Fixed**
LUNA-262	M	**Problem:** On Linux, non-root users receive error (CKR_DATA_INVALID) when creating an HA group. **Fixed**

Issue	Severity	Synopsis
CPP-3385 LUNA-801	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. **Fixed**
CPP-632	M	**Problem:** When using CKdemo with HA groups, an **Attribute type invalid** error is returned. **Fixed**
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. **Fixed**
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. **Fixed**

Revision History

Revision B: 23 January 2018

> Added to "Advisory Notes" on page 2:

- CKA_EXTRACTABLE=FALSE on New Private Keys

> Added to "Supported Cryptographic APIs" on page 5:

- Java 9

> Added to "Known Issues" on page 5:

- LUNA-2677

Revision A: 7 December 2017

> Initial Release

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
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

Region	Telephone number (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
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