THALES

gemalto
a Thales company

SafeNet Luna PCIe HSM 7.3

CUSTOMER RELEASE NOTES

Issue Date: 18 July 2019

Document Part Number: 007-013579-005 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 7.3 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

SafeNet Luna PCIe HSM 7.3 introduces the following new features and enhancements:

HSM Firmware version 7.3.3 is FIPS 140-2 validated.

Firmware 7.3.3 update incorporates the features and fixes supported by firmware versions 7.1, 7.2 and 7.3, and is now the preferred FIPS-validated SafeNet Luna HSM firmware version.

CMVP Certificate #3205

See the "HSM Firmware version 7.3.3 caveats " on the next page in the Advisory Notes section, below.

BIP32 Algorithm

SafeNet Luna PCIe HSM 7.3 includes new mechanisms that use the BIP32 cryptographic algorithm. This allows SafeNet Luna PCIe HSM to support applications that use Hierarchical Deterministic Wallets, used in Bitcoin and blockchain transactions (requires firmware 7.3.0).

JavaSP support for ECC Curve 25519

The SafeNet Java Provider now includes support for mechanisms using ECC Curve 25519.

Fixes

Issues addressed in this release are listed in "Resolved Issues" on page 12.

Advisory Notes

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

HSM Firmware version 7.3.3 caveats

Firmware 7.3.3 update incorporates the features and fixes supported by firmware versions 7.1, 7.2 and 7.3, and is now the preferred FIPS-validated SafeNet Luna HSM firmware version.

The firmware version shipped from the factory remains 7.0.3. Version 7.3.3 is a field-installable update.

Update paths and considerations

From f/w version	To f/w version	Comment or caveat
PASSWORD-AUTHENTICATED		
7.0.3, 7.1.0, 7.2.0, 7.3.0	7.3.3	Normal firmware update procedure (see Updates and Upgrades section of main HSM documentation) - no issues.
PED-AUTHENTICATED		
7.0.3	7.3.3	Normal firmware update procedure (see Updates and Upgrades section of main HSM documentation) - no issues.
partition created in HSM at one of f/w versions 7.1, 7.2, or 7.3.0 with Partition Policy 15 set to ON	7.3.3	Normal firmware update procedure (see Updates and Upgrades section of main HSM documentation) - EXCEPT you must reset the challenge secret, after f/w update, so that partition objects become accessible again.
Partition created in HSM at one of f/w versions 7.1, 7.2, or 7.3.0 with Partition Policy 15 set to OFF (*)	7.3.3	1. Before updating firmware, back up your partition contents. 2. Update your HSM to firmware version 7.3.3. 3. Your existing partition is no longer accessible -- re-initialize the existing partition. 4. Restore your partition objects from backup.

(* By default, Partition Policy 15 is off. Turning Policy 15 ON is destructive.)

Resolved Issue LUNA-7533: Java DERIVE and EXTRACT flag settings for keys injected into the HSM

Formerly, the DERIVE and EXTRACT flags were forced to "true" in the JNI, which overrode any values passed by applications via Java. This is resolved in Luna 7.3 release.

As of release 7.3:

- The default values for the DERIVE and EXTRACT flags are set to "false" (were set to “true” in previous releases.
- JNI accepts and preserves values set by applications via the following Java calls:

```
LunaSlotManager.getInstance().setSecretKeysDerivable( true );
LunaSlotManager.getInstance().setPrivateKeysDerivable( true );
LunaSlotManager.getInstance().setSecretKeysExtractable( true );
LunaSlotManager.getInstance().setPrivateKeysExtractable( true );
```

> **NOTE** If you have existing code that relies on the DERIVE and EXTRACT flags being automatically defined by the JNI for new keys, you will need to modify your application code to set the flag values correctly.

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 7.3 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

Detailed procedures for installing the SafeNet Luna PCIe HSM 7.3 software and firmware updates can be found in the product documentation. Before you install any of the updates, consider the following guidelines:

- 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.
- For firmware 7.3.3 see "Update paths and considerations " on page 3 in case your HSM is affected by a special case.

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	7.3
SafeNet Luna HSM firmware	7.0.1, 7.0.2	7.0.3, 7.2.0
	7.0.3, 7.1.0, 7.2.0, 7.3.0	7.3.3*
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

(* Check the CRN "Advisory Notes" section, to see if any caveat applies to your HSM)

(** Note that firmware 6.24.7 is the latest FIPs-validated version for the Backup HSM. FIPS validation might not be strictly necessary for a Backup HSM because it does not perform cryptographic operations with contained objects, but some audit checklists might not make that distinction.)

FIPS-Validated Firmware Versions

The following firmware versions are all FIPS-140-2 Level 3 certified per certificate #3205:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3205

- Luna firmware v. 7.3.3 (recommended)
- Luna firmware v. 7.0.2 (see F5 note, below)
- Luna firmware v. 7.0.3

Recommended Minimum Versions

Generally, Gemalto recommends that you always keep your HSM firmware and client software up to date, to benefit from the latest 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.

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 7.3

Issue	Severity	Synopsis
LKX-4868	H	**Problem:** On a 64-bit client operating system, running **multitoken** with different BIP32 modes against an STC HA virtual slot causes **multitoken** to fail with an error (CKR_TOKEN_NOT_PRESENT). **Workaround:** Do not use BIP32 modes with STC HA groups; use NTLS instead.
LKX-4543	H	**Problem:** After a firmware update, duplicate entries are produced in the audit logs. These duplicate entries cause log verification to fail with an error (CKR_LOG_BAD_RECORD_HMAC). **Workaround:** There is no way to avoid the duplicate entries. However, the other entries in the log file can be verified without error. When verifying the logs, specify a range that excludes the duplicate entries: lunacm:>**audit verify file** <log_file> **start** <first_entry> **end** <last_entry>
LUNA-7438	H	**Problem:** When using **CKdemo** to perform a multipart sign/verify operation with a key that has exceeded its specified usage count, an expected error is returned (CKR_KEY_NOT_ACTIVE). The next sign/verify operation with an active key fails with an unexpected error (CKR_OPERATION_ACTIVE). **Workaround:** Restart **CKdemo** and attempt the operation again.
LUNA-7436	H	**Problem:** Encrypt operations using DES3_CBC_PAD and specifying a NULL buffer fail (CKR_BUFFER_TOO_SMALL). **Workaround:** Manually specify a buffer size for these operations.
LKX-4852	M	**Problem:** Reset timestamp displayed when reporting metrics via LunaSH or REST can vary, each time the commands are used, by approximately 6s. **Workaround:** Reset the timers. This causes the value to be written to a file, so that the reported reset time remains constant until the next reset.
LKX-4250	M	**Problem:** CA_DeriveKeyAndWrap does not handle AES_KW, AES_KWP, or AES_CTR mechanisms. **Workaround:** None.
LUNA-7170	M	**Problem:** When installing PCIe HSM 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 Luna HSM Client.
LUNA-7074	M	**Problem:** In LunaCM, when switching the active slot between partitions on different HSMs, **ped connect** and **ped get** sometimes report an active Remote PED connection, even though the connection is broken. Authentication commands fail. **Workaround:** Use **ped disconnect** on the active slot before switching to a different slot and running **ped connect**.

Issue	Severity	Synopsis
LUNA-7430	L	**Problem:** When running commands in some Luna utilities on Windows 10, password characters are duplicated. **Workaround:** Contact Gemalto Customer Support.
LUNA-7194 RAPI-1416	L	**Problem:** Webserver starts even if no SSL key/cert exists, but is not accessible. **Workaround:** Generate the SSL key/cert before starting the webserver.

Table 3: List of known issues from prior releases

Issue	Severity	Synopsis
LKX-3184	M	**Applies to firmware 7.0.3 only. This issue has been fixed in firmware 7.2.0 and later.** **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.
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.x HSM.
LUNA-3691	M	**Problem:** When resetting the HSM to factory conditions with audit logging enabled and an existing audit log file, new events are not logged after the Auditor role is re-initialized. **Workaround:** None.
LUNA-3683	M	**Problem:** On Linux clients, when a non-root user attempts to uninstall the Luna HSM Client software, the process fails and the client software remains installed, but "`Uninstall of the Luna HSM Client 7.3.0-165 completed`" is displayed in the command output. **Workaround:** Ignore this message and log in as the root user to uninstall the Luna HSM Client software.
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-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/crystoki.ini. Refer to the *SDK Reference Guide* for details.
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.
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.
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) 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.

Issue	Severity	Synopsis
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-632 LUNA-7429	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-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-3511	L	**Problem:** Audit logging -- **hsm zeroize** is not logged after performing a factory reset of the HSM, since the audit configuration is erased during factory reset. **Workaround:** None.
LUNA-3276	L	**Problem:** When installing the Luna HSM Client software to a custom directory with spaces in the directory name, the installer creates a new named directory that ignores everything after the first space. **Workaround:** Do not use spaces when naming your custom install directory.
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**.

Issue	Severity	Synopsis
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-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
LUNA-7533	M	**Problem:** Java DERIVE and EXTRACT flag settings for keys injected into the HSM. The DERIVE and EXTRACT flags were forced to "true" in the JNI, which overrode any values passed by applications via Java. **Resolved:** Fixed in Luna release 7.3.
LUNA-7258	M	**Problem:** When running **cmu** commands on Windows 10, password characters are duplicated. **Resolved:** Fixed in Luna release 7.3.
LUNA-3275	M	**Problem:** When using CKdemo to query an application partition, the Crypto Officer password is entered in visible plaintext. **Resolved:** Fixed in Luna release 7.3.
LUNA-3298	M	**Problem:** When installing Backup HSM and Luna 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. **Resolved:** Fixed in Luna HSM Client release 7.3.

Issue	Severity	Synopsis
LUNA-3167	M	**Problem:** Cannot migrate keys using MS2Luna.exe for CSP. **Resolved:** Fixed in Luna release 7.3.
LUNA-3071	M	**Problem:** When LunaCM is launched in Luna Minimal Client, an unexpected error is displayed (Error: Failed to initialize remote PED support). **Resolved:** Fixed in Luna HSM Client release 7.3.
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. **Resolved:** Fixed in Luna HSM Client release 7.3.

Revision History

Revision A: 21 September 2018

> Initial Release

Revision B: 02 May 2019

> Added to **Advisory Notes**: "Product Description" on page 2

Revision C: 20 July 2019

> Added to **Advisory Notes**: "HSM Firmware version 7.3.3 is FIPS 140-2 validated. " on page 2

> Added to **Advisory Notes**: "HSM Firmware version 7.3.3 caveats " on page 3

> Updated **Valid Update Paths** table in "Update Considerations" on page 6

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

The support portal also lists telephone numbers for voice contact. (KB0013367)

Email Support

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