SafeNet HSM 6.2.3

CUSTOMER RELEASE NOTES

Issue Date: 16 March 2017

Document Part Number: 007-012225-009 Rev. A

The most up-to-date version of this document is at:

http://www.securedbysafenet.com/releasenotes/luna/crn_luna_hsm_6-2-3.pdf

Product Description

The SafeNet HSM (hardware security module) family provides FIPS-certified, PKCS#11-compliant cryptographic services in a high-performance, ultra-secure, and tamper-proof hardware package. By securing your cryptographic keys in hardware, SafeNet HSMs provide robust protection for your secure transactions, identities, and applications. They also offer high-performance encryption, decryption, authentication, and digital signing services.

SafeNet Network HSM

SafeNet Network HSM is a network-based, Ethernet-attached HSM appliance that offers high-availability configuration options, remote management PED and backup, and dual hot-swappable power supplies. SafeNet Network HSM provides cryptographic services for network clients that are authenticated and registered against HSM partitions. Two performance variants are available, the SafeNet Network HSM-1700 and SafeNet Network HSM-7000, which are capable of 1700 and 7000 (RSA 1024-bit) signings per second respectively.

Release Description

SafeNet HSM Release 6.2.3 :

- is a factory release of the SafeNet Network HSM appliance, only (the SafeNet USB HSM and SafeNet PCI-E HSM are not included)
- is a new Client, Network HSM appliance software, and Appliance/Backup HSM firmware implementing the Scalable Key Storage feature
- is not a field upgrade of any earlier release
- supports all features of release 6.2.2, except
  - Per-partition Security Officer (PPSO)
  - Host Trust Link (HTL -- deprecated feature)
  - NTLS Keys in Hardware
  - Secure Trusted Channel (STC)
  - Small Form-Factor Backup (SFF)
  - Crypto Command Center (CCC)
  - firmware rollback (from version 6.25.0)
- only PED-authenticated HSMs are supported
- a maximum of one partition is supported on the HSM

A Scalable Key Storage HSM can be identified by two entries in the lunashell "hsm displaylicenses" command output:

- Scalable key storage
- Enable network replication

An SKS HSM must be ordered from the factory. Non-SKS HSMs in the field cannot be upgraded to SKS functionality.

A Scalable Key Storage Remote Backup HSM can be identified by the firmware version 6.25.x. (lunacm "hsm showinfo" command). If you have a cloning (non-SKS) Remote Backup HSM with any firmware other than 6.25.x, it cannot be upgraded to become an SKS Remote Backup HSM in the field. An SKS Remote Backup HSM must be ordered from the factory. An SKS Network HSM can be backed up only to an SKS Remote Backup HSM.

Note: Apply a physical label to differentiate your SKS Backup HSM, if you possess any non-SKS Backup HSMs.

Critical Information

Patch 6.2.4 **must** be applied and firmware version updated to 6.25.1 **before** using the HSM.

Any SKS-encrypted blobs created prior to the 6.2.4 field update will not be usable after the update is applied. Due to this issue, the stability of High Availability synchronization, autorecovery, and manual recovery features is adversely affected.

Therefore, all customers must apply the 6.2.4 field update before using the SKS HSM (and SKS Backup HSM).

New Features and Enhancements

The following is a summary of the single feature new to SafeNet Network HSM 6.2.3

Scalable Key Storage (SKS)

Scalable Key Storage, or SKS, adds the ability to extract keys from the HSM as encrypted BLOBs and then insert the key BLOBs back into the HSM at a later time, when the key is needed, in a secure manner. This feature addresses use-cases where the number of keys needed for your application exceeds the capacity of the HSM. This allows for highly scalable solutions.

Scalable Key Storage is one of three main configurations of SafeNet HSM, available from the factory: Cloning, Key Export, and SKS.

CAUTION: You must apply field update 6.2.4 to your 6.2.3 HSM appliance (updates appliance software to version 6.2.4, and both appliance HSM and Backup HSM firmware to version 6.25.1) before using the HSM.

The following are summaries of features new to SafeNet HSM in release 6.2.2 and applicable to 6.2.3, 6.2.4, and newer, as well.

HA Auto-Reconnect

The HA feature now includes the ability of the Client to reconnect and resume application operation, without intervention, after completely losing contact with the HA group of HSMs. Context is retained, and token object states are preserved. Login is hands-free.

HA Failover withstands member deactivation and reconnects on activation of member partition

The following scenarios are addressed in 6.2.2 Client:

- When an application starts up the HA system ensures that the partition is activated.
- If a member has failed, during recovery the system checks that the partition is activated and confirms activation before the member is added back to the group.
- When a new member is being added to an HA group, the system checks whether or not the new member partition is activated and subsequently ensures activation before the member is successfully added to the HA group.

Network HSM gets OpenSSL upgrade

The SafeNet Network HSM receives enhanced OpenSSL to address the vulnerability described in CVE-2016-6304.

Advisory Notes

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

SKS Notes

The SKS feature is a factory-only release of the Network Appliance HSM and the SKS Backup HSM, both at firmware 6.25.0.

- There is ***no*** ability to modify existing units in the field to install SKS functionality.
- SKS HSM supports a single application partition, with the SKS Master Key (or SMK) created when the partition is created.
- SKS backup and restore operations archive only the SMK (not crypto objects).
- The SKS Backup HSM can backup multiple SMKs, but requires a unique partition for each one.
- SIM Multisign is not supported for this release.
- The SKS object (blob) preserves all attributes, including fingerprints.
- The SKS object and header have SHA512 integrity. Objects are encrypted using AES-GCM with random IV per object.
- Key creation, blob export, blob import, and encryption/decryption of data records make use of session objects exclusively - only the SKM resides in flash memory, so there are no ongoing flash rewrite operations when using the SKS feature.

CAUTION: Do ***not*** perform firmware roll-back; the available roll-back firmware direct from factory is a place-holder version and cannot support the SKS capability. Rolling forward again, after that rollback, would not restore the capability. If a rollback operation is performed, the unit will need to be returned to the factory for reprovisioning.

Notes from recent releases

Terminology Change

The feature formerly called SIM is now called Scalable Key Storage. The Capability Update now appears under that name when capabilities are listed. The terminology has also been updated throughout the documentation where appropriate.

Create a new SSL/NTLS Certificate on first use

All SafeNet Network HSMs come from the factory with the same SSL (NTLS) key. For proper security, run the **sysconf regencert** command before configuring your system for first use.

After SRK is enabled lunacm reports transport mode disabled

If Lunacm **srk show** command does not show the expected state for SRK after you run this command, the cache might not have been updated, following the most recent change. Exit and re-launch lunacm to see the current state of SRK.

Minimum Recommended Firmware for SafeNet Remote Backup HSM

For SKS-capable HSMs (release 6.2.3), the Backup HSM should be at firmware version 6.25.0.

SQL 2016 Support

Firmware 6.25.0 supports SQL 2016 only in non-FIPS mode.

HTL is deprecated

The HTL feature is now deprecated, and will be discontinued in a future release. If you have been using HTL, please plan for configuration and work-flow that does not make use of it.

Compatibility and Upgrade Information

The SafeNet Network HSM appliance version 6.2.3 is configured and shipped from the factory. There is no provision to field-upgrade to version 6.2.3 from other versions.

	Appliance Software	HSM Firmware	Client Software
SKS HSM Network Appliance	6.2.3	6.25.0	6.2.3
SKS Backup HSM	n/a	6.25.0	6.2.3

Orderable configurations and bundles

Part numbers for orderable items/bundles include:

908-000353-001 LUNA SA 7000 PED-AUTHENTICATED,1 HSMP,SKS,SW 6.2.3,FW 6.25.0

908-000354-001 LUNA SA 1700,PED-AUTHENTICATED,1 HSMP,SKS,SW 6.2.3,FW 6.25.0

908-000355-001 LUNA REMOTE BACKUP HSM FOR SKS,FW 6.25.0

908-000356-001 LUNA SA 7000 REMOTE PED BUNDLE (1 HSMP,SKS,SW 6.2.3,FW 6.25.0,REMOTE PED,20 PED KEYS,BACKUP HSM)

908-000358-001 LUNA SA 1700 REMOTE PED BUNDLE (1 HSMP,SKS,SW 6.2.3,FW 6.25.0,REMOTE PED,20 PED KEYS,BACKUP HSM)

Note: If you intend to backup the SMK (which should be mandatory in any production environment), you will need at least one SKS Backup HSM. Regular Backup HSMs for archiving crypto objects are not supported for SKS.
However, you can use your SKS HSM to archive crypto objects

Certifications and Compliance

About FIPS Validation

Note: HSMs with firmware 6.25.0 (for SKS) are not FIPS validated at this time, and have not been submitted for evaluation.

About Common Criteria

Note: HSMs with firmware 6.25.0 (for SKS) are not Common Criteria validated at this time, and have not been submitted for evaluation.

Supported Operating Systems

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

SafeNet HSM Client

Operating system	Version	64-bit client installer on 64-bit OS	32-bit applications on 64-bit OS	32-bit client installer on 64-bit OS	32-bit client installer on 32-bit OS
Windows **Note:** The 64-bit Windows installer also installs the 32-bit libraries for compatibility with 32-bit client applications. No standalone 32-bit SafeNet HSM client is available.	2008 R2	Yes	Yes	No	No
	2012 R2	Yes	Yes	No	No
	2016	Yes	Yes	No	No
	10	Yes	Yes	No	No
Redhat-based Linux (including variants like CentOS and Oracle Enterprise Linux)	5	Yes	Yes	Yes	Yes
	6	Yes	Yes	Yes	Yes
	7	Yes	Yes	Yes	Yes

Remote PED Server

The remote PED server must be installed on any workstation used to host a remote PED. The remote PED server software is supported on the following Windows operating systems only:

- Windows 2016
- Windows 2012 and 2012 R2
- Windows 2008 R2
- Windows 10
- Windows 7 (64-bit)

Supported APIs

The following APIs are supported :

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

RADIUS Compatibility

For this release, we support the use of one RADIUS server, only.

Update Instructions

(SafeNet GPHSM release 6.2.3 is shipped from the factory and is not an upgrade/update from an earlier version.)

HSM Summary Information

The following is the output of "hsm show" command for a SafeNet Network HSM release 6.2.3.

```
Luna SA 6.2.3-1 Command Line Shell - Copyright (coffee) 2001-2017 SafeNet, Inc. All r ights
reserved.

[auto224] lunash:>hsm show


   Appliance Details:
   ==================
   Software Version: 6.2.3-1

   HSM Details:
   ============
   HSM Label: mysa
   Serial #: 156674
   Firmware: 6.25.0
   HSM Model: K6 Base
   Authentication Method: PED keys
```

```
   HSM Admin login status: Not Logged In
   HSM Admin login attempts left: 3 before HSM zeroization!
   RPV Initialized: Yes
   Audit Role Initialized: No
   Remote Login Initialized: No
   Manually Zeroized: No

   Partitions created on HSM:
   ==========================
   There are no partitions.


   Number of partitions allowed: 1
   Number of partitions created: 0

   FIPS 140-2 Operation:
   ====================
   The HSM is NOT in FIPS 140-2 approved operation mode.

   HSM Storage Information:
   ========================
   Maximum HSM Storage Space (Bytes): 2097152
   Space In Use (Bytes): 0
   Free Space Left (Bytes): 2097152


Command Result : 0 (Success)
```

The following is the output of "hsm showinfo" command for a SafeNet Backup HSM release 6.2.3.

```
lunacm:> hsm si

        Partition Label -> StellaG5BkSIM
        Partition Manufacturer -> Safenet, Inc.
        Partition Model -> G5Backup
        Partition Serial Number -> 475289
        Partition Status -> OK
        Token Flags ->
                CKF_RNG
                CKF_USER_PIN_INITIALIZED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
                CKF_TOKEN_INITIALIZED
        RPV Initialized -> No
        Slot Id -> 28
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID: 00000000000000000099400700

        Partition Storage:
                Total Storage Space:  262144
                Used Storage Space:   52604
                Free Storage Space:   209540
                Object Count:         4
                Overhead:             9424

        *** The HSM is NOT in FIPS 140-2 approved operation mode. ***
```



```
        Firmware Version -> 6.25.0
        Rollback Firmware Version -> 6.0.8
        HSM Storage:
                Total Storage Space:  16252928
                Used Storage Space:   21748
                Free Storage Space:   16231180
                Allowed Partitions:   20
                Number of Partitions: 2

        License Count -> 5
                1. 621010355-000 Luna remote backup HSM base configuration
                1. 621000006-001 Enabled for 15.5 megabytes of object storage
                1. 621000007-001 Enable the master tamper key to be stored externally
                1. 621000008-001 Enable remote PED capability
                1. 621000005-001 Maximum 20 partitions

Command Result : No Error
```

The following is the output of "slot list" command for a SafeNet Backup HSM release 6.2.3 (firmware 6.25.0).

```
Slot Id -> 3
HSM Label -> no label
HSM Serial Number -> 7002733
HSM Model -> G5Backup
HSM Firmware Version -> 6.25.0
HSM Configuration -> Luna G5 (PED) Undefined Mode / Uninitialized
HSM Status ->  Zeroized
Current Slot Id: 1
```

Known Issues

This section lists the issues known to exist in the product at the time of release. Workarounds are provided where available.

Issue Priority Definitions

The following table defines the priority of the issues listed in this section.

Priority	Classification	Definition
C	Critical	No reasonable workaround exists.
H	High	Reasonable workaround exists.
M	Medium	Medium level priority problems.
L	Low	Lowest level priority problems.

Known Issues

Issues from release 6.2.3

Issue	Priority	Synopsis
LHSM-42420	C	**Problem:** OUIDs in HA members are NOT the same When a key was generated from HA slot, in each of HA members it should have the key with the same uid, but in 6.2.3, they are different.
LHSM-42487	M	**Problem:** Inserting an existing SKS object should return a more meaningful message If the SKS object already exists on the HSM, CA_SIMInsert returns CKR_CANCEL, which is ambiguous. It should return "Object already exists."
LHSM-42408 / LHSM-42436	M	**Problem:** HA slot "partition contents" throws CKR_OBJECT_HANDLE_INVALID error
LHSM-42389	M	**Problem:** sysconf config factoryReset issue When performing "sysconfig config factoryReset", previously configured network setting maybe lost. When the Network HSM appliance is rebooted, it can come back with a new DHCP configured IP address. If the appliance is configured for radius server, ssh login after the reboot might result in some delay as radius server does not recognise the new IP as a registered client. **Workaround:**When the Network HSM appliance is rebooted after performing "sysconfig config factoryReset", ensure that network configuration is updated such that the HSM appliance is assigned an IP address that is registered with the radius server.
LHSM-42323	H	**Problem:** Snmp Trap Missing trap messages are generated locally at the Network HSM appliance /var/log however they are not being sent out to rsyslog.
LHSM-42322	M	**Problem:** Mismatched configuration in LunaCM for SIM partitions
LHSM-42320	M	**Problem:** SSH to SA Audit Role Failed at public-key Authentication with error "Unsupported option "gssapiauthentication""

Resolved Issues

This feature-only release does not fix any previously unresolved issues. The Known Issues list from release 6.2.2 remains valid.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, ensure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Consult that support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact method	Contact
Customer Support Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.