xylem
Let's Solve Water

INTEGRATION GUIDE

AIG-10023-27

FlexNet RNI Hardware Security Module

SENSUS
a xylem brand

Revision history

Rev No.	Date	Description
01	10-OCT-10	Initial version.
02	16-APR-12	Updated for RNI 3.1.
03	8-OCT-12	Updated for RNI 3.1 SP2.
04	24-JUL-14	Updated for RNI 3.1 SP4.
05	30-JUL-15	Updated for RNI 3.3.
06	16-FEB-16	Updated for RNI 4.0.
07	5-OCT-16	Updated for RNI 4.1.
08	9-DEC-16	Updated for RNI 4.1.2.
09	23-MAR-17	Updated for RNI 4.1.3.
10	28-FEB-18	Updated for RNI 4.3.
11	08-JUN-18	Updated for RNI 4.3.1.
12	28-AUG-18	Updated for RNI 4.4.0.
13	26-OCT-18	Updated for RNI 4.4.1.
14	25-FEB-19	Updated for RNI 4.5.0.
15	29-APR-19	Updated for RNI 4.5.1.
16	27-AUG-19	Updated for RNI 4.6.0.
17	29-OCT-19	Updated for RNI 4.6.1.
18	26-FEB-20	Updated for RNI 4.7.0.
19	30-APR-20	Updated for RNI 4.7.1.
20	28-AUG-20	Updated for RNI 4.8.
21	10-JUN-21	Updated for RNI 4.9.
22	18-JAN-22	Updated for RNI 4.10.
23	23-FEB-22	More updates for RNI 4.10.
24	06-JUN-22	Updated for RNI 4.11.
25	02-DEC-22	Updated for RNI 4.12.
26	16-JUN-23	Updated for RNI 4.13.
27	25-NOV-23	Updated for RNI 4.14.

Copyright

Sensus
637 Davis Drive
Morrisville, NC 27560
1-800-638-3748
www.sensus.com

Document: FlexNet® RNI Hardware Security Module Installation Guide
Document Number: AIG-10023-27

Contents

Introduction

Sensus provides support for the integration of Hardware Security Modules (HSM) into our Regional Network Interface (RNI) software. The integration of an HSM into the Sensus solution provides customers with a dedicated hardware solution for managing cryptographic keys, accelerating cryptographic processes, and providing strong authentication to access critical keys for Sensus applications. HSMs are physical devices in the form of a plug-in PCI card or an external network-based security device that attaches directly to the network for access.

There are several advantages to using an integrated HSM:

- Onboard secure generation and storage of symmetric and asymmetric keys in hardware
- Use of cryptographic and sensitive data material inside the HSM rather than in software
- Offloading application servers for complete asymmetric and symmetric cryptography processing

HSMs provide both logical and physical protection of high-value cryptographic keys from non-authorized use and potential adversaries.

This document was written to be impartial regarding the specific version or type of Thales network HSM that can be used. The primary focus is to demonstrate guidance through installation and support of the Universal Luna Client for Luna 7 model hardware.

Note: Please note that certain terms such as Luna Client, Universal Client, Luna Client SA, and/or Universal Client are the same and relate to the Luna Client software as installed on the RNI.

Architecture

There are three types of HSM that are manufactured by Thales: Network HSM, PCIe HSM, and USB HSM. For our purpose, we are validating interoperability in using the Luna Network S700 with NTLS (Network Trust Links) provisioned. The Thales network HSM comes in various models such as (the Luna A Series, and Luna S Series. The main differentiators between these two HSM appliance types are that the A Series models use Password management as its base for management and authentication, while the Series S models use Multifactor PED Authentication. Both models also offer three different model variations that are based on their ability to scale/perform encrypted transactions per second, the number of supported partitions, and the amount of physical memory that is on board.

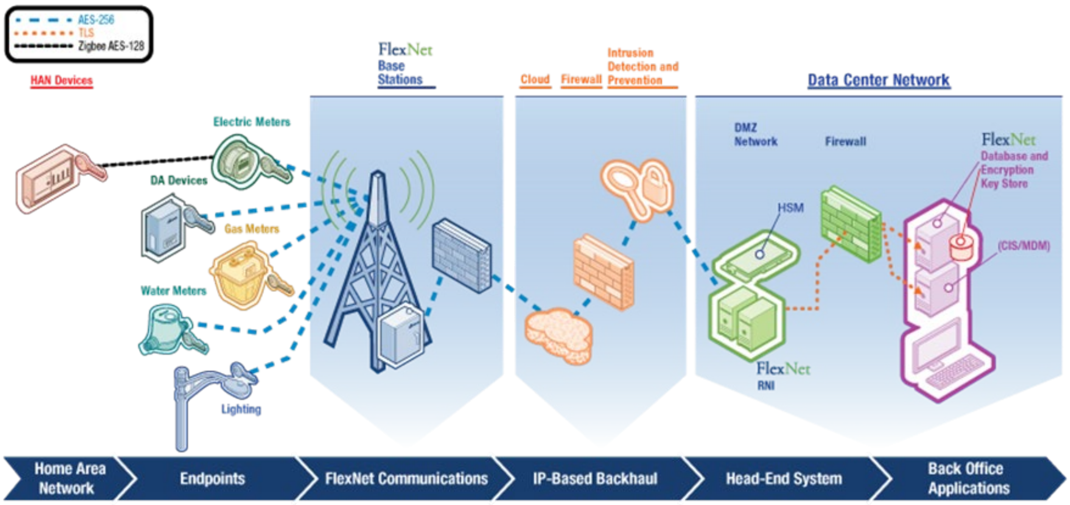

Figure 1 – FlexNet End-to-End Security

Note: Sensus will work with customers on an individual basis to determine the best solution for their requirements. Additional information is available during these discussions about configuration.

Security options

The HSM has several security configuration options. Depending on the level of security required by the customer, Sensus can configure the HSM to meet these security requirements.

Table 1 - HSM security options

Authentication Model	HSM Startup	Master Key Create/Rotate	FIPS 140-2 Compliance
None	No Action required	No action required	Level 2
Password-based	Password required	Password required	Level 3
Single USB token with PIN	Single USB Token with PIN required	Single USB Token with PIN required	Level 3
Multiple USB tokens with PIN	Multiple USB Tokens (M of N) required with PIN*	Multiple USB Tokens (M of N) required with PIN*	Level 3

Installation

Prerequisites

- The Luna appliance must be physically installed and configured prior to installation of the RNI software.
- The creation of an HSM partition is recommended prior to installing the Universal Client software.

- During RNI installation, please choose ***not*** to select the HSM option. There are some subtle differences in how the (Token ID) is generated between Luna 5 and Luna 7 releases. To avoid confusion, HSM configuration attributes can be added manually. This is further described within this document.

Note: The (Token ID) is no longer created on the PED display automatically for LUNA 7. This must be created through role management.

Supported versions

The current supported versions of the HSM Appliance Software, HSM Firmware, and Luna Client are as follows:

Note: Thales has officially retired Luna 5/6 Hardware/Software. A bulletin/notice regarding this has been documented here:
End of Sale and End of Support for SafeNet Luna HSM 5.x/6.x

Note: If you have not yet migrated from Luna 5/6 to the later Luna 7 Platform, please contact your Sensus/Xylem Technical Manager about engaging with Thales.

Luna 7 Hardware

- Software: 7.8.1-174 (Thales Article Details KB0026671)
- Firmware: 7.8.1 (Thales Article Details KB0026671)
- HSM Bootloader: 1.1.5
- LunaSA Client: 10.5.1-174 (Thales Article Details KB0026648)
- Luna PED: V.2.9.0-2
- Luna USB Backup HSM: 7.7.2

Note: Prior to integration with the RNI, ensure that the HSM environment is configured with the preceding software versions.

Note: Newer Thales Luna software releases may have become available during our testing. This is the baseline that was used during integration.

Installation considerations

Important: This procedure assumes that you have migrated your data from all previous Luna 5/6 platforms. If you have not, please contact your Sensus/Xylem Technical Manager about engaging with Thales and do not proceed.

- **Current HSM user/customer**: You are currently an HSM customer/user that is using the Luna 7 HSM Appliance.
- **New HSM user/customer**: You are integrating an HSM for the first time with the Luna 7 HSM appliance.

Current HSM user/customer (Luna 7)

This installation will continue to use the Luna Universal Client as described within the Universal Client Installation section of this document. Installation of the Client software is very similar as it was in previous Luna 5/6 installations. It is important to note that what is described in this section is complimentary to specific language written within Thales literature. Additional commentary has been added beyond Luna Client installation as a guide. This should follow the scheme of:

1. Maintaining your current attributes located in /opt/flexnet/conf/flexnet.local.properties on the RNI.

   ```
   fce.hsm.use=true
   fce.hsm.token.label=Sensus-Test
   fce.hsm.token.id=gibberish
   fce.hsm.version=LUNA5
   ```

Note: The attributes listed above are only an example. Please refer to your configuration characteristics.

2. It is assumed that you already have a partition already created on the HSM itself. If not, you will need to create one.
3. Follow installation of the Universal Luna Client on the RNI as indicated below in the Universal Client Installation section.
4. Follow the steps as identified in Configure Universal Client software.
5. The following policy attributes have been enabled.

Example:

```
>partition changePolicy -par Sensus-Test -po 22 -v 1

'partition changePolicy' successful.
Policy "Allow activation" is now set to: On
```

Command Result: 0 (Success)

Example:

```
>partition changePolicy -par Sensus-Test -po 23 -v 1
```

6. Activate the Partition.

Example:

```
>partition activate -par Sensus-Test

Please enter the password for the partition:
>gibberish

Luna PED operation required to activate partition on HSM - use
Partition Owner (black) PED key.
'partition activate' successful
```

New HSM user/customer (Luna7)

This procedure should relate to the customer/user that is onboarding the Luna 7 HSM Appliance as a first-time endeavor and/or fresh installation. If this is the case, please reference Appendix A on page 11 for links to consider/review. This includes documents that detail how to recover your HSM from Secure Transport Mode, general commissioning, configuration capabilities, upgrading, patching, high-availability, and so forth. This procedure also assumes that the customer has fully commissioned their HSM and can use this section of the document as a complimentary means.

Note: Some of these steps are high-level and require frequent interactions with PED commands and/or other steps.

1. Follow the installation of the Luna Universal Client as described within the Universal Client Installation section of this document.

2. Create a new partition on the HSM.

Example:

```
[sectest2] lunash:>partition create -partition Sensus-Test

Type 'proceed' to create the partition, or
'quit' to quit now.
> proceed
'partition create' successful.
```

3. From the RNI, initialize the partition.

Example:

```
lunacm:>partition init -label Sensus-Test

You are about to initialize the partition.
All contents of the partition will be destroyed.
Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now ->proceed

Please attend to the PED.
```

Command Result: No Error

4. On the RNI, login with the PO role.

Example:

```
lunacm:>role login -name po

Please attend to the PED.
```

Command Result: No Error

5. From the RNI, make the following partition policy changes:

```
lunacm:>partition changepolicy -policy 22 -value 1
```

Command Result: No Error

```
lunacm:>partition changepolicy -policy 23 -value 1
```

Command Result: No Error

6. From the RNI, initialize the CO role.

```
lunacm:>role init -name co
```

```
Please attend to the PED.
```

Command Result: No Error

7. Create challenge secret for the CO role.

```
lunacm:>role createchallenge -name co

Please attend to the PED.

enter new challenge secret: originalpwd

re-enter new challenge secret: originalpwd
```

Note: This can be set to a user-defined value.

Command Result: No Error

8. Logout of the PO role.

Example:

```
lunacm:>role logout
```

Command Result: No Error

9. From the RNI, login using the CO role.

Example:

```
lunacm:>role login -name co

enter password: originalpwd
```

Note: This is the password that you created in Step 8.

```
Please attend to the PED.
```

Command Result: No Error

10. This step creates the fce.hsm.token.id that we need for our configuration in /opt/flexnet/conf/flexnet.local.properties.

Example:

```
lunacm:>role changePW -name co -old originalpwd -newpw gibberish

This role has secondary credentials.
You are about to change the secondary credentials.
Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now ->proceed

Please attend to the PED.
```

Universal Client installation

The installation software for the 10.5.1 Universal Client is available from Thales (formerly Gemalto). You may download the software from the web site at the following URL: Thales Customer Support Portal - Thales Customer Support (thalesgroup.com)

Note: A service account is needed to download software from Thales.

Note: If a previous client is installed, you need to uninstall it.

1. Download the Luna 10.5.1 Universal Client software.
2. Copy the software package to the Network Controller server (for example, /tmp).
3. Extract the software package to a directory for example:

   ```
   tar -xvf 610-000397-007_SW_Linux_Luna_Client_V10.5.1_RevC.tar
   ```

4. Install Luna SA Client Software:

   a. Change the directory to the location of the LunaSA client software to /tmp/LunaClient_10.5.1-174_Linux/64

   b. Run the install program:

      - ./install.sh
      - Answer **Y** to accept License packaging terms.
      - Accept the default installation directory of /usr and press Enter.
      - Select Option #1 Luna Network HSM, and then type N|n for next, and press Enter.
      - Select Option #2 Luna JSP (Java), and the type I|i Install, and press Enter.
      - The installation completes.

5. Issue the following command:

   ```
   cd /usr/safenet/lunaclient/jsp/lib
   ```

6. Issue the following command:

   ```
   cp /usr/safenet/lunaclient/jsp/lib/libLunaAPI.so /etc/alternatives/jre/lib
   ```

7. Issue the following command:

   ```
   cp /usr/safenet/lunaclient/jsp/lib/LunaProvider.jar /opt/flexnet/ncprogs/lib/
   ```

8. Issue the following command:

   ```
   cd /etc/alternatives/jre/lib
   ```

9. Issue the following command:

   ```
   chmod 755 libLunaAPI.so
   ```

10. Issue the following command:

    ```
    cd /opt/flexnet/ncprogs/lib/
    ```

11. Issue the following command:

    ```
    chown flexnet:flexnet LunaProvider.jar
    ```

12. Issue the following command:

    ```
    chmod 664 LunaProvider.jar
    ```

13. Issue the following command:

    ```
    cd /opt/flexnet/ncprogs/lib
    ```

14. Issue the following command:

    ```
    mv LunaProvider-1.0.0.jar LunaProvider-1.0.0.jar.back
    ```

15. Issue the following command:

    ```
    usermod -a -G hsmusers flexnet
    ```

16. Shut down FlexNet Crypto Engine:

    ```
    flexnet-control stop tgblistener
    ```

17. Add the following values to the /opt/flexnet/conf/flexnet.local.properties file:

    ```
    vi /opt/flexnet/conf/flexnet.local.properties

    # FCE HSM Configuration
    fce.hsm.use=true
    fce.hsm.version=LUNA5
    fce.hsm.token.label=<Partition Name> OR <HA Group Label>
    fce.hsm.token.id=<Partition Password>
    ```

    Note: Some of these attributes, such as fce.hsm.token.label and/or fce.hsm.token.id may not be known until a later time.

18. Save the file.

On the DB server

1. In the FlexNet DB, verify that the MasterKey table has NO rows:

    ```
    SELECT * FROM master_key
    ```

2. In the FlexNet DB, verify tblCryptoEndpoints returns no rows for fldUniqueKey NOT equal to NULL:

    ```
    SELECT * FROM tblCryptoEndpoints WHERE fldUniqueKey != NULL
    ```

3. In the FlexNet DB, verify that there are no rows in table tbluniquekeys_1:

    ```
    SELECT * FROM tblKeysUniqueKeys
    ```

4. In the FlexNet DB, verify table tblCryptoEndpoints where fldEncrypted is = true (1) returns 0 rows:

    ```
    SELECT * FROM tblCryptoEndpoints WHERE fldEncrypted = 1
    ```

5. If all the preceding queries return 0 rows, delete the single rows from the Shared Key table in the FlexNet database:

    ```
    Delete from tlbKeysShared
    ```

Note: If any of the queries return rows, then additional assistance is required to integrate the HSM to an RNI with encrypted endpoints. As a protective mechanism, it is recommended to ensure any entries in tblcryptoendpoints that have ‘test’ encryption keys are deleted from the RNI DB.

On the NC server

1. To restart the FlexNet Crypto Engine, delete the existing FlexNet Crypto Engine local cache:

```
/opt/flexnet/ncprogs/bin/clear_crypto_cache.sh tgblistener
```

Configure Universal Client software

This method considers a single instance HSM. Please reference Appendix A on page 11 for high-availability considerations.

Configure the Network Controller server

1. Change directory:

```
cd /usr/safenet/lunaclient/bin
```

2. Copy the server certificate from the HSM to the local machine:

```
scp admin@<IP Address of the HSM Server>:<server>.pem
    /usr/safenet/lunaclient/cert/server/
```

Example:

```
scp admin@10.x.x.x:.pem /usr/safenet/lunaclient/cert/server/
```

Note*: The HSM admin password will be required. Note: the <server>.pem will be unique to that HSM.*

3. Register the HSM server with the client and tie it to the server certificate:

```
./vtl addServer -n <IP Address of the HSM Server> -c
/usr/safenet/lunaclient/cert/server/<server>.pem
```

Example:

```
./vtl addServer -n 10.x.x.x –c
/usr/safenet/lunaclient/cert/server/server.pem
```

4. Create a client certificate:

```
./vtl createCert -n <IP Address of the Network Controller>
```

Example:

```
vtl createCert -n 10.x.x.x
```

Output:

Private Key created and written to: /usr/safenet/lunaclient/cert/client/<IP Address>-Key.pem

Certificate created and written to: /usr/safenet/lunaclient/cert/client/<IP Address>.pem

5. Copy the client certificate to the HSM Server:

   ```
   scp /usr/safenet/lunaclient/cert/client/<IP Address of the
       Network Controller>.pem admin@<IP Address of the HSM Server>:
   ```

   Example:

   ```
   scp /usr/safenet/lunaclient/cert/client/10.x.x.x.pem
   admin@10.x.x.x:
   ```

Perform the following steps on the HSM

1. SSH to IP Address of the HSM server:

   ```
   ssh -l admin <IP Address of HSM>
   ```

2. Enter HSM admin password.
3. Register the client to the HSM and create a client name:

   ```
   client register -client <HSM Client IP> -ip <IP Address of the
       Network Controller>
   ```

   Example:

   ```
   client register -client 10.x.x.x -ip 10.x.x.x
   ```

   Note: This can be the same IP address.

4. Assign the client to an HSM partition:

   ```
   client assignPartition –client <HSM Client IP> –partition <HSM Token Label>
   ```

   Note: <HSM Token Label> is the partition name. Please ensure that you have created your partition on the HSM first.

   Example:

   ```
   client assignPartition -client 10.x.x.x -partition Security-Test
   ```

5. Display the configuration of the client:

   ```
   client -list (shows all the available clients)
   >client show -client <HSM Client Name>
   ```

   ClientID: <HSM Client Name>

   IPAddress: <IP Address of the Network Controller>

   Partitions: <HSM Token Label>

6. Exit the HSM server.

Verify the HSM configuration on the Network Controller

1. Change directory:

   ```
   cd /usr/safenet/lunaclient/bin
   ```

2. Validate the client configuration and ensure communication with the HSM:

   ```
   >./vtl verify
   ```

Example output:

```
The following Luna SA Slots/Partitions were found:

Slot       Serial #                 Label
====       ========                 =====
 1         <Partition Serial #>     <Partition Name>
```

Delete an existing client

If the following error displays when registering the NC HSM client on the HSM, you can remove the client registration from the partition.

Error: 'client register' failed. (C000040C : RC_OBJECT_ALREADY_EXISTS)

1. Log in to the HSM as admin.
2. Delete a client on the HSM:

   ```
   client delete -c <HSM Client Name>
   ```

   Note: *HSM Client Name = hostname of Network Controller (for example, nc.company.com)*

   ```
   CAUTION: Are you sure you wish to delete client named: <HSM Client Name>
   Type 'proceed' to delete the client, or 'quit' to quit now.

   > proceed

   'client delete' successful.
   ```

   Command Result: 0 (Success)

Appendix A: HSM product and user information

The following are links to the product information for the Thales Luna Appliance Hardware:

- Thales Customer Support Portal
  Thales Customer Support Portal - Thales Customer Support (thalesgroup.com)

- Thales CPL Documentation Hub
  Network HSM Releases (thalesdocs.com)

- Thales Luna Network HSM 7.x.x PRODUCT OVERVIEW
  Luna Network HSM 7.x.x Product Overview (thalesdocs.com)

- Thales Luna Network HSM 7.x.x APPLIANCE ADMINISTRATION GUIDE
  About the Appliance Administration Guide (thalesdocs.com)

- Thales Luna Network HSM 7.x.x HSM ADMINISTRATION GUIDE
  https://thalesdocs.com/gphsm/luna/7/docs/network/Content/admin_hsm/preface.htm

- Thales Luna Network HSM 7.x.x PARTITION ADMINISTRATION GUIDE
  https://thalesdocs.com/gphsm/luna/7/docs/network/Content/admin_partition/Preface.htm

- High-Availability Groups
  High-Availability Groups (thalesdocs.com)

Xylem |ˈzīləm|

1) The tissue in plants that brings water upward from the roots;

2) a leading global water technology company.

We’re a global team unified in a common purpose: creating advanced technology solutions to the world’s water challenges. Developing new technologies that will improve the way water is used, conserved, and re-used in the future is central to our work. Our products and services move, treat, analyze, monitor and return water to the environment, in public utility, industrial, residential and commercial building services settings. Xylem also provides a leading portfolio of smart metering, network technologies and advanced analytics solutions for water, electric and gas utilities. In more than 150 countries, we have strong, long-standing relationships with customers who know us for our powerful combination of leading product brands and applications expertise with a strong focus on developing comprehensive, sustainable solutions.

For more information on how Xylem can help you, go to www.xylem.com

Sensus
637 Davis Drive
Morrisville, NC 27560
Tel +1.800.638.3748
www.sensus.com