User Manual

HSMEncryptor

For Nuance Voice Biometrics Suite 8.2

Table of Content

1. Introduction

This document describes the Nuance HSMEncryptor component and capabilities. The HSMEncryptor is an encryption plug-in designed for Nuance Voice Biometrics Suite 8 (VocalPassword, FreeSpeech, S.P.I.D.). HSMEncryptor interacts with PKCS#11 compliant encryption products. Knowledge about PKCS#11 standard and capabilities is required to configure HSMEncryptor and related third-party products (SafeNet, Inc.).

1.1. System requirements

Nuance Voice Biometrics

- ✓ Voice Biometrics 8.2 product installation, e.g. VocalPassword
- ✓ See the Voice Biometrics documentation and release notes for system requirements and tested environments

Hardware Encryption product:

- ✓ SafeNet Luna SA K5 with Luna SA 4.4.1 client software
- ✓ Used encryption algorithm: AES-256

VoiceBiometrics 8.2 products support so-called key swapping or key versioning, which allows migration to new encryption keys in case needed or desired. The HSMEncryptor 8.2 plugin has been upgraded to support the new functionality and cannot be used with older VoiceBiometrics product releases.

2. Installation and configuration

Overall procedure:

1. Install and configure the SafeNet Luna appliance (encryption hardware); section 2.1.1.
2. Install and configure the SafeNet Luna SA client software on the processing server; section 2.1.2.
3. Install and configure the HSMEncryptor on the processing server; section 2.2.

2.1. SafeNet Luna SA encryption product

The following sections only give an overview and describe the essential steps. Please refer to the SafeNet Luna SA documentation for more information about how to install and configure the encryption server (HSM) and the client software.

2.1.1. Luna appliance (HSM)

This section describes HSMEncryptor requirements for setting up a Luna SA HSM appliance, but does not describe all aspects of the installation.
The appliance must be available on the network, and then configured. Use the SafeNet, Inc installation documentation for details to set up the appliance.

HSMEncryptor is tested with Password Authenticated HSM appliances (and not PED Authenticated). Authentication type is predetermined when you purchase the HSM appliance.

The SafeNet, Inc installation documentation steps through the configuration in a sequence of screens beginning with the “Configuration (Setup Appliance after Installing)”. The following procedure mirrors the sequence to show specific requirements for Voice Biometrics:

1. Configure the encryption server for your network. There are no specific requirements for these screens. Luna SA has approximately 9 configuration screens beginning with “Recommended Network Characteristics” and ending with “Generate a New Luna Server Certificate”.
2. Initialize the onboard HSM.
3. Adjust the HSM Policies — There are no specific requirements unless you want to combine multiple Luna SA HSMs into a high-availability array. See section 2.1.3.
4. Prepare virtual HSMs for your clients by creating HSM Partitions. For high-availability (HA) systems, you must use the same partition password for each HSM in the array.
5. Adjust the Partition Policies as desired.
6. Set up a Network Trust Link. You must define a secure network connection by exchanging certificates between the HSM and each Luna SA client that connects to the appliance. For high-availability systems, each client must exchange certificates with each HSM appliance in the array.
7. Assign clients to HSM Partitions — You must assign each Luna SA client to the partition created on the HSM. For high-availability systems, assign every client to a partition on every HSM appliance in the array.

2.1.2. Luna SA client software

Important note: You must install the SafeNet Luna SA client software that matches your Voice Biometrics and HSMEncryptor installation, especially 32-bit and 64-bit editions must not be mixed. Install the 64-bit SafeNet client and the 64-bit HSMEncryptor if the 64-bit VoiceBiometrics product is installed.

Note: You must be an operating system administrator or root user to install the software.

1. Using the installation media provided by SafeNet, Inc., double-click START_HERE.html to open the Luna SA documentation.
2. Click the Windows installation instructions button, and use the Luna SA documentation to perform the installation. Important: Install the **appropriate** edition of the SafeNet Luna SA client software. You will be asked whether Luna CSP, JSP and SDK components should be installed. HSMEncryptor does not require those components, so Nuance recommends unselecting the boxes.
3. After the Luna SA client installation completes, note the path to the cryptoki.dll file, e.g. C:\Program Files\LunaSA\cryptoki.dll
4. Each Luna SA client must have a Network Trust Link and an assigned partition on every appliance. The SafeNet documentation guides you through the procedure; see also steps 6 and 7 in section 2.1.1.
5. After configuring Luna SA, use the `vtl` command line tool to check that the client can communicate with the HSM. See section 2.1.4.

Note: If your system has more than one processing server, use identical configurations across all hosts.

2.1.3. Configure the Luna SA for high-availability

High-availability (HA) is an optional configuration to supply load-balancing and failover capabilities for your encryption system. The Luna SA documentation describes this in a topic called “HA and Load Balancing.” The HA configuration requires a cluster of HSM appliances (two or more HSM devices) on your network. The system works as follows:

- The Luna SA client communicates with a virtual HSM appliance.
- The virtual appliance represents the entire cluster of physical devices.
- The system automatically routes communications to a physical device.
- Every Luna SA client has a Network Trust Link with every physical device.

Note: The definition of an HA group resides entirely on a Luna SA client. HSM appliances do not operate differently when they are part of an HA group, and their software has no HA definition. The Luna SA client manages all data replication, load balancing and failover among the appliances.

To enable high-availability, follow the instructions in the Luna SA documentation. The instructions for configuring HSM appliances as an HA group are in a topic called “Appliance HA Setup.” You must create and configure an HA group on every client, and the groups should have the same name and contain the same partitions from the same HSMs.

- Nuance recommends using the same partition name on every HSM device in the high-availability group. See step 4 in section 2.1.1.
- The Luna SA documentation instructs you to perform an HSM backup on the Primary HSM in the HA group, and an HSM restore on the other HSMs in the group. These operations can be time-consuming, and are unnecessary for most Password-Authenticated HSMs:
  - The backup and restore sequence is required only when the "Enable cloning" policy is set to Disallowed. Use "hsm showPolicies" to see the setting on your appliance.
  - The sequence is not required when “Enable cloning" is set to Allowed (because the system automatically replicates data across all HSMs in the HA group when you create that group on the Luna SA client).

The Luna SA documentation describes how to create and configure the HA group on a client in a topic called “Client - Create HA Group.” Configuration steps:

1. Required. Each Luna SA client must have a Network Trust Link and an assigned partition on every appliance in the HA group. See steps 6 and 7 in section 2.1.1.
2. Recommended. Use the same name for the HA group on each Luna SA client.
   Recommended (for VocalPassword): `VocalPasswordHAGroup`
3. Required. Configure the client to only use HA slots, else failover cannot work properly.
   ```
   vtl haAdmin -HAOnly -enable
   ```
4. Required only if multiple HA groups exists on the Luna SA client. Use the `ckdemo` program to determine the slot ID that corresponds to the desired HA group (`VocalPasswordHAGroup`). You should see something like this:
   ```
   C:\Program Files\LunaSA>ckdemo
   ```
   (The menu is displayed)
   ```
   Enter your choice : 12
   Slots available:
           slot#1 - HA Virtual Card Slot
           slot#2 - HA Virtual Card Slot

   Select a slot: 1
   Token Info:
           Token label -> VocalPasswordHAGroup
   ```

```
        Token Manufacturer -> Safenet, Inc.
        Token Model -> LunaVirtual
```

(other output)

Important: `ckdemo` counts slots starting with 1, but Cryptoki starts with 0. Subtract 1 from the slot number reported by `ckdemo` to get the slot ID for the HSMEncryptor configuration.
In this case, slot #**1** was found to be the one to use, so the `HsmSlotID` must be set to **0**.

5. Required. Specify the slot ID in the `HSMEncryptor.dll.config` file on each processing server by setting `HsmSlotID` to 0 or to the number determined in step 4, respectively.
6. Required. Repeat these steps to create an HA group containing the same partitions on each processing server. Although you create identical partitions for the HA groups on each Luna SA client, you should change the listed order of those partitions for optimal load-balancing. Each Luna SA client sends requests in the order of the list. When the client detects that a partition load has passed a specific threshold, it sends to the next partition. By changing the partition list from client to client, you optimize performance by ensuring that requests are sent to all partitions, even at low and medium load conditions.
7. Required for Luna SA 4.4.1 and above. Enable automatic HSM recovery to handle situations when HSM appliances go out of service temporarily.
   a. Configure the Luna SA crystoki.ini on the processing server by running this command:
      `vtl haAdmin -autoRecovery -retry 30`
   b. Configure the Luna SA client to write messages to %CHRYSTOKICONFIGURATIONPATH%\haErrorLog.txt when an HSM appliance becomes unavailable:
      `vtl haAdmin -HALog -path "%CHRYSTOKICONFIGURATIONPATH%"`

Note: If your system has more than one processing server host, use identical configurations across all hosts.

For Luna SA 4.3, you must run the restore command on every Luna SA client that connects to an HSM appliance when that HSM goes offline and returns to service. (The explicit command "`vtl haAdmin –recover`" is needed because clients do not automatically detect when a partition in an HA group goes offline and returns.)

2.1.4. Troubleshooting HSM connectivity

System administrators must monitor HSM connectivity as part of their normal runtime procedures. Confirm that connectivity with the HSM is available:

1. Open a cmd shell and type:

   ```
   cd C:\Program Files\LunaSA          (default on Windows)
   cd C:\Program Files (x86)\LunaSA    (32-bit product on Windows 64-bit)
   vtl verify
   ```

2. The program displays connected partitions. For example:

   ```
   Slot Serial # Label
   ==== ======== =====
   1 950826001 Nuance
   2 951046001 Nuance2
   ```

   The program displays physical partitions on the HSM, but not logical partitions. If no partitions are displayed, your system might have a basic connectivity problem.

3. In HA configurations, check the HA status:

   ```
   vtl haAdmin -status –show
   ```

   The program displays something like this:

   ```
   HA Group Label:  VocalPasswordHAGroup   HA Group Number: 1950826001
   Synchronization:  enabled
          *** 95082600 is alive ***
          *** 95104600 is alive ***
   ```

   If error messages are shown, refer to the SafeNet documentation for information.

4. In HA configurations, check that only HA slots are considered:

   ```
   vtl haAdmin -HAOnly -show
   ```

Furthermore, check that your HSMEncryptor configuration is valid (path to cryptoki.dll, slot ID, password).

2.2. Nuance HSMEncryptor

Unpack the HSMEncryptor ZIP file to a location of your choice, e.g. C:\Nuance\HSMEncryptor.
Ensure that you use the appropriate package, i.e. use the HSMEncryptor 64-bit package if you installed the 64-bit Voice Biometrics edition.

Configure the HSMEncryptor plug-in and the processing server as described in the following sections. After configuration, restart the Voice Biometrics product.

2.2.1. Preconditions

Make sure that the Luna SA client configuration is working (section 2.1.4).

Usually, the HSM administrator (Security Officer or appropriate staff) recommends encryption algorithm and creates required encryption keys. Partitions, slots and keys must exist before the HSMEncryptor can be used. For highest available security, it is strongly recommended to use the AES algorithm (default) with keysize 256.

The plaintext slot (partition) password must be encrypted with Voice Biometrics' built-in encryption. Please contact Nuance for assistance.

The following information is needed to configure the HSMEncryptor:

- Path to the PKCS#11 compliant SafeNet C library (Cryptoki DLL coming with the client software)
- Slot ID to use. In HA configurations use the virtual slot determined during Luna SA configuration.
- Slot (partition) password (encrypted with Nuance means)
- Label of the encryption key for speakerID
- Label of the encryption key for audio data
- Algorithm (mechanism); default: AES_CBC_PAD
- Initialization vector suitable for the selected algorithm

2.2.2. HSMEncryptor configuration

The HSMEncryptor is configured through the XML file `HSMEncryptor.dll.config` stored in the same directory as the DLL. There are three relevant sections below the `applicationSettings` tag in the configuration file:

Section name	Description
Nuance.Encryption.HSMEncryptor.Properties. **Settings**	This section contains general settings.
Nuance.Encryption.HSMEncryptor.Properties. **KeysForSpeakerID**	This section specifies key labels and corresponding version numbers for the encryption of speaker and group IDs.
Nuance.Encryption.HSMEncryptor.Properties. **KeysForAudio**	This section contains key labels and corresponding version numbers for the encryption of audio data.

The following parameters are supported in section `Settings`:

Parameter	Description	Default value
CryptokiLibraryFilename	Absolute filename to the PKCS#11 compliant library (Cryptoki DLL) coming with the LunaSA client software.	C:\\Program Files\\LunaSA\\cryptoki.dll
HsmSlotID	ID (integer) of the slot to be used. The slot must exist. It depends on the Luna SA client configuration whether the ID denotes a real slot or a virtual slot (HA group).	0
HsmSlotPassword	The slot (partition) password; must be encrypted with Nuance means.	myEncryptedSlotPassword (just a placeholder)
HsmUserType	The type of user access, either “user” or “SO”. Usually “user”.	User
InitializationVector	The initialization vector (IV) as hexadecimal string. Must correspond to the algorithm. For **AES**, it is 16 bytes of data, i.e. **32** hexadecimal chars.	00000000000000000000000000000000
Algorithm	The algorithm (PKCS mechanism) to be used. AES is strongly recommended.	AES_CBC_PAD
ConfigReloadInterval	The time span in seconds after which HSMEncryptor reloads its configuration, esp. the keys. 0 means it never reloads. Change on Nuance advice only.	10

The following parameters are supported in sections `KeysForSpeakerID` and `KeysForAudio`:

Parameter	Description	Example

(positive integer)	Map a version number to a key label. Key versions must be unique (within the section) and new	`<setting name="`**`1`**`"`
		`      serializeAs="String">`
		`  <value>`**`myKeyLabel`**`</value>`
		`</setting>`

	version numbers must be greater than existing ones. Existing numbers must not be reused.	Map version 1 to key label `myKeyLabel`. The key `myKeyLabel` must exist on the HSM.

Sample configuration file `HSMEncryptor.dll.config`:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>    <sectionGroup name="applicationSettings"
        type="System.Configuration.ApplicationSettingsGroup, System,
          Version=4.0.0.0, Culture=neutral,
          PublicKeyToken=b77a5c561934e089" >
      <section name="Nuance.Encryption.HSMEncryptor.Properties.Settings"
          type="System.Configuration.ClientSettingsSection, System,
            Version=4.0.0.0, Culture=neutral,
            PublicKeyToken=b77a5c561934e089" requirePermission="false" />
      <section
        name="Nuance.Encryption.HSMEncryptor.Properties.KeysForSpeakerID"
        type="System.Configuration.ClientSettingsSection, System,
        Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"
        requirePermission="false" />
      <section name="Nuance.Encryption.HSMEncryptor.Properties.KeysForAudio"
        type="System.Configuration.ClientSettingsSection, System,
        Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"
        requirePermission="false" />
    </sectionGroup>
  </configSections>
  <applicationSettings>
    <Nuance.Encryption.HSMEncryptor.Properties.Settings>
      <setting name="CryptokiLibraryFilename" serializeAs="String">
        <value>C:\\Program Files\\LunaSA\\cryptoki.dll</value>
      </setting>
      <setting name="HsmSlotID" serializeAs="String">
        <value>0</value>
      </setting>
      <setting name="HsmSlotPassword" serializeAs="String">
        <value>myEncryptedSlotPassword</value>
      </setting>
      <setting name="HsmUserType" serializeAs="String">
        <value>user</value>
      </setting>
      <setting name="InitializationVector" serializeAs="String">
        <value>00000000000000000000000000000000</value>
      </setting>
      <setting name="Algorithm" serializeAs="String">
        <value>AES_CBC_PAD</value>
      </setting>
      <setting name="ConfigReloadInterval" serializeAs="String">
        <value>10</value>
      </setting>
    </Nuance.Encryption.HSMEncryptor.Properties.Settings>
    <Nuance.Encryption.HSMEncryptor.Properties.KeysForSpeakerID>
        <setting name="1" serializeAs="String">
            <value>myKey1ForSpeakerID</value>
        </setting>
        <!--
        <setting name="2" serializeAs="String">
            <value>myKey2ForSpeakerID</value>
        </setting>
        -->
    </Nuance.Encryption.HSMEncryptor.Properties.KeysForSpeakerID>
    <Nuance.Encryption.HSMEncryptor.Properties.KeysForAudio>
        <setting name="1" serializeAs="String">
            <value>myKey1ForAudio</value>
        </setting>
        <!--
        <setting name="2" serializeAs="String">
            <value>myKey2ForAudio</value>
        </setting>
        -->
    </Nuance.Encryption.HSMEncryptor.Properties.KeysForAudio>
  </applicationSettings>
  <startup useLegacyV2RuntimeActivationPolicy="true">
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.0"/>
  </startup>
</configuration>
```

2.2.3. HSMEncryptor QuickTest

The HSMEncryptor package includes the utility `TestHSMEncryptor.exe` for a basic functionality test. Execute the utility on the command line. Example for a successful quick test:

```
C:\Nuance\HSMEncryptor>TestHSMEncryptor.exe
HSMEncryptor quick test
Initialize
Adapter: {HSMEncryptor, Version=8.2.0.1, Culture=neutral, PublicKeyToken=null,
CryptokiFilename: C:\\Program Files\\LunaSA\\cryptoki.dll}; Cryptoki: {Version: 2.1,
LibDescription: Chrystoki, LibVersion: 0.6}; Token: {Label: VocalPasswordHAGroup,
Manufacturer: Safenet, Inc., Model: LunaVirtual, Serial: nnnnnnnnnn, HWVersion: 0.0}
Test with speakerID key label
Encrypt...
Decrypt...
Test passed
Test with audio key label
Encrypt...
Decrypt...
```

```
Test passed
Test GetLatestKeyVersion
GetLatestKeyVersion(0) (speakerKey) returned 1
GetLatestKeyVersion(1) (audioKey) returned 1
HSMEncryptor quick test was successful.
```

2.2.4. Voice Biometrics configuration

Configure the Voice Biometrics product (e.g. VocalPassword) to use the HSMEncryptor as the custom encryption plug-in and decide whether to encrypt speaker IDs, audio data, or both.
In particular:

- Set parameter `CustomEncryptionAssembly` to point to the HSMEncryptor DLL (full path), e.g.: `C:\Nuance\HSMEncryptor\HSMEncryptor.dll`
- Set parameter `EncryptIDs` to `true` to encrypt speaker IDs.
- Set parameter `EncryptAudio` to `true` to encrypt audio data.

For more information about how to change configuration parameters please refer to the product help suite.