

# **Thycotic Secret Server**

INTEGRATION GUIDE THALES LUNA NETWORK HSM THALES DATA PROTECTION ON DEMAND

#### **Document Information**

Document Part Number	007-000480-001
Release Date	7 May 2020

#### **Revision History**

Revision	Date	Reason
A	July 24, 2019	Initial release
В	7 May 2020	Update

#### Trademarks, Copyrights, and Third-Party Software

Copyright © 2020 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

#### Disclaimer

All information herein is either public information or is the property of and owned solely by Thales Group and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales' information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- > The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- > This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-

infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

# CONTENTS

PREFACE	5
Audience	5
Document Conventions	5
Notifications	5
Command Syntax and Typeface Conventions	6
Related Documents	6
Support Contacts	7
Customer Support Portal	7
Telephone Support	7
Email Support	7
CHAPTER 1: Getting Started	8
Using a Compatible Device	8
Configuring Luna Network HSM	8
Provisioning DPOD Service	9
Setting up Thycotic Secret Server	10
CHAPTER 2: Integrating Thycotic Secret Server with a Luna Network HSM 1	11
Configuring the SafeNet Key Storage Provider	11
Enabling HSM	12
CHAPTER 3: Integrating Thycotic Secret Server Cluster with a Luna Network HSM 1	17
Configuring the SafeNet Key Storage Provider	17
Enabling HSM	18

# PREFACE

This document describes steps to integrate Thycotic Secret Server with a Thales Luna Network HSM or a Thales Data Protection On Demand (DPOD) service. It contains the following chapters:

- > Getting Started
- > Integrating Thycotic Secret Server with a Luna Network HSM
- > Integrating Thycotic Secret Server Cluster with a Luna Network HSM

## Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure, including Luna Network HSM users and security officers, key manager administrators, and network administrators. It is assumed that the users of this document are proficient with security concepts.

All products manufactured and distributed by Thales Group are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

## **Document Conventions**

This section provides information on the conventions used in this template. The information presented is to instruct the writer on how to use the template and can be removed if you do not wish to include it in your customer-facing document. For example, you may wish to remove the "Hyperlinks" sections but keep the "Notifications" section.

### Notifications

This template uses notes, cautions, and warnings to alert you to important information that may help you to complete your task, or prevent personal injury, damage to the equipment, or data loss.

#### Notes

Notes are used to alert you to important or helpful information.

NOTE: Take note. Notes contain important or helpful information.

#### Cautions

Cautions are used to alert you to information that may help prevent unexpected results or data loss.

**CAUTION!** Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

#### Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

\*\*WARNING\*\* Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury

Convention	Description
bold	The bold attribute is used to indicate the following:
	> Command-line commands and options (Type <b>dir /p</b> .)
	> Button names (Click <b>Save As</b> .)
	> Check box and radio button names (Select the <b>Print Duplex</b> check box.)
	> Window titles (On the <b>Protect Document</b> window, click <b>Yes</b> .)
	> Field names (User Name: Enter the name of the user.)
	Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.)
	> User input (In the <b>Date</b> box, type <b>April 1</b> .)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document.
<variable></variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[ optional ] [ <optional> ]</optional>	Square brackets enclose optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.</variable></variables>
[ a   b   c ] [ <a>   <b>   <c>]</c></b></a>	Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.
{ a   b   c } { <a>   <b>   <c> }</c></b></a>	Braces enclose required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.</variables>

## Command Syntax and Typeface Conventions

### **Related Documents**

The following documents contain related or additional information:

Thales Luna Network HSM Product Documentation

## Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or <u>Thales Customer Support</u>.

Thales 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 Thales 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 <u>https://supportportal.thalesgroup.com</u>, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository 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 Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

## **Email Support**

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

# CHAPTER 1: Getting Started

This chapter explains the setup that you require for integrating Thycotic Secret Server with a Thales Luna Network HSM or a DPOD service. It includes the following sections:

- > Using a Compatible Device
- > Configuring Thales Luna Network HSM
- > Provisioning DPOD Service
- > Setting up Thycotic Secret Server

### Using a Compatible Device

This integration is verified with:

- > Thales Luna Network HSM on Windows 2016 Server operating system
- > Thales DPOD on Windows 2016 Server operating system

This integration is also compatible with:

- > Thales Luna PCIe HSM on Windows 2016 Server operating system
- > Thales Luna USB HSM on Windows 2016 Server operating system

#### Configuring Luna Network HSM

Before you begin the integration process:

- 1. Ensure that the HSM is setup, initialized, provisioned, and ready for deployment.
- 2. Create a partition on the HSM that will be later used by Thycotic Secret Server.
- **3.** Register a client for the system and assign the client to the partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition.
- 4. Ensure that the partition is registered and configured. The command to see the registered partition is:

```
lunacm.exe (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
Available HSMs:
Slot Id ->
                        0
Label ->
                        Thycotic
Serial Number ->
                        1280780175917
Model ->
                        LunaSA 7.3.0
Firmware Version ->
                        7.3.0
Configuration ->
                        Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description ->
                        Net Token Slot
Current Slot Id: 0
```

**NOTE:** Follow the steps mentioned in *Thales Luna Network HSM Documentation* for creating NTLS connection, initializing the partition, and various user roles.

#### Using Luna Network HSM in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the Luna Network HSM in FIPS mode, you have to make the following change to the configuration file:

[Misc]

RSAKeyGenMechRemap = 1;

This setting redirects the older calling mechanism to a new approved mechanism when Luna Network HSM is in FIPS mode.

#### Setting up Thales Luna Network HSM HA

Refer to the *Thales Luna Network HSM Product Documentation* for steps and details regarding configuring and setting up two or more HSM boxes on host systems. You must enable the HAOnly setting in HA for failover to work.

### **Provisioning DPOD Service**

This DPOD service provides your client machine with access to an HSM Application Partition for storing cryptographic objects used by your applications. Application partitions can be assigned to a single client, or multiple clients can be assigned to, and share a single application partition.

To use the DPOD service, you need to provision your application partition by initializing the following roles:

- > Security Officer (SO) responsible for setting the partition policies and for creating the Crypto Officer.
- Crypto Officer (CO) responsible for creating, modifying, and deleting crypto objects within the partition. The CO can use the crypto objects and create an optional, limited-capability role called Crypto User that can use the crypto objects but cannot modify them.
- > Crypto User (CU) optional role that can use crypto objects while performing cryptographic operations.

#### **Resolving Issues with DPOD Services**

**Enabling DPOD Service in Non-FIPS mode:** DPOD services operate in a FIPS and non-FIPS mode. Ensure you enable the **Allow non-FIPS approved algorithms** check box when configuring your DPOD service. The FIPS mode is enabled by default. Refer to the *Mechanism List* in the *SDK Reference Guide* for more information about available FIPS and non-FIPS algorithms.

Verifying DPOD <slot> value: LunaCM commands work on the current slot. If there is only one slot, then it is always the current slot. If you are completing an integration using DPOD services, you need to verify the slot on the DPOD service for sending the commands. If there is more than one slot, then use the **slot** set command to direct a command to a specified slot. You can use slot list to determine which slot numbers are currently in use by the DPOD service.

## Setting up Thycotic Secret Server

Install Thycotic Secret Server on the target machine. Refer to *Thycotic Documentation* for detailed instructions.

# CHAPTER 2: Integrating Thycotic Secret Server with a Luna Network HSM

Integrating Thycotic Secret Server with a Luna Network HSM involves the following steps:

- > Configuring the SafeNet Key Storage Provider
- > Enabling HSM

## Configuring the SafeNet Key Storage Provider

To configure the SafeNet Key Storage Provider:

- 1. Navigate to the <Luna HSM Client installation Directory>\KSP directory. If you are using a DPOD service, the \KSP folder is available in the service client package.
- 2. Double-click KspConfig.exe. The SafeNet KSP configuration wizard will appear on your screen.
- 3. Double-click Register or View Security Library on the left side of the pane.
- 4. Click Browse and select a cryptographic library such as <Luna HSM Client installation Directory>\cryptoki.dll>.
- 5. Click **Register**. If using a DPOD service client, the cryptographic libraries are available in the service client package. On successful registration, you will see the following message:

"Success registering the security library"

- 6. Double-click Register HSM Slots and enter the Slot (Partition) password.
- Click Register Slot to register the slot for Domain and Service Account that has access to database and running the IIS Application Pool(s) dedicated to Secret Server. On successful registration, you will see the following message:

"The slot was successfully and securely registered."

SafeNet Key Storage Provider Config Wizard			- 🗆 X
File Help			
- SafeNet KSP Config	Register For User	Domain	Register By
Register OF View Security Library Register HSM Slots	svc_thycotic	TEST-THYCOTIC -	Slot Label
	Available Slots	Slot Password	-
	0 Thycotic		C Slot Number
	1		
	1		Register Slot
			View Registered Slots
	Registered Slots		
	SlotLabel:Thycotic		

- 8. Register the same slot for NT\_AUTHORITY\SYSTEM.
- 9. Place SafeNetKSP.dll in service client package under C:\Windows\System32, if you are using a DPOD service client.
- 10. Restart the IIS after registering KSP for changes to take effect.

## Enabling HSM

To configure the HSM, complete the following steps:

- 1. Go to the Admin menu and click Configuration.
- 2. Select the HSM tab.
- 3. Click Enable HSM to initiate the HSM configuration process.

A ttps://win-d94ndrrjf89/Secr	etServer/ConfigurationHsm.aspx	P → A C Secret Server	× 🥕 my.thycotic.com	
thycotic,				
슈 Home	Configuration			
C Recent				
Shared With Me	General Login SAML Folders	Local User Passwords Security	Ticket System Email Session Recording	HSM
🔂 Favorites	Enable USM		No	
🗘 Inbox			NU	
Reports +	Back Enable HSM			
合 Secrets +				

4. Click Next.

e 🕞 🖲 https://win-d94ndrrjf89/	ecretSener/ConfigurationHamEdit.aspx D - 🔒 C 💿 Secret Server × 🏓 mythycotic.com	-	<b>0</b> 2 5
thycotic	Q		0
슈 Home	Configuration		
() Recent			
Shared With Me	General Login SAML Folders Local User Passwords Security Ticket System Email Session Recording		
🛱 Favorites			
🗘 Inbox	HSM SETUP		
Reports +			
Secrets +	Secret Server supports encryption key protection with an HSM. For Secret Server to be able to communicate to the HSM, the HSM must have a registered Cryptographic Next Generation (CNG) provider. Please consult your HSM venc information about installing a CNG provider. For more information about HSM integration and requirements, please see our HSM Integration Guide. Enabling the HSM will perform the following steps:	dor for more	
	<ol> <li>The CNG provider and HSM will be tested for compatibility before any changes are made.</li> <li>You must back up your encryption.config file before proceeding.</li> <li>An encryption key will be generated by the HSM and presisted. The name of this key is generated and displayed on the configuration page once HSM setup is complete. The encryption.config file is updated with information ab</li> <li>An encryption key will be generated by the HSM and presisted. The name of this key is generated and displayed on the configuration page once HSM setup is complete. The encryption config file is updated with information ab</li> <li>HSM keys are user specific. You cannot change the identity of the Application Pool while HSM integration is enabled. You must disable HSM integration before changing the Application Pool's identity.</li> </ol>	out the HSN	1 ke
	X Cancel PNext		

- 5. Select SafeNet Key Storage Provider from Persistent Provider drop down box under HSM PROVIDERS section and select key size of RSA from Key size drop down box.
- 6. Click Next. After this, Secret Server will simulate encryption and decryption operations.

+ Martin - d94ndrrjf89/Sec	retServer/ConfigurationHsr	nEdit.aspx	,O → 🚔 C 🙆 Secre	et Server	×			
thycotic.								
G Home	Configuration							
C Recent	5							
Shared With Me	General Login	SAML Folde	rs Local User Passwords	Security	Ticket System	Email	Session Recording	HSM
☆ Favorites								
🗘 Inbox								
Reports +	HSM PROVIDERS							
🔓 Secrets +	Persistent Provider			SafeNet Ke	ey Storage Provide	er 🗸		
	Key size			2048 🗸				
	🗙 Cancel 🦱	Next						

7. Verify whether the configuration has been successful by checking the details under the **HSM PROVIDERS TEST RESULTS** section.

(=) (a) https://win-d94ndrrjf89/Secr	etServer/ConfigurationHs	mEdit.aspx		,D → 🗎 C 🍙 Secret	Server	×			
thycotic,									
යි Home	Configuration								
C Recent									
Shared With Me	General Login	SAML	Folders	Local User Passwords	Security	Ticket System	Email	Session Recording	HSM
☆ Favorites									
🗘 Inbox									
Reports +	HSM PROVIDERS T	EST RESULT	rs						
合 Secrets +	SafeNet Key Provider Key	Storage Pr Testing Su	rovider Jccess						
	Write Check	<b>onfig</b> Success							
	Success	Pool Identi	ty						
	Your HSM is ready	for use. Th	e next step	will show a summary of	f the configu	uration before HS	SM integra	ation is enabled.	
	X Cancel	Next							

8. Click Next to access the HSM VERIFY CONFIGURATION section. Review HSM configuration and then click Save to enable the HSM.

https://win-d94ndrrjf89/Se	ecretServer/ConfigurationHsmEdit.aspx $\mathcal{P} \stackrel{\sim}{\hfill} \textcircled{\hfill} \textcircled{\hfill}$ Secret Server $\times$
thycotic,	
合 Home	Configuration
C Recent	
Shared With Me	General Login SAML Folders Local User Passwords Security Ticket System Email Session Recording HSM
🗙 Favorites	
🗘 Inbox	
Reports +	
🛆 Secrets +	Persistent Provider SafeNet Key Storage Provider
	Please review your HSM configuration. Continuing will enable HSM integration.  1. The encryption.config file will be modified.  2. The database will be updated with the selected provider.  3. You will need to recycle the application pool.  X Cancel Cancel Save

9. Click Finished after you see the following message under the HSM SETUP COMPLETE section:

"The HSM is now enabled."

https://win-d94ndrrjf89/Sec	retServer/ConfigurationHsml	dit.aspx	오 두 🗎 Ċ 🍙 Secre	t Server	×			
cotic.								
Home	Configuration							
Recent								
Shared With Me	General Login	SAML Folders	Local User Passwords	Security	Ticket System	Email	Session Recording	HSM
Favorites								
Inbox								
Reports +	HSM SETUP COMPLE	IE.						
Secrets +	The HSM is n	ow enabled.						
	8∋ Finished							
	https://win-d94ndrrjf89/Sec cotics Horne Recent Shared With Me Favorites Inbox Reports + Secrets +	Image: https://win-d94ndrrjf89/SecretServer/ConfigurationHsmt Home Recent Shared With Me Favorites Inbox Reports Secrets + Secrets Image: the text of the text of the text of text o	https://win-d94ndrrjf89/SecretServer/ConfigurationHsmEdit.aspx colic. Home Recent Shared With Me Favorites Inbox Reports Secrets + HSM SETUP COMPLETE The HSM is now enabled. [XM Finished]	<ul> <li>         Integrit/win-d94ndrrjf89/SecretServer/ConfigurationHsmEdit.aspx         P ~ m c m c         Image: Secret Server/ConfigurationHsmEdit.aspx         P ~ m c m c         Image: Secret Server/ConfigurationHsmEdit.aspx         P ~ m c m c         Image: Secret Server/ConfigurationHsmEdit.aspx         P ~ m c m c         Image: Secret Server/ConfigurationHsmEdit.aspx         P ~ m c m c         Image: Secret Server/ConfigurationHsmEdit.aspx         P ~ m c m c         Image: Secret Server/ConfigurationHsmEdit.aspx         P ~ m c m c         Image: Secret Server/ConfigurationHsmEdit.aspx         P ~ m c m c         Image: Secret Server/ConfigurationHsmEdit.aspx         P ~ m c m c         Image: Secret Server/ConfigurationHsmEdit.aspx         P ~ m c m c         Image: Secret Server/ConfigurationHsmEdit.aspx         P ~ m c m c         Image: Secret Server/ConfigurationHsmEdit.aspx         P ~ m c m c         Image: Secret Server/ConfigurationHsmEdit.aspx         P ~ m c m c         Image: Secret Server/Configuration         Image: Secret Server/Configuration         HSM SETUP COMPLETE         Image: Secret Server Server Secret Server Secret Server Secret Server Secret Secre</li></ul>	<ul> <li>https://win-d94ndrijf89/SecretServer/ConfigurationHsmEdit.aspx</li> <li>r d d e Secret Server</li> <li>Secret Server</li> </ul>	<ul> <li>https://win-d94ndrijf89/SecretServer/ConfigurationHsmEdit.aspx</li> <li>A * A C</li> <li>Secret Server</li> <li>Secret Server</li> <li>Configuration</li> <li>General Login SAML Folders Local User Passwords Security Ticket System</li> <li>HSM SETUP COMPLETE</li> <li>HSM SETUP COMPLETE</li> <li>The HSM is now enabled.</li> </ul>	<ul> <li>https://win-d94ndrijf89/SecretServer/ConfigurationHsmEdit.aspx</li> <li>A * d C</li> <li>Secret Server</li> <li>Secret Server</li> </ul>	<ul> <li>The HSM is now enabled.</li> <li>The HSM is now enabled.</li> </ul>

 Restart the IIS for configuration changes to take effect. You can now view the HSM configuration details under the HSM tab. The Secret Server encryption key is now stored on Luna Network HSM partition.

E State Stat	cretServer/ConfigurationHsm.aspx	,Ω → 🚔 🖒 🍙 Secret Server	×		
thycotic					
合 Home	Configuration				
C Recent					
Shared With Me	General Login SAML Folders	Local User Passwords Security	Ticket System Email	Session Recording	HSM
☆ Favorites	Enable HSM	Yes			
Ļ Inbox	Developent Deceller	CofeNiet	Kay Starage Bravidar		
Reports +	resistent rioidei	SaleNet	Rey Storage Provider		
🛆 Secrets +	Key Identifier	06e9498	38-f797-4cf3-9792-b1f1aca9	2aa9	
	Key Size	2048-bit			
	Back Sisable HSM				

11. Verify the key using the lunacm utility.

```
C:\Program Files\SafeNet\LunaClient>lunacm.exe
lunacm.exe (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
           Available HSMs:
           Slot Id ->
                                               0
           Slot 1d ->
Label ->
Serial Number ->
Model ->
Firmware Version ->
Configuration ->
Slot Description ->
                                               o
Thycotic
1280780175917
LunaSA 7.3.0
7.3.0
Luna User Partition With SO (PW) Key Export With Cloning Mode
Net Token Slot
           Current Slot Id: 0
lunacm:> role login -n co
           enter password: *******
 command Result : No Error
lunacm:> partition contents
           The 'Crypto Officer' is currently logged in. Looking for objects accessible to the 'Crypto Officer'.
           Object list:
           Label:
Handle:
                                  f81597e9-b459-4a4e-89c5-d5c3af22821b
                                 Private Key
4c09000018000003cb640800
           Object Type:
Object UID:
           Label:
Handle:
                                  f81597e9-b459-4a4e-89c5-d5c3af22821b
                                 186
Public Key
4b09000018000003cb640800
           Object Type:
Object UID:
           Number of objects: 2
 ommand Result : No Error
```

This completes the integration of Thycotic Secret Server with Thales Luna Network HSM or Thales Data Protection On Demand Service. Secrets created in Thycotic Secret Server will now use encryption keys residing in HSM partition.

# CHAPTER 3: Integrating Thycotic Secret Server Cluster with a Luna Network HSM

Integrating Thycotic Secret Server Cluster with a Luna Network HSM involves the following steps:

- > Configuring the SafeNet Key Storage Provider
- > Enabling HSM

### Configuring the SafeNet Key Storage Provider

Perform the following steps on all the nodes of the Thycotic Secret Server Cluster:

- 1. Navigate to the <Luna HSM Client installation Directory>\KSP directory.
- 2. Double-click KspConfig.exe. The SafeNet KSP configuration wizard displays.
- 3. Double-click Register or View Security Library on the left side of the pane.
- 4. Click Browse and select a cryptographic library such as <Luna HSM Client installation Directory>\cryptoki.dll>.
- 5. Click Register. On successful registration, you will see the following message: "Success registering the security library" displays.
- 6. Double-click Register HSM Slots on the left side of the pane.
- 7. Enter the Slot (Partition) password.
- 8. Click Register Slot to register the slot for Domain and Service Account that has access to database and running the IIS Application Pool(s) dedicated to Secret Server. On successful registration, you will see the following message: "The slot was successfully and securely registered"

🛚 - SafeNet Key Storage Provider Config Wizard			- 🗆 X
File Help			
⊡- SafeNet KSP Config	Register For User	Domain	Register By
Register Or View Security Library     Register HSM Slots	svc_thycotic -	TEST-THYCOTIC	Slot Label
	Available Slots	Slot Password	-
	0 Thycotic		C Slot Number
			Register Slot
			View Registered Slots
	Registered Slots		
	SlotLabel:Thycotic		

- 9. Register the same slot for NT\_AUTHORITY\SYSTEM.
- **10.** Restart the IIS after registering KSP for changes to take effect.

### **Enabling HSM**

To configure the HSM, complete the following steps on only one of the node of cluster:

- 1. Log in to Secret Server from browser : <u>http://localhost:80/SecretServer</u>
- 2. Go to the Admin menu and click Configuration.
- **3.** Select the **HSM** tab. This initiates the HSM configuration, which guides the process of selecting the HSM's CNG provider.
- 4. Click **Enable HSM** to initiate the configuration process.

**NOTE:** Back up the encryption.config before proceeding to enable HSM.

Image: Antropy of the second secon	etServer/ConfigurationHsm.aspx $\mathcal{P} = egin{array}{c} & & & \\ \hline \hline$	et Server 🛛 🗙 🍌 my.thycotic.com
thycotic,		
슈 Home	Configuration	
C Recent	5	
Shared With Me	General Login SAML Folders Local User Passwords	Security Ticket System Email Session Recording HSM
🛠 Favorites	Englis USM	No
¢ Inbox		INU
Reports +	Back Enable HSM	
🛆 Secrets +		

5. Click Next.

🗲 🛞 🔒 https://win-fi7q7vg9g9g	ecretServer/ConfigurationHomEdit.supx P + 🔒 C 🔒 Secret Server X 🗸 Secret Server Clustering	ය හ ම
thycotic,	Q	
合 Home	Configuration	
C Recent		
Shared With Me	General Login SAML Folders Local User Passwords Security Ticket System Email Session Recording HSM	
🔂 Favorites		
🗘 Inbox		
Reports	↑ The second se	
A Sacrets	<ul> <li>Secret Server supports encryption key protection with an HSM. For Secret Server to be able to communicate to the HSM, the HSM must have a registered Cryptographic Next Ge provider. Please consult your HSM vendor for more information about installing a CNG provider. For more information about HSM integration and requirements, please see our Foundation the following steps:</li> <li>1. The CNG provider and HSM will be tested for compatibility before any changes are made.</li> <li>2. You must back up your encryption.config file before proceeding.</li> <li>3. An encryption key will be generated by the HSM and persisted. The name of this key is generated and displayed on the configuration page once HSM setup is complete. The incryption forming file is updated with information about the HSM key.</li> <li>4. HSM keys are user specific. You cannot change the identity of the Application Pool while HSM integration is enabled. You must disable HSM integration before changing the pool's identity.</li> <li>After the HSM integration is enabled, the encryption.config file must be copied to each node in your cluster, then IIS must be restarted.</li> <li><b>X</b> Cancel</li> <li><b>X</b> Cancel</li> </ul>	neration (CNG) 4SM Integration he he Application

6. Select SafeNet Key Storage Provider from the Persistent Provider drop down box under the HSM PROVIDERS section and select key size of RSA from Key size drop down box.

Attps://win-d94ndrrjf89/Sec	cretServer/ConfigurationHsmEdit.aspx $\mathcal{P} \star \triangleq \mathcal{C}$ Secret Server $\star$
thycotic,	
යි Home	Configuration
C Recent	
Shared With Me	General Login SAML Folders Local User Passwords Security Ticket System Email Session Recording
☆ Favorites	
🗘 Inbox	
Reports +	
合 Secrets +	Persistent Provider SafeNet Key Storage Provider
	Key size 2048 🔽
	X Cancel

- 7. Click Next. After this, Secret Server will simulate encryption and decryption operations.
- 8. Verify whether the configuration has been successful by checking the details under the HSM PROVIDERS TEST RESULTS section.

æ	🗧 🛞 📵 https://win-d94ndrrjf89/SecretServer/ConfigurationHsmEdit.aspx 🔎 🖛 🚔 🖒 🕘 Secret Server 🛛 🖌			
∎ 2 © ©	Home Recent Shared With Me	Configuration	HSM	
☆	Favorites			
À Inbox III Reports + A Secrets + ✓ You		HSM PROVIDERS TEST RESULTS         Image: SafeNet Key Storage Provider Provider Key Testing Success         Image: Provider Key Tes		
		X Cancel Mext		

9. Click Next. Review your HSM configuration under the HSM VERIFY CONFIGURATION section.

	tServer/ConfigurationHsmEdit.aspx $\mathcal{P} \star \triangleq \mathcal{C}$ Secret Server $\star$
thycotic,	
合 Home	Configuration
C Recent	
Shared With Me	General Login SAML Folders Local User Passwords Security Ticket System Email Session Recording HSM
🗙 Favorites	
🗘 Inbox	
Reports +	HSW VERIFI CONFIGURATION
🔓 Secrets +	Persistent Provider SafeNet Key Storage Provider
	Please review your HSM configuration. Continuing will enable HSM integration.  1. The encryption.config file will be modified.  2. The database will be updated with the selected provider.  3. You will need to recycle the application pool.

10. Click Save to complete the HSM setup. You will see the following message on the screen:

"The HSM is now enabled."

🗧 🛞 🖲 https://win-d94ndrrjf89/SecretServer/ConfigurationHsmEdit.aspx 🛛 🖓 🖌 🔒 🖒 💽 Secret Server 🛛 🗙									
thycotic,									
合 Home	Configuration								
C Recent									
Shared With Me	General Log	in SAML	Folders	Local User Passwords	Security	Ticket System	Email	Session Recording	HSM
☆ Favorites									
Ļ Inbox									
Reports +	HSM SETUP CO	<b>MPLETE</b>							
A Secrets +	The HSM	l is now ena	bled.						
	≈ Finished								

11. Click Finished and then restart the IIS for configuration changes to take effect.

**12.** The HSM configuration is saved and can be viewed under **HSM** tab. The Secret Server encryption key is now stored on Luna Network HSM partition.

Comparison (ConfigurationHsm.aspx (Configurat					
thycotic					
合 Home	Configuration				
() Recent					
Shared With Me	General Login SAML Folders Local User Passwords	Security Ticket System Email Session Recording			
☆ Favorites	Enable HSM	Yes			
Ļ Inbox	Parsistant Provider	SafeNet Key Storane Provider			
Reports +					
合 Secrets +	Key Identifier	06e94988-f797-4cf3-9792-b1f1aca92aa9			
	Key Size	2048-bit			
	Back Disable HSM				

**13.** Verify the key using the lunacm utility:

C:\Program Files\SafeNet\LunaClient≻lunacm.exe lunacm.exe (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.							
	Available HSMs:						
	Slot Id -> Label -> Serial Number Model -> Firmware Versi Configuration Slot Descripti	-> on -> -> on ->	0 Thycotic 1280780175917 LunaSA 7.3.0 7.3.0 Luna User Partition With SO (PW) Key Export With Cloning Mode Net Token Slot				
	Current Slot I	d: Ø					
lunacm:	> role login -n	со					
	enter password: *******						
Command	Result : No Er	ror					
lunacm:	> partition con	itents					
	The 'Crypto Officer' is currently logged in. Looking for objects accessible to the 'Crypto Officer'.						
	Object list:						
	Label: Handle: Object Type: Object UID:	f81597e9 325 Private 4c090000	0-b459-4a4e-89c5-d5c3af22821b Key 118000003cb640800				
	Label: Handle: Object Type: Object UID:	f81597e9 186 Public K 4b090000	0-b459-4a4e-89c5-d5c3af22821b Gey 018000003cb640800				
	Number of objects: 2						
Command	Result : No Er	ror					

- 14. Copy encryption.config file from this node to all other nodes.
- **15.** Restart each nodes' Application Pool for the changes to take effect.

16. Log in to Secret Server from any node and verify that the HSM is enabled and key identifier displayed is correct. This completes the integration of Thycotic Secret Server Cluster with a Thales Luna Network HSM. Secrets created in Thycotic Secret Server Cluster from any node will now use encryption keys residing in the HSM partition.