vSEC CMS with Luna 7 HSM and DPoD

Integration Guide



All information herein is either public information or is the property of and owned solely by Gemalto 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 Gemalto's 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 publicly accessible 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, Gemalto 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, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto 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 Gemalto 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.

Gemalto 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 Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto 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.

© 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto 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.

Contents

Pı	reface	
	Scope	4
	Revisions	4
	Gemalto Rebranding	4
	Document Conventions	5
	Command Syntax and Typeface Conventions	5
	Support Contacts	7
1	Introduction	8
	Overview	8
	3rd Party Application Details	8
	Supported Platforms	8
	Prerequisites	9
	SafeNet Network HSM Setup	9
	Data Protection on Demand (DPoD) HSM service Setup	9
	vSEC CMS Prerequisites for Installation	9
	vSEC CMS Installation and Configuration	10
2	Integrating SafeNet Luna HSM with vSEC CMS	11
	Creating a Connection with HSM from vSEC CMS	11
	Troubleshooting Tip>	14
	Generate New Master Key	15
3	Integrating DPoD with vSEC CMS	20
	Creating a Connection with DPoD from vSEC CMS	20
	Important>	20
4	Appendix	21

Preface

This document is intended to guide security administrators through the steps for the vSec CMS *S* Series Integration with SafeNet Network HSM and HSMoD service, and also covers the necessary information to install, configure and integrate vSEC CMS with SafeNet Network HSM and HSMoD.

Scope

This document outlines the steps to integrate vSEC CMS with SafeNet HSM. SafeNet HSM is used to secure the Master Encryption Key for vSEC CMS.

Revisions

Name	Date	Reason for change	Version
Akhil Babal	06/08/2019	Document created	1.0

Gemalto Rebranding

In early 2015, Gemalto completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the Luna name has been removed from the SafeNet HSM product line, with the SafeNet name being retained. As a result, the product names for SafeNet HSMs have changed as follows:

Old product name	New product name
Luna SA HSM	SafeNet Network HSM
Luna PCI-E HSM	SafeNet PCI-E HSM
Luna G5 HSM	SafeNet USB HSM
Luna Client	SafeNet HSM Client



NOTE: These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:



NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:



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. These elements use the following format:



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.

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following:
	 Command-line commands and options (Type dir /p.)
	Button names (Click Save As.)
	• Check box and radio button names (Select the Print Duplex check box.)
	• Window titles (On the Protect Document window, click Yes .)
	• 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 Date box, type April 1 .)

Convention	Description
italic	The italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
Consolas	Denotes syntax, prompts, and code examples.

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information				
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA				
Phone	US 1-800-545-6608 International 1-410-931-7520				
Technical Support Customer Portal	rt https://serviceportal.safenet-inc.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 Knowled Base.				

1 Introduction

Overview

This document is intended to guide security administrators through the steps for the vSEC CMS Integration with SafeNet Luna 7 HSM and DPoD (HSM on demand service), and also covers the necessary information to install, configure and integrate vSEC CMS with SafeNet Luna HSM.

A HSM can be used to store the master key(s) used when performing administration key operations with the *S*-*Series* such as registering a smart card token or PIN unblock operations. The *S*-*Series* makes use of the PKCS#11 interface available in the HSM. All management functions around the master key stored on the HSM should be managed by the HSM key management tools available with LunaClient or DPoD service client.



NOTE: It is expected that the HSM PKCS#11 module is installed and configured to connect to the HSM on the server where the *S*-Series is installed. It is required that the 32 bit version (dll) of the HSM PKCS#11 module is available. The *S*-Series will search in the system path for the PKCS#11 module.

3rd Party Application Details

• vSEC CMS S Series 5.4

Supported Platforms

The following platforms are tested with SafeNet Luna HSM:

vSEC CMS S Series 5.4

Platforms Tested	SafeNet Luna HSM	SafeNet Network HSM	SafeNet Network HSM
	Client Software Version	Appliance S/W version	Appliance F/W version
Windows 2016	7.3	7.3.0-165	7.3.0

Prerequisites

SafeNet Network HSM Setup

Refer to the SafeNet Network HSM documentation for installation steps and details regarding the configuration and setup of the box on Windows systems. Before you get started ensure the following:

- SafeNet Network HSM appliance and a secure admin password.
- SafeNet Network HSM, and a hostname, suitable for your network.
- SafeNet Network HSM network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Network HSM appliance.
- Create and exchange certificates between the SafeNet Network HSM and your Client system.
- Create a partition on the HSM, remember the partition password that will be later used by vSEC CMS.
- Register the Client with the partition. And run the "vtl verify" command on the client system to display a
 partition from SafeNet Network HSM. The general form of command is "C:\Program
 Files\SafeNet\LunaClient> vtl verify" for Windows.
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Data Protection on Demand (DPoD) HSM service Setup

Refer to SafeNet Data Protection on Demand Documentation for service client setup steps and details.

https://gemalto.na.market.dpondemand.io/docs/tenant_admin/Content/dpod/services/hsmod/hsmod.html

Before you get started ensure the following:

- SafeNet DPOD subscription is available.
- HSM on Demand tile is available under Tenant Account.
- Application owner account is created and has access to HSMoD service tile.
- HSMoD service client is configured.
- HSMoD service is accessible using the service client.
- Partition is initialized using LunaCM tool.
- Partition roles are initialized and password for Crypto Office is created. This CO password will be required in vSEC settings.

vSEC CMS Prerequisites for Installation

Before installing vSEC CMS on a Windows Server, ensure that the system chosen meets the necessary operating system, hardware, software, and communications requirements.

For the installation requirements for data server products, see Appendix.

vSEC CMS Installation and Configuration

vSEC CMS must be installed on the target machine to carry on with the integration process. For a detailed installation procedure of vSEC CMS refer to the Versasec Documentation, reference of the same is provided in Appendix.

2 Integrating SafeNet Luna HSM with vSEC CMS

Creating a Connection with HSM from vSEC CMS

Follow these steps to create a connection with Luna 7 after vSEC CMS is installed using System Owner card.

1. Navigate to Options> Connections option

versasec	cycle Acti	ons v	Repository v	Templates v	Options v	
lome					License	
License information License ID: 50000170 Gemalto				System In vSEC:CMS®	<u>S</u> ettings <u>S</u> ecurity	vSEC:CMS
End-User License Agreement				More inform:	S <u>m</u> art Cards	
Number of user smart card licens	es used:	1		Available sp	₽I <u>V</u>	
	1 / 10 cards				Device Management	bytes used, 29846 free
Enrollment certificate expiration:		2021-03-0	01	_	Master <u>K</u> ey	
	634 days left					3 GB left on C:\
	634 days left				Virtual Smart Card	3 GB left on CA

2. To create a new connection, select Add and then Hardware Security Module (HSM)

		Deservites	Tomoloton	0-1		
ersasec	Lifecycle Actions V	Repository V	remplates v	Opuons V		
ome > Options > Connections						
vSEC:CMS - Add Extras Co	nnector	×				
- Connectors			h			
Available:	[Search 🔍	J			
Active Directory	1.		Ŋ			
API Service			J			
Data Export			h			
Email						
External Trace Hardware Security Module (HSM)		L L			
LDAP Server						
Operator Console Service						
Photo Capture Physical Access						
Plugin API			2			
RSDM Service						
SQL Database						
Configure Hardware Security	Module (HSM) Connectors					
	,					
	(<u>o</u> k) (<u>C</u> ancel)				
			[~	_	
		(Coi	nfigu <u>r</u> e)	[<u>A</u> dd		
				-		

3. Create a Template name and select SafeNet Luna from the drop down list.

Home > Options > Connections	
Enabled Connections —User Self-Service	✓ vSEC:CMS - HSM Configuration - □ X
Self-service server stopped. Hardware Security Module (H	HSM Configuration Template name:
Active Directory	Luna 7
Number of connections configured:	SafeNetLuna
Number of connections configured: Number of pending records:	PKCS11 DLL name: C:\Program Files\SafeNetiLunaClient\win32\cryptoki.dli
	URL: luna7.auth-demo.com:1792
	Slot. [0000000] vsec@Net Token Slot ▼
	Credentials PIN:
	Check connection
	Save Cancel
	Enrollment certificate OK NUM

4. Notice that if the Luna client is correctly installed on the vSEC CMS server and configured properly with Luna 7 HSM, the PKCS11 DLL and server details will auto populate. Select your slot ID and provide the

Cypto Officer password in the fields and check connection to verify CMS can connect to the partition on Luna HSM.



Troubleshooting Tip>

If the Luna Client is not correctly configured then it is warranted to run into errors.

When selecting SafeNet Luna HSM from the drop down list while adding a HSM connection, if you run into below shown error messages

	vSEC:CMS - Connections	_ 🗆 X
File Go Help		
versasec	Lifecycle Actions v Repository v Templates v Options v	
Home > Options > Connecti	VSEC:CMS - HSM Configuration	
Enabled Connectio	HSM Configuration	
-User Self-Service	Template name:	
Self-service server sto	Luna 7 HSM	
	Cataliat una	
	The driver for the SafeNet Luna HSM has not been installed.	
	Please install the driver before continue and configure it.	
	<u>Save</u>	
1		
	•	NUM

vSEC:CMS	•
Failed to retrieve HSM info. [OS error: 0x86000057] For detailed information about this issue click here. OK	
	VSEC:CMS Failed to retrieve HSM info. [OS error: 0x86000057] For detailed information about this issue click here. OK

The reason is by default Luna Client does not set ChrystokiConfigurationPath in System Environment Variables to point to 32 bit library

NOTE: It is expected that the HSM PKCS#11 module is installed and configured to connect to the HSM on the server where the *S*-*Series* is installed. It is required that the 32 bit version (dll) of the HSM PKCS#11 module is available. The *S*-*Series* will search in the system path for the PKCS#11 module.

When you modify and update the path in env variable then error will be resolved.

	System Properties
Computer Name	Hardware Advanced Remote
	Environment Variables
	Edit System Variable
Variable r	name: ChrystokiConfigurationPath
Variable	value: C:\Program Files\SafeNet\LunaClient\win32
	OK Cancel
	OK Califei
System vari	ables
System vari	ables
System vari Variable Chrystoki	ables Value Config C:Program Files\SafeNet\LunaClient\vi
System vari Variable Chrystoki0 ComSpec	ables Value Config C: (Program Files)SafeNet)LunaClient(wi C: (Windows)system32(pmd.exe
System vari Variable Chrystokić ComSpec FP_NO_He	ables Value Crifticu: C:\Pirogram Files\SafeNet\LunaClient\u0. C:\Vindows\pstem32\ord.exe OST_C NO
System varia Variable Chrystokić ComSpec FP_NO_He NUMBER_	ables Value Config C:\Program Files\SafeNet\LunaClient\ui C:\Windows\system32\cmd.exe OST_C NO OF_P 1 V
System varia Variable Chrystokić ComSpec FP_NO_H NUMBER_	ables Value Criffing C:fVrogram Files(SafeNet/LunaClient/wi C:fVlindows/system32/pmd.exe OF_P NO V New Edit Delete

Generate New Master Key

If it is required to generate a new master key, either on the operator token or on the HSM follow the instruction here.

WARNING: It is important to remember that any new user smart card administration key will be diversified from the newly generated master key. Any user smart card administration key diversified from the old administration key of the *S*-*Series* application will remain operable. However, it is recommended to re-register those user cards issued from the old administration key of the *S*-*Series*. This will update the user's smart card administration key so that it is diversified from the new master key.

For a new installation of vSEC CMS after successfully creating a HSM connection explained in previous section it is required to generate a new Master Key. This is shown as under System Status too

vSEC:CMS - Connections Go Help									×
versasec	Lifecycle	Actions v	Repository v	Templates v	Options v				
Home > Options > Connections	3								
Enabled Connection	VSEC:CMS - S	System Status				:	×		
-User Self-Service									
Self-service server stop	1	Title		Timestamp		[
Hardware Security	024	Self-service service	er not configured.	Mar 02, 201	9 01:34:57				
Module:	045	Only one (1) sys	tem owner.	Mar 02, 201	9 01:34:57				
	074	HSM has invalid	key or no valid key.	Mar 02, 201	9 01:38:12				
						Details			
					C	<u>C</u> lose			
			Co	onfigu <u>r</u> e	<u>A</u> dd				
				`					
								NUM	

Follow these steps to generate a new Master Key

1. From Options - Master Key click the Generate new master key button to start the process. A

vSEC:CMS - Master Key					- 🗆 X
Go Help					
versasec	Lifecycle Actio	ons v Repository	v Templates v	Options v	
versusee					
Iome > Options > Master Key					
New Master Key					
Master key seed:	77 0F 3D 81 8AA6 41	DE C4 41 83 A4			
	EF F1 37 4A C1 DB F0	95 C3 2C FE 80			
	1				
Com <u>m</u> ent					
	Generate new r	naster key			
	vSEC:CMS				
	0	The selected operatio	n requires Operator Toker	1	
	(A)	Token passcode to pr	oceed.	1	
		December 1			
	~	Passcode.			
			<u>C</u> ancel		
				Enrollment certificate OK	NUM

A dialog will be displayed.

2. Select **On vSEC:CMS Operator Card** if it is required that the new master key is generated on the connected full-featured operator token. The new master key will also be migrated to the HSM and any

other full-featured operator token(s) used in the *S*-*Series*. For a full-featured operator token the migration will take place the next time an operator logs onto the **S**-Series

 Select the option On server side HSM if it is required that the new master key should be generate on the HSM only. In this case the new master key will only be available on the HSM. Therefore, all operations that require master key access to the newly generated master key will need to use the HSM.

NOTE: For any smart card that was previously managed by the *S*-Series with a full-featured operator token that used an older master key that was not generated by the HSM it will be possible to continue to manage these cards but it is recommended to update these cards so that they will be managed by the newly created master key.

NOTE: For any smart card that was previously managed by the *S*-*Series* with a full-featured operator token that used an older master key that was not generated by the HSM it will be possible to continue to manage these cards but it is recommended to update these cards so that they will be managed by the newly created master key.

versasec	Lifecycle	Actions v	Repository v	Templates v Options v		
Home > Options > Master Key				GL/SEC/CMS		_
New Master Key				V VSCCONS		
Master key seed:	F3 C8 7D 29 [07 00 D5 35 8E E	7 C3 AC	Generate New Master	Key	
	31 A5 7B 44 1	5 EB 95 57 A8 CA		On vSEC:CMS Operator C	ard	
	,			Note: This option will gene Card and synchronizes it b	rate the new Master Key on the Operator netween all secure storages within the	
Com <u>m</u> ent:				system		
				On server side HSM		
	Genera	te <u>n</u> ew master key		Note: This option will gene	rate the new Master Key only on the	
				selected Operator Service only be available to the sys	Key Store (HSM). This means the key will stem if the HSM device is running and	
				activated from the Options	- Operators page.	
				Operator Service Key Store	a (HSM):	
						ì
)

As shown in the screen shot above the option to select **On Server side HSM** is unavailable. This will mean that the OSKS will need to be activated from the **Options - Operators** page. Instructions to create Operator Service Key Store (OSKS), see Appendix.

NUM

It is required to create OSKS before you follow next steps. Please see Appendix.

4. After generating, creating and enabling the OSKS the next step is to generate the new master key.

From Option > Master Key, select Generate new master key option and provide operator card login

Ø

Wersaser	Lifecycle Actions v	Repository v	Templates v Options v			
-versusee						
New Master Key						
Master key seed.	100 25 59 43 00 35 40 CEFC 91 50 52 60 27 88 44 37 44	F9 TE 41. 10 23:30				
Comment						
	0					
	Generate gew master	key				
		VSEC:CMS				
		A	The selected operation requires Operator Token passcode validation. Please enter your Operator Token passcode to proceed.	1		
			Passcode:			
			QK Cancel			
						Contract Contract

Select On server side HSM option and select key store added in step 3 (instruction in Appendix)

V VSEC:CIVIS	
Generate New Master Key	
O On vSEC:CMS Operator Card	
Note: This option will generate the new Master Key on the Op Card and synchronizes it between all secure storages within system	erator the
On server side HSM	
Note: This option will generate the new Master Key only on the selected Operator Service Key Store (HSM). This means the only be available to the system if the HSM device is running a activated from the Options - Operators page.	e key will nd
Operator Service Key Store (HSM):	
Operator Service Key Store (HSM):	•

Please read the warning message carefully and select yes.

vSEC:CMS	
?	It is important to remember that any new user smart card administration key will be diversified from the newly generated master key. Any user smart card administration key diversified from the old administration key of the system will remain operable. However, it is recommended to re-register those user cards issued from the old administration key of the system. This will update the user's smart card administration key so that it is diversified from the new master key.
	Do you want to generate a new Master Key at this time?
	<u>Y</u> es <u>N</u> o

After selecting yes, the new master keys will be created on the HSM as you can see via lunacm

```
Administrator: Command Prompt - Iunacm
lunacm:> par con
       The 'Crypto Officer' is currently logged in. Looking for objects
       accessible to the 'Crypto Officer'.
       Object list:
        Label:
                       CMS MK4097
       Handle:
                       130
       Object Type:
                       Symmetric Key
       Object UID:
                       760000035000001c26f0800
       Label:
                       CMS MKØ
       Handle:
                       246
       Object Type:
                       Symmetric Key
       Object UID:
                       7500000035000001c26f0800
       Label:
                       adnmfa-EC2AMAZ-T32BU5C-CA
       Handle:
                       252
       Object Type:
                       Private Key
       Object UID:
                       7300000035000001c26f0800
       Label:
                       adnmfa-EC2AMAZ-T32BU5C-CA
       Handle:
                       129
       Object Type:
                       Public Key
       Object UID:
                       7200000035000001c26f0800
       Number of objects: 4
Command Result : No Error
lunacm:>
```

Notice two symmetric keys are available, one was generated and one was migrated from your operator card in to HSM as explained in one of the steps in OSKS configuration.

At this stage, vSEC CMS is correctly configured with master key generated on the HSM.

3 Integrating DPoD with vSEC CMS

Steps to integrate vSEC CMS with HSM on Demand service are exactly same as they are explained in integration HSM with vSEC CMS (Chapter 2).

NOTE: It is expected that the HSM PKCS#11 module is installed and configured to connect to the HSM on the server where the *S-Series* is installed. It is required that the 32 bit version (dll) of the HSM PKCS#11 module is available. The *S-Series* will search in the system path for the PKCS#11 module.

A

M

WARNING: DPoD client by default only provides 64-bit version dlls. However, for vSEC integration it is required that 32 bit version dll of cryptoki.dll (PKCS#11 module) is available. Please contact Technical support team to request 32 bit version of dlls for DPoD client.

Creating a Connection with DPoD from vSEC CMS

Refer to the steps mentioned in integration with HSM, previous section. The steps are exactly same.

Important>

Once 32 bit version dlls are available, copy the win32 folder to DPoD client location and follow these steps before creating a connection in vSEC CMS.

- 1. Ensure to retain the original crystoki.ini created using DPoD client by running setenv
- Crystoki.ini initially created using setenv must be available to the location where 32 bit version dlls are located.
- 3. Accordingly update the System and user environment variable to update the ChrystokiConfigurationPath to location where 32 bit version cryptoki.dll is located.
- 4. In vSEC CMS while creating the connection select SafeNet Luna as option to add DPoD HSM on Demand to generate a new master key.

4 Appendix

1. The installation requirements for vSEC CMS products are listed in:

https://versasec.zendesk.com/hc/en-us/articles/115000766453-S-Series-Overview

2. The installation procedure of vSEC CMS is described in:

https://versasec.zendesk.com/hc/en-us/articles/115000402934-Install-and-Configure-S-Series-on-First-Use

3. Procedure to create Operator Service Key Store:

Follow the instructions in this section on how to configure the *S*-Series to use an HSM for OSKS. During this process, the master key stored on the operator smart card token will be migrated to the HSM.

Important: It will be required to RDP to the server where the S-Series is installed Ø to perform all the steps below. Important: The OSKS in this case is an encrypted component that runs as a Ц service which is accessible only by the S-Series. Important: The Operator needs to use a Full-Featured Operator Card that has a И role of System Administrator in order to carry out this process. **Important:** It will be necessary to have setup a connection to the HSM from ¥ Options - Connections before starting this setup.

From vSEC CMS version 5.3 onwards Activator Tool (AT) is available. The activator tool can be used to Generate Operator Service Key Store (OSKS) installer.

The AT is a standalone application that is located in the **tools** folder of the *S*-Series installation. The AT is named **Versasec-Activator.exe** in this folder. The AT requires internet access so it may be necessary to copy the AT to a host that has internet access if the *S*-Series is installed in a restricted environment.

Generate OSKS Installer

The OSKS is used by the S-Series to perform administration key operations. In order to set this up it will be firstly required to generate an OSKS installer.



Important: It will be required to use the SO to perform this task.

Important: It will be required to have the latest version of the Gemalto minidriver installed on the host where you are running the AT from.

Important: The host where you are running the AT from will need to have an internet connection.

In order to generate the OSKS installer start the AT. Attach the SO token and from the **Smart Card Selection** select the reader from the drop-down list that the SO is inserted into.

Smart Card Selection	Jasec	
Gemalto USB Sma	t Card Reader 0	•
icense Information		
icensed to:	Gemalto	
cense ID:	50000170	
icense volume:	10	
mart Card Action -		
Iccue System Ou	ner Card Issue Operator Card Clean Smart Card Create Key St	ore

g

A

•

Click the Create Key Store button. Enter the PIN for the SO when prompted. At the end of the process you will
be prompted to save the OSKS installer. Save the installer to complete this process.

🐼 Versasec Activator 5.3	× Save As			×
versasec	Save in:	Desktop		▼ ← m → m +
Smart Card Selection	Quick access	<mark>2</mark> at	abal	This PC
	Desktop	in a	braries	Network
Licensed to: Gemalto	Libraries		EC.CMS_S_Series fortcut 21 KB	610-013143-006_SW_Client
License ID: 50000170 Making Operator Key Store	This PC	da	ıt	vSEC_CMS_5.4.0.0
Smart Card Action	Network.			
Maling Operator Key Store		File name: Save as type:	keystore exe Files (*.exe)	✓ Save ✓ Cancel
				~

Versasec Activator 5.3	×
versasec	
_Smart Card Selection	
Gemalto USB Smart Card Reader 0	•
License Information Versasec Activator Licensed to: License ID: Operator Service Key Store successfully created.	×
-Smart Card Action	
Issue System Owner Card Issue Operator Card Clean Smart Card	Create Key Store
Making Operator Key Store	

Then you should move this installer to the server where the S-Series is installed.

Copy the installation package to the *S*-Series server. Make sure to close any open *S*-Series consoles and start the installation.

vSEC:CMS Operator Ser	vice Key Store Setu	р	_		×
<pre>(versasec</pre>	Install vSEC:CN	AS Operator Serv	ice Key Stor	e	
Setup will install vSEC:CM	S Operator Service K	ey Store in the follo	wing folder.		
Destination Folder					
C:\Program Files (x86	i)\Versasec\vSEC_CM	IS S-Series	Brow	se	
Space required: 1.9MB Space available: 32.7GB Nullsoft Install System v2.46					
		< Back	Install	Cano	el 🛛

Enable OSKS on vSEC CMS

When the installation completes log onto the *S*-*Series* application with the full-featured operator token used in step 1 or the System Owner token if you are using the **Activator Tool**.

Errolment certificate OK NUM



Important: You should see a message dialog informing the Operator that the package was successfully installed. If you do not see this message dialog then the installation was not successful.

Start the S-Series application and from the **Options - Security** page enable **Allow external smart card** administration key loading and **Enable operator service key store** check boxes.





Enable COM API for Operator Console

Remember Operator Token Passcode ✓ Inabled Berember Passcode for: 15 minutes (max: 15 min) Change backup passcode Change backup passcode VSEC:CMS Plugin Security Allow loading of unsigned library extensions (DLLs) Administrator Key Security ✓ Allow external smart card administrator key loading ✓ Enable operator gervice key store Application Security Allow application usage without operator card Logout without any action for: Ominutes (max: 15 min) Allow currently logged on Operator to self-issue token Enable collenge/response for offline PUC based unblock Yes No	versasec	Lifecycle Actions v Re	pository v ⁻	remplates ∨	Options v		
Image Passcode for: 15 minutes (max: 15 min) Apply Backup Passcode Change backup passcode vsEC:CMS Plugin Security Allow loading of unsigned library extensions (DLLs) Security By enabling the Operator Service Key Store the system's security will be lowered since the security of the system Image backup passcode Image backup passcode Image backup passcode Plugin Security Allow external smart card administrator key loading Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Plugin Security Allow external smart card administrator key loading Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode Image backup passcode backup passcode Image backup passcode	Remember Operator	Token Passcode					
Bernember Passcode for: 15 minutes (max: 15 min) △pply Backup Passcode Change backup passcode vsEC:CMS Plugin Security Allow loading of unsigned library extensions (DLLs) Administrator Key Security By enabling the Operator Service Key Store the system's security will be lowered since the security of the system ✓ Allow external smart card administrator key loading If you wish to enable this feature it is strongly recommended to harden the security of the server. ✓ Enable operator genvice key store Do you want to enable this feature now? Application Security If you without operator to self-issue token △ Allow currently logged on Operator to self-issue token Yes △ Allow currently logged on Operator Console Yes	Enabled						
Backup Passcode	Remember Passcode for:	15 minutes (max: 15 min)	Apply				
Change backup passcode vSEC:CMS Plugin Security Allow loading of unsigned library extensions (DLLs) Administrator Key Security Will be lowered since the security critical key for the system will be held in the server's memory and not protected by hardware. Image backup passcode If you wish to enable this feature it is strongly recommended to harden the security of the server. Image backup passcode If you wish to enable this feature now? Application Security Allow application usage without operator card Logout without any action for: Image: minutes (mac: 15 min) Allow currently logged on Operator to self-issue token Yes Enable challenge/response for offline PUC based unblock Yes Enable COM API for Operator Console Security	Backup Passcode						
Plugin Security Allow loading of unsigned library extensions (DLLs) Administrator Key Security By enabling the Operator Service Key Store the system's security will be lowered since the security critical key for the system Allow external smart card administrator key loading If you wish to enable this feature it is strongly recommended to harden the security of the server. By enablication Security Allow application usage without operator card Logout without any action for: minutes (mar: 15 min) Allow currently logged on Operator to self-lissue token Yes Enable challenge/response for offline PUC based unblock Yes	(Change <u>b</u> ackup passcode) vsec:cms				
Application Security □ Allow application usage without operator card Logout without any action for: 0 □ Allow currently logged on Operator to self-issue token ¥es □ Enable challenge/response for offline PUC based unblock □ Enable COM API for Operator Console	Plugin Security Allow loading of unsign Administrator Key Sec Allow external smart car C Enable operator <u>service</u>	eg library extensions (DLLs) c urity rd administrator <u>k</u> ey loading key store	?	By enabling will be lo will be held If you wis	the Operator Service Key Store the system wered since the security critical key for the s in the server's memory and not protected by th to enable this feature it is strongly recomm to harden the security of the server. Do you want to enable this feature now?	's security system r hardware. nended	
 Allow application usage without operator card Logout without any action for: 0 minutes (max: 15 min) Allow currently logged on Operator to self-issue token Enable challenge/response for offline PUC based unblock Enable COM API for Operator Console 	Application Security						
Allow currently logged on Operator to self-issue token Enable challenge/response for offline PUC based unblock Enable COM API for Operator Console	Allow application usage Logout without any action for	e without operator card or: 0 minutes (max: 15 min)					
Enable challenge/response for offline PUC based unblock Enable COM API for Operator Console	Allow currently logged o	n Operator to self-issue token			Yes <u>N</u> o		
Enable COM API for Operator Console	Enable challenge/respo	onse for offline PUC based unblock					
	Enable COM API for Ope	erator Console					

From the **Options - Operators** page click the **Add service key store** button. You should see that the **Key store** field is automatically populated with HSM. Enter a name for the **Store name** field and click the **Add** button to create the key store.

Versaser Lifecycle Actions v Reposite	ory v Templates v Options v	
Home > Options > Options		
Operators Registered operator smart cards:		Ethered by IQ
2 operator card(s) used.		Filtered by: All
ID Name Role(s) CSN	Type	Registered at Last logon at
00001 İşəhər Owwer İşətərin Admissistrator 20011351504	DAGOTIONE Pill Peaked Operator Card	W MCCAR-Add Service Key Store (MM)
		Ced reguest signing Lipdate keys Add gence key store Dirphin Add schoole Plachoole Bath Dirbhin Copy

When complete you will see that the service key store is added and that it is active. This completes the setup. The *S*-*Series* will use the master key stored in the HSM for any operations requiring administration key operations.

Versasec -	ifecycle Actions v	Repository v Templa	tes v Options v				
Home > Options > Operators Operators Registered operator smart card	15:					Eiltered by ID: Filtered by:	All 💌
3 operator card(s) used.	Role(s)	CSN	Type	Registered at	Lastlogon at		Show <u>a</u> ll
00002 ababal 00001 System Owner * 00000 Luna7 Key Store	All System Administrator n/a	380D2A7533000094380D2 5701135126BBA6071D1EF 8421AA05482DBEBAE7BD	Full Featured Operator Card Full Featured Operator Card n/a	Mar 02, 2019 02:42:43 Mar 01, 2019 18:50:10 Service key store (HSM)	Mar 02, 2019 03:30:20 Mar 02, 2019 03:39:24 Mar 02, 2019 03:43:58		

Cert reguest signing Lipdate keys Add genice key store Details Add school Inactivate Edit Details Copy