



VERSASEC VSEC:CMS

Integration Guide

Applicable Devices:

KMES Series 3



THIS DOCUMENT CONTAINS CONFIDENTIAL INFORMATION PROPRIETARY TO FUTUREX, LP. ANY UNAUTHORIZED USE, DISCLOSURE, OR DUPLICATION OF THIS DOCUMENT OR ANY OF ITS CONTENTS IS EXPRESSLY PROHIBITED.

TABLE OF CONTENTS

[1] DOCUMENT INFORMATION	3
[1.1] DOCUMENT OVERVIEW	3
[1.2] APPLICATION DESCRIPTION	3
[1.3] HSM SUPPORT IN VSEC:CMS	3
[2] PREREQUISITES	4
[3] INSTALL FUTUREX PKCS #11 (FXPKCS11)	5
[3.1] INSTRUCTIONS FOR INSTALLING THE FXPKCS11 MODULE USING FXTOOLS IN WINDOWS	5
[4] KMES SERIES 3 CONFIGURATION	6
[4.1] CREATE A ROLE AND IDENTITY FOR VERSASEC WITH THE REQUIRED PERMISSIONS	6
[4.2] ENABLE THE HOST API COMMANDS REQUIRED FOR THE VSEC:CMS OPERATION	6
[4.3] CONFIGURE TLS COMMUNICATION BETWEEN THE KMES SERIES 3 AND THE VSEC:CMS INSTANCE	7
[5] EDIT THE FUTUREX PKCS #11 CONFIGURATION FILE	14
[5.1] DEFINE CONNECTION INFORMATION	14
[5.2] SPECIAL DEFINES REQUIRED FOR THIS INTEGRATION	15
[6] CONFIGURING THE FUTUREX PKCS #11 LIBRARY IN VSEC:CMS	16
[6.1] LOG IN TO THE VSEC:CMS OPERATOR CONSOLE (OC)	16
[6.2] ENABLE THE HARDWARE SECURITY MODULE (HSM) CONNECTOR	16
[6.3] ADD A NEW HSM CONNECTION TEMPLATE AND CONFIRM SUCCESSFUL CONNECTION TO THE KMES SERIES 3	16
[7] CREATING AN OPERATOR SERVICE KEY STORE (OSKS) WITH HSM	17
[7.1] LOG IN TO THE VSEC:CMS OPERATOR CONSOLE (OC)	17
[7.2] ADD SERVICE KEY STORE WITH HSM	17
[7.3] VIEWING THE KEYS VSEC:CMS CREATED ON THE KMES SERIES 3	19
APPENDIX A: XCEPTIONAL SUPPORT	20

[1] DOCUMENT INFORMATION

[1.1] DOCUMENT OVERVIEW

The purpose of this document is to provide information regarding the configuration of the Futurex KMES Series 3 with vSEC:CMS using Futurex PKCS #11 libraries. For additional questions related to your KMES Series 3 device, see the relevant user guide.

[1.2] APPLICATION DESCRIPTION

From the [Versasec documentation website](#): "vSEC:CMS S-Series (vSEC:CMS) is an innovative, easily integrated and cost effective Credential Management System (CMS) that will help you deploy and manage credentials within your organization.

The vSEC:CMS is fully functional with minidriver enabled credentials such as smart cards and it streamlines all aspects of managing credentials by connecting to enterprise directories, certificate authorities, physical access control systems, email servers, log servers, biometric fingerprint readers, PIN mailers... the list goes on. With vSEC:CMS organizations can issue badges to employees, personalize the badges with authentication credentials and manage the lifecycle of the badges - directly from the off-the-shelf product."

Architecture Components

vSEC:CMS is separated into four main components:

- A MS Windows service, named vSEC:CMS Service (1) in the architecture drawing above, which manages the vSEC:CMS database in addition to operator account management for those operators who have access to vSEC:CMS. This service runs as a MS Windows service and will be installed by default to run under the MS Windows SYSTEM account;
- A MS Windows service, named vSEC:CMS SOAP/gRPC Service (11) in the architecture drawing above, which communicates with the vSEC:CMS Service and is the SOAP/gRPC service for the vSEC:CMS Agent (2) or vSEC:CMS Admin (3) and the vSEC:CMS User Self-Service Console (12);
- The vSEC:CMS Agent (2) or vSEC:CMS Admin (3), which is run by each operator in the user's context;
- The vSEC:CMS User (12) which is run on an end user's workstation from where credential users can perform self-service credential operations with conventional smart cards (8) or virtual smart cards (14).

[1.3] HSM SUPPORT IN VSEC:CMS

An HSM can be used to store the master key(s) used when performing administration key operations with the vSEC:CMS, such as registering a smart card token or PIN unblock operations. The vSEC:CMS interfaces with the HSM through the PKCS #11 protocol. All management functions around the master key stored on the HSM should be managed by the HSM key management tools available from the HSM vendor.

[2] PREREQUISITES

Supported Hardware:

- KMES Series 3, 6.3.x.x and above

Supported Operating Systems:

- Microsoft Windows 2012 Server
- Microsoft Windows 2012 R2 Server
- Microsoft Windows 2016 Server
- Microsoft Windows 2019 Server

Note: Virtual servers are supported.

Other:

- OpenSSL
- Futurex PKCS #11 (FXPKCS11) version 4.47 and above
- vSEC:CMS with an activated license (please refer to the installation and setup instructions in the following Versasec Support article: <https://versasec.zendesk.com/hc/en-us/articles/360014298379>)

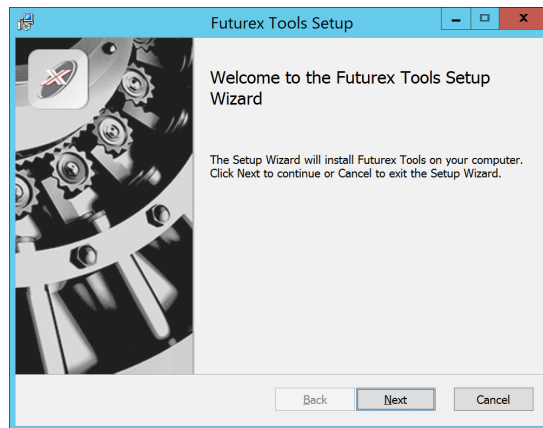
[3] INSTALL FUTUREX PKCS #11 (FXPKCS11)

In a Windows environment, the easiest way to install the **Futurex PKCS #11 (FXPKCS11)** module is with **Futurex Tools (FXTools)**. You can download FXTools from the Futurex Portal. Step-by-step installation instructions are provided below.

Note: The Futurex PKCS #11 module needs to be installed on the computer where **Versasec vSEC:CMS** is installed.

[3.1] INSTRUCTIONS FOR INSTALLING THE FXPKCS11 MODULE USING FXTOOLS IN WINDOWS

- Run the FXTools installer as an administrator



By default, all tools are installed on the system. A user can overwrite and choose not to install certain modules.

- **Futurex Client Tools** –Command Line Interface (CLI) and associated SDK for both Java and C.
- **Futurex CNG Module** –The Microsoft Next Generation Cryptographic Library.
- **Futurex Cryptographic Service Provider (CSP)** –The legacy Microsoft cryptographic library.
- **Futurex EKM Module** –The Microsoft Enterprise Key Management library.
- **Futurex PKCS #11 Module** –The Futurex PKCS #11 library and associated tools.
- **Futurex Secure Access Client** –The client used to connect a Futurex Excrypt Touch to a local laptop, via USB, and a remote Futurex device.

After starting the installation, all noted services are installed. If the Futurex Secure Access Client was selected, the Futurex Excrypt Touch driver will also be installed (Note this sometimes will start minimized or in the background).

After installation is complete, all services are installed in the **C:\Program Files\Futurex** directory. The CNG Module, CSP Module, EKM Module, and PKCS #11 Module all require configuration files, located in their corresponding directory with a **.cfg** extension.

Note: Only the HSM version of the PKCS #11 configuration file is installed. For KMES integrations, the **<HSM>** section needs to be replaced with a **<KMS>** section.

[4] KMES SERIES 3 CONFIGURATION

The first half of this section covers general configurations users must make on the KMES to allow Versasec vSEC:CMS to integrate with the KMES for storing the master key(s) used when performing administration key operations with the vSEC:CMS, such as registering a credential or PIN unblock operations. The second half of this section covers the steps required to configure TLS communication between the KMES and the vSEC:CMS instance.

[4.1] CREATE A ROLE AND IDENTITY FOR VERSASEC WITH THE REQUIRED PERMISSIONS

A new role and identity need to be created for vSEC on the KMES Series 3.

Note: In a later section, the name of this identity will be configured inside of the Futurex PKCS #11 configuration file.

1. Log in to the KMES Series 3 application interface with the default Admin identities.
2. Go to the **Identity Management** menu, select **Roles**, and click the [**Add...**] button. This will pull up the **Role Editor** dialog.
3. Specify a name for the role, set the number of logins required to **1**, and navigate to the **Advanced** tab and allow authentication to the **Host API** port only. All other fields can be left as the default values.
4. Move to the **Permissions** tab and select the following permissions:
 - **Cryptographic Operations** -> **Sign, Verify, Encrypt, Decrypt**
 - **Keys** -> **Add, Export**
5. Click the [**OK**] button to finish creating the role.
6. Go to **Identities**, right-click anywhere on in the window and select **Add > Client Application**.
7. In the **Identity Editor** dialog:
 - a. Under **Info**, select **Application** for the storage location, and specify a **name** for the identity.
 - b. Under **Assigned Roles**, select the role you created.
 - c. Under **Authentication**, configure the password.
 - d. Leave all other fields as the default values and click the [**OK**] button to finish creating the identity.

[4.2] ENABLE THE HOST API COMMANDS REQUIRED FOR THE VSEC:CMS OPERATION

Because the Futurex PKCS #11 library will be connecting to the Host API port on the KMES, users must define which Host API commands will be enabled for execution by the FXPKCS11 library. To set the enabled commands, complete the following steps:

1. Log in to the KMES Series 3 application interface with the default Admin identities.
2. Go to **Administration > Configuration > Host API Options**, enable the commands listed below, then click [**Save**].

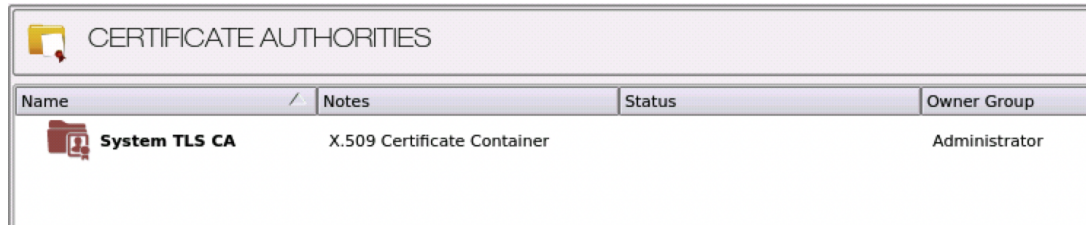
- **ATKG**: Manipulate HSM trusted asymmetric key group
 - **add**
 - **modify**
 - **delete**
 - **get**
- **ECHO**: Communication Test/Retrieve Version
- **RAFA**: Filter Issuance Policy
- **RKCP**: Get Command Permissions
 - **get**
 - **modify**
- **RKCS**: Create Symmetric HSM Trusted Key Group
- **RKDP**: Delete Asymmetric HSM Trusted Key
- **RKED**: Encrypt or Decrypt Data
- **RKLN**: Lookup Objects
- **RKLO**: Login User
- **RKPK**: Pop Generated Key
- **RKRC**: Get HSM Trusted Key
- **RKRU**: RSA unwrap symmetric key
- **TIME**: Set Time


[4.3] CONFIGURE TLS COMMUNICATION BETWEEN THE KMES SERIES 3 AND THE VSEC:CMS INSTANCE

[4.3.1] Create a Certificate Authority (CA)

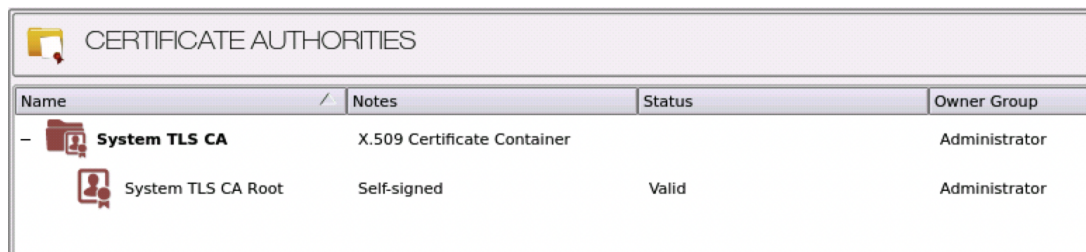
1. Log in to the KMES Series 3 application interface with the default Admin identities.
2. Select **PKI > Certificate Authorities** in the left menu, then click the [**Add CA...**] button at the bottom of the page.
3. In the **Certificate Authority** dialog, enter a name for the Certificate Container, leave all other fields as the default values, then click [**OK**].



- The Certificate Container that was just created will be listed now in the Certificate Authorities menu.



CERTIFICATE AUTHORITIES			
Name	Notes	Status	Owner Group
 System TLS CA	X.509 Certificate Container		Administrator

- Right-click on the Certificate Container and select **Add Certificate > New Certificate...**
- In the **Subject DN** tab, set a Common Name for the certificate, such as "System TLS CA Root".
- In the **Basic Info** tab, leave all of the default values set
- In the **V3 Extensions** tab, select the **Certificate Authority** profile, then click [OK].
- The root CA certificate will be listed now under the previously created Certificate Container.

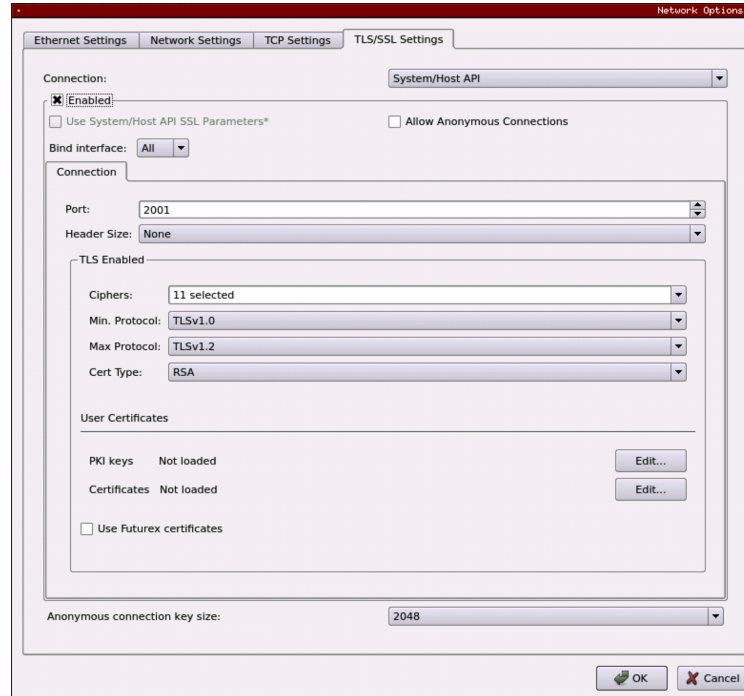


CERTIFICATE AUTHORITIES			
Name	Notes	Status	Owner Group
-  System TLS CA	X.509 Certificate Container		Administrator
 System TLS CA Root	Self-signed	Valid	Administrator

[4.3.2] Generate a CSR for the System/Host API connection pair

- Go to **Administration > Configuration > Network Options**.
- In the **Network Options** dialog, select the **TLS/SSL Settings** tab.

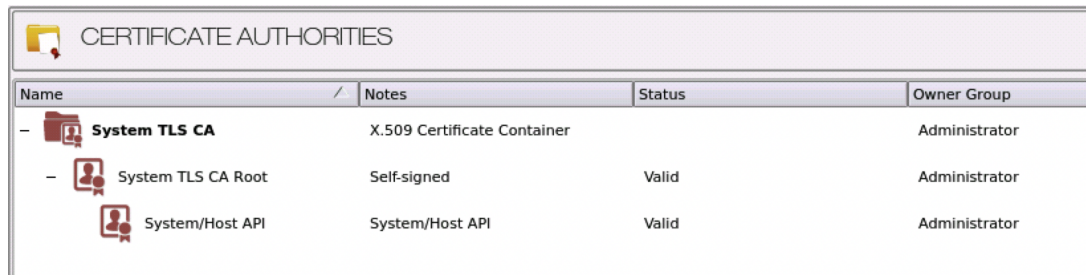
- Under the **System/Host API** connection pair, uncheck **Use Futurex certificates**, then click [**Edit...**] next to PKI keys in the User Certificates section.



- In the **Application Public Keys** dialog, click [**Generate...**]
- There will be a warning stating that SSL will not be functional until new certificates are imported. Select [**Yes**] if you wish to continue.
- In the **PKI Parameters** dialog, leave the default values set and click [**OK**].
- It should show that a PKI Key Pair is loaded now in the **Application Public Keys** dialog. If this is the case, click [**Request...**]
- In the **Subject DN** tab, set a Common Name for the certificate, such as "KMES".
- In the **V3 Extensions** tab, select the **TLS Server Certificate** profile.
- In the **PKCS #10 Info** tab, select a save location for the CSR, then click [**OK**].
- There should be a message stating that the certificate signing request was successfully written to the file location that was selected. Click [**OK**].
- Click **OK** again to save the **Application Public Keys** settings.
- In the main **Network Options** dialog, it should now show **Loaded** next to **PKI keys** for the System/Host API connection pair.

[4.3.3] Sign the System/Host API CSR

1. Go to **PKI > Certificate Authorities** menu.
2. Right-click on the root CA certificate created in section 2.1.1, then select **Add Certificate > From Request...**
3. In the file browser, find and select the CSR that was generated for the System/Host API connection pair.
4. Once loaded, none of the settings need to be modified for the certificate. Click **[OK]**.
5. The signed System/Host API certificate should now show under the root CA certificate on the **Certificate Authorities** page.



Name	Notes	Status	Owner Group
System TLS CA	X.509 Certificate Container		Administrator
System TLS CA Root	Self-signed	Valid	Administrator
System/Host API	System/Host API	Valid	Administrator

[4.3.4] Export the Root CA certificate

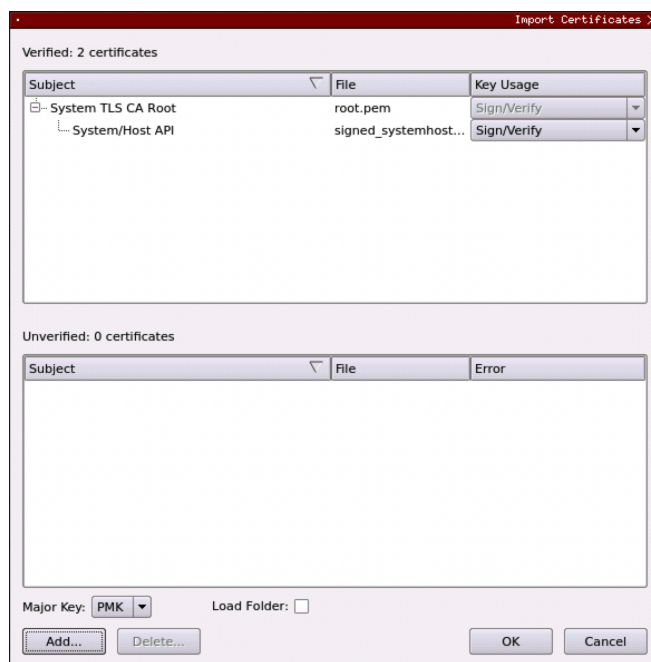
1. Go to **PKI > Certificate Authorities** menu.
2. Right-click on the **System TLS CA Root** certificate, then select **Export > Certificate(s)...**
3. In the **Export Certificate** dialog, change the encoding to **PEM**, then click **[Browse...]**.
4. In the file browser, navigate to the location where you want to save the Root CA certificate. Specify "tls_ca.pem" as the name for the file, then click **[Open]**.
5. Click **[OK]**. A message box will pop up stating that the PEM file was successfully written to the location that you specified.

[4.3.5] Export the signed System/Host API certificate

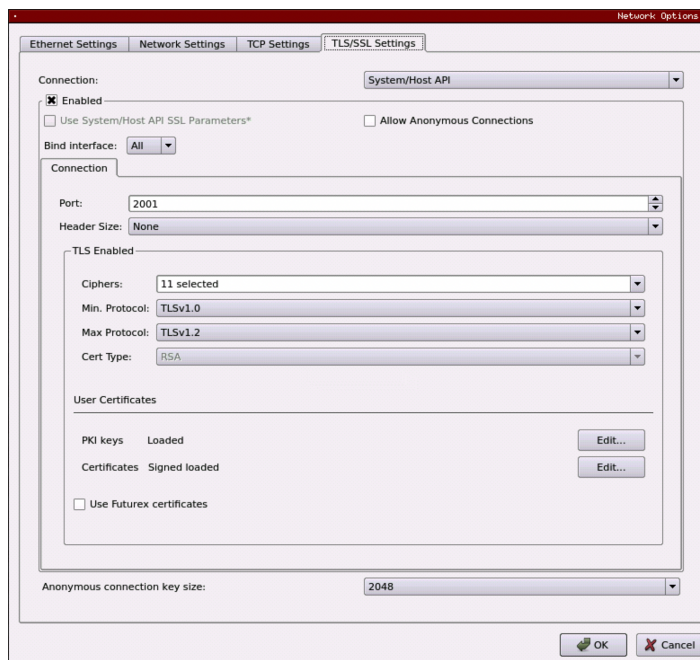
1. Go to **PKI > Certificate Authorities** menu.
2. Right-click on the **KMES** certificate, then select **Export > Certificate(s)...**
3. In the **Export Certificate** dialog, change the encoding to **PEM**, then click **[Browse...]**
4. In the file browser, navigate to the location where you want to save the signed System/Host API certificate. Specify "tls_ca.pem" as the name for the file, then click **[Open]**.
5. Click **[OK]**. A message box will pop up stating that the PEM file was successfully written to the location that you specified.

[4.3.6] Load the exported certificates into the System/Host API connection pair

1. Go to **Administration > Configuration > Network Options**.
2. In the **Network Options** dialog, select the **TLS/SSL Settings** tab.
3. Click [**Edit...**] next to Certificates in the User Certificates section.
4. Right-click on the **System/Host API SSL CA X.509 Certificate Container**, then select [**Import...**]
5. Click [**Add...**] at the bottom of the **Import Certificates** dialog.
6. In the file browser, find and select both the root CA certificate and the signed System/Host API certificate, then click [**Open**]. The certificate chain should appear as shown below:



- Click [**OK**] to save the changes. In the **Network Options** dialog, the System/Host API connection pair should show **Signed loaded** next to Certificates in the **User Certificates** section, as shown below:



- Click [**OK**] to save and exit the Network Options dialog.

[4.3.7] Issue a client certificate for vSEC:CMS

Note: The client certificate that is being created for vSEC:CMS will be configured inside of the Futurex PKCS #11 configuration file.

- Go to **PKI > Certificate Authorities** menu.
- Right-click on the **System TLS CA Root** certificate and select **Add Certificate > New Certificate....**
- In the **Subject DN** tab, set a Common Name for the certificate, such as "vSEC".
- All settings in the **Basic Info** tab should be left as the default values.
- In the **V3 Extensions** tab, select the **TLS Client Certificate** profile, then click [**OK**].
- The vSEC certificate will be listed now under the **System TLS CA Root** certificate.

[4.3.8] Export the vSEC:CMS certificate as PKCS #12 file

Note: To be able to perform the steps below you must go to **Configuration > Options** and enable the **Allow export of certificates using passwords** option.

- Go to **PKI > Certificate Authorities** menu.
- Right-click on the vSEC certificate, then select **Export > PKCS12...**

3. Make sure that the **Export Selected** option is selected, specify a unique name for the export file, then click **Next**.
4. Input a file password of your choosing, then click **Next**.
5. Click [**Finish**] to initiate the export.

Note: The **vSEC** certificate and the Root CA certificate that was exported in section 4.4.4 both need to be moved to the computer that will be running the vSEC:CMS instance. In a later section, they will be configured and used for TLS communication with the KMES Series 3.

[5] EDIT THE FUTUREX PKCS #11 CONFIGURATION FILE

[5.1] DEFINE CONNECTION INFORMATION

The **fxpkcs11.cfg** file allows the user to set the Futurex PKCS #11 (FXPKCS11) library to connect to the KMES Series 3. To edit, run a text editor as an Administrator and edit the configuration file accordingly. Most notably, the fields shown below must be set inside the **<KMS>** section (note that the full **fxpkcs11.cfg** file is not included).

Note: The Futurex PKCS #11 (FXPKCS11) library expects the configuration file to be in a certain location (i.e., **C:\Program Files\Futurex\fxpkcs11\fxpkcs11.cfg** for Windows, but that location can be overwritten using an environment variable (**FXPKCS11_CFG**).

```
<KMS>
# Which PKCS11 slot
<SLOT>                0                </SLOT>

# Login username
<CRYPTO-OPR>          vSEC                </CRYPTO-OPR>

# Key group name
<KEYGROUP-NAME>      vSEC-symmetric-keygroup    </KEYGROUP-NAME>

# Connection information
<ADDRESS>             10.0.8.20          </ADDRESS>
<PROD-PORT>           2001                </PROD-PORT>
<PROD-TLS-ENABLED>    YES                </PROD-TLS-ENABLED>
<PROD-TLS-ANONYMOUS> NO                </PROD-TLS-ANONYMOUS>
# <PROD-TLS-CA>        /home/user/tls/root.pem          </PROD-TLS-CA>
# <PROD-TLS-CERT>      /home/user/tls/signed-client-cert.pem    </PROD-TLS-CERT>
<PROD-TLS-KEY>        /home/user/tls/vsec-client-cert.p12  </PROD-TLS-KEY>
<PROD-TLS-KEY-PASS>   safest                </PROD-TLS-KEY-PASS>

# YES = This is communicating through a Guardian
<FX-LOAD-BALANCE>    NO                </FX-LOAD-BALANCE>
</KMS>
```

The **<SLOT>** field can remain set to the default value of 0.

In the **<CRYPTO-OPR>** field, specify the name of the identity that was created on the KMES in section 4.3.

The **<KEYGROUP-NAME>** field can remain set to the default value, **keygroup1**, or a different name can be specified, as shown above.

In the **<ADDRESS>** field, specify the IP or hostname of the KMES that the FXPKCS11 library should connect to.

In the **<PROD-PORT>** field, set the FXPKCS11 library to connect to the default Host API port on the KMES, port **2001**.

Set the **<PROD-TLS-ENABLED>** field to **YES**.

The **<PROD-TLS-ANONYMOUS>** field defines whether the FXPKCS11 library will attempt to authenticate to the KMES. Set this value to **YES** since mutual TLS authentication was configured.

Because a PKCS #12 file is being used to connect, the **<PROD-TLS-CA>** and **<PROD-TLS-CERT>** tags need to either be removed or commented out.

In the **<PROD-TLS-KEY>** tag, specify the location of the PKCS #12 file exported in section 4.1.8. This file contains the Venafi private key and certificate, encrypted under the password specified in the **<PROD-TLS-KEY-PASS>** field.

If a Guardian is being used to manage KMES Series 3 devices in a cluster, the **<FX-LOAD-BALANCE>** field must be defined as “YES”. If a Guardian is not being used it should be set to “NO”.

For additional details, reference the Futurex PKCS #11 technical reference found on the Futurex Portal.

Once the `fxpkcs11.cfg` file is edited, run the **PKCS11Manager** file to test the connection against the KMES Series 3, and check the **fxpkcs11.log** for errors and information. For more information, see our Administrator’s Guide.

[5.2] SPECIAL DEFINES REQUIRED FOR THIS INTEGRATION

For the Versasec integration, the following defines must be added to the **<CONFIG>** section of the `FXPKCS11` configuration file:

```
# Required for the vSEC integration
<KEY-REQUIRE-LOGIN>      NO          </KEY-REQUIRE-LOGIN>
<ALLOW-DUPLABELS>       YES         </ALLOW-DUPLABELS>
<ENFORCE-IMMUTABLE>     NO          </ENFORCE-IMMUTABLE>
```

[6] CONFIGURING THE FUTUREX PKCS #11 LIBRARY IN VSEC:CMS

Note: Before proceeding with the steps below, vSEC:CMS must be installed and set up per the instructions outlined in the following Versasec Support article: <https://versasec.zendesk.com/hc/en-us/articles/360014298379>

Once vSEC:CMS is installed and configured, proceed with the steps below to configure the Futurex PKCS #11 (FXPKCS11) library in vSEC:CMS.

[6.1] LOG IN TO THE VSEC:CMS OPERATOR CONSOLE (OC)

1. Start the **vSEC:CMS Admin** application.
2. When prompted, insert your System Owner (SO) hardware credential.
3. Enter the operator passcode for the System Owner and click **Authenticate**.
4. If authentication is successful, the Admin application will start, and you will be logged in to the Operator Console.

[6.2] ENABLE THE HARDWARE SECURITY MODULE (HSM) CONNECTOR

1. In the navigation menu, select **Options > Connections**.
2. Click the **Configure** button. This will bring up the **Extras Connector Configuration** dialog.
3. Select **Hardware Security Module (HSM)** in the list of available Connectors, click the **>>** button, then click **OK**. **Hardware Security Module (HSM)** will now be listed under **Enabled Connections**.

[6.3] ADD A NEW HSM CONNECTION TEMPLATE AND CONFIRM SUCCESSFUL CONNECTION TO THE KMES SERIES 3

1. In the navigation menu, select **Options > Connections**.
2. Select the **Hardware Security Module (HSM)** under **Enabled Connections**. This should bring up the **HSM Connection** dialog.
3. Click the **Add** button. This will bring the **HSM Configuration** dialog.
4. Enter a name for the template, then select **FutureX VirtuCrypt** in the drop-down list. If vSEC:CMS can find the Futurex PKCS #11 module in the system path, the **HSM Parameters** section will appear, and the path to the FXPKCS11 DLL file will be shown in the **PKCS11 DLL name** field.
5. In the **Slot** field, select slot number **0**.
6. In the **PIN** field, enter the password for the identity configured in the FXPKCS11 configuration file (i.e., fxpks11.cfg), then click **Check connection**.

If the connection is successful, you will see the message, "Server connection successfully established."

7. Click **OK**, then click **Save** to finish creating the template.

[7] CREATING AN OPERATOR SERVICE KEY STORE (OSKS) WITH HSM

This section will explain how to configure vSEC:CMS to use the KMES Series 3 for the Operator Service Key Store (OSKS). During this process, the master key stored on the System Owner (SO) token will be migrated to the KMES.

[7.1] LOG IN TO THE VSEC:CMS OPERATOR CONSOLE (OC)

1. Start the **vSEC:CMS Admin** application.
2. When prompted, insert your System Owner (SO) hardware credential.
3. Enter the operator passcode for the System Owner and click **Authenticate**.
4. If authentication is successful, the Admin application will start, and you will be logged in to the Operator Console.

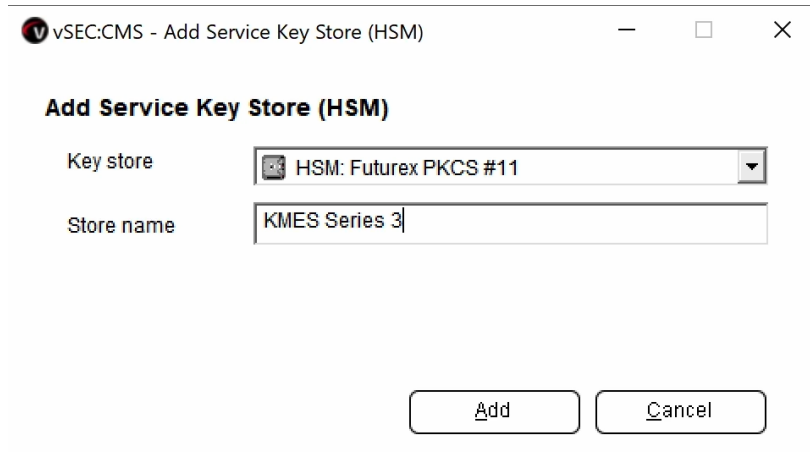
[7.2] ADD SERVICE KEY STORE WITH HSM

1. In the navigation menu, select **Options > Operators**.
2. Click the **Add service key store** button. This will bring up the **Add Service Key Store (HSM)** dialog.

The screenshot shows the 'Operators' page in the Versasec interface. The breadcrumb trail is 'Home > Options > Operators'. The page title is 'Operators'. Below the title, it says 'Registered operator smart cards:' and '2 operator card(s) used.'. There are filters for 'Filtered by ID:' and 'Filtered by:' (set to 'All'). A 'Show all' button is present. A table lists the registered cards with columns for ID, Name, Role(s), CSN, Type, Registered at, and Last logon at. Below the table is a row of action buttons: 'Cert request signing', 'Update keys', 'Add service key store', 'Details', 'Activate', 'Inactivate', 'Edit', 'Add', 'Delete', and 'Copy'. At the bottom right, there is a 'NUM' label.

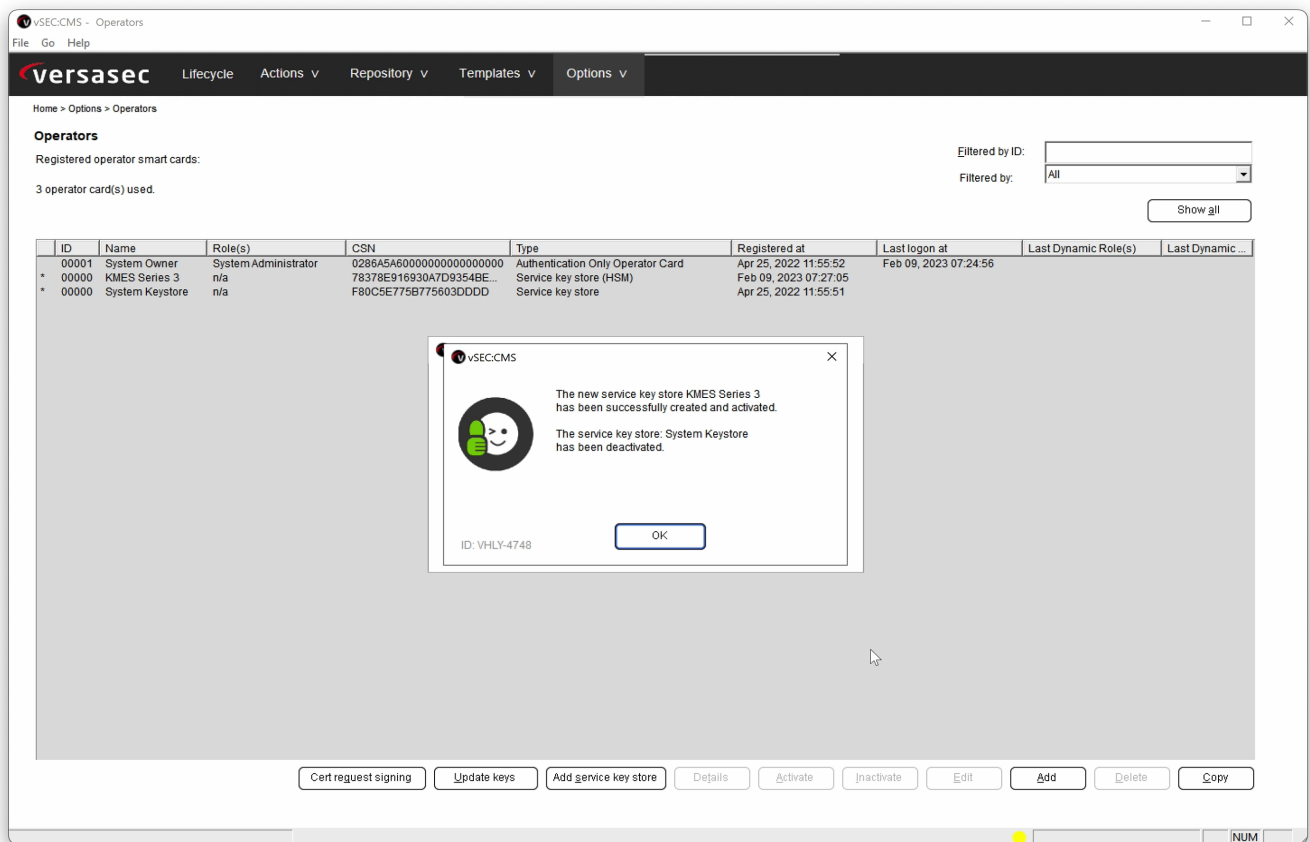
ID	Name	Role(s)	CSN	Type	Registered at	Last logon at
00001	System Owner	System Administrator	0286A5A60000000000000000	Authentication Only Operator Card	Apr 25, 2022 11:55:52	May 12, 2022 09:24:
* 00000	System Keystore	n/a	F80C5E775B775603DDDD	Service key store	Apr 25, 2022 11:55:51	

3. Select the Futurex PKCS #11 library in the **Key store** dropdown, specify a **Store name**, then click **Add**.



4. Enter the operator passcode for the System Owner, then click **OK**.

The new service key store will now be created, and the master keys will be stored on the KMES Series 3. You should see the message shown below, confirming that the operation was successful:



Now, all administration key operations performed with the vSEC:CMS, such as registering a smart card token or PIN unblock operations, will use the master keys stored on the KMES Series 3.

[7.3] VIEWING THE KEYS VSEC:CMS CREATED ON THE KMES SERIES 3

vSEC:CMS creates two 3DES symmetric encryption keys on the KMES Series 3. These are the master keys used by the vSEC:CMS application (they are assigned the "CMS MK0" and "CMS MK1" PKCS #11 labels).

To view the keys, perform the following steps:

1. Log in to the KMES application interface with the default admin identities (i.e., Admin1 and Admin2).
2. Navigate to the **Key Management > Keys** menu.
3. Select the symmetric key group that Versasec created on the KMES through the PKCS #11 library. This will display the two Triple 3DES symmetric data encryption keys in the **Keys** section of the menu.

The screenshot shows the Futurex application interface. On the left is a navigation menu with 'Key Management' selected. The main area is divided into two sections: 'KEY GROUPS' and 'KEYS'. The 'KEY GROUPS' table has one entry: 'vSEC-symkeygroup-feb9' with 2 keys. The 'KEYS' table has two entries:

Name	Key Group	Certificate	Version	Storage	Key type	Algorithm	Check Digits
CMS MK0_VSEC0000_1675956422	vSEC-symkeygroup-feb9			Trusted	Data Encryption Key	Triple 3DES	849F
CMS MK1_VSEC0001_1675956423	vSEC-symkeygroup-feb9			Trusted	Data Encryption Key	Triple 3DES	8BAF

At the bottom of the interface, it shows 'Roles: Administrator, Single Admin' and 'Users: Admin1, Admin2'. The status bar at the very bottom indicates 'VNC config', 'Futurex', and the time '20:45'.

APPENDIX A: XCEPTIONAL SUPPORT



In today's high-paced environment, we know you are looking for timely and effective resolutions for your mission-critical needs. That is why our Xceptional Support Team does whatever it takes to ensure you have the best experience and support possible. Every time. Guaranteed.

- 24x7x365 mission critical support
- Level 1 to level 3 support
- Extremely knowledgeable subject matter experts

At Futurex, we strive to supply you with the latest data encryption innovations as well as our best-in-class support services. Our Xceptional Support Team goes above and beyond to meet your needs and provide you with exclusive services that you cannot find anywhere else in the industry.

- Technical Services
- Onsite Training
- Virtual Training
- Customized Consulting
- Customized Software Solutions
- Secure Key Generation, Printing, and Mailing
- Remote Key Injection
- Certificate Authority Services

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com



ENGINEERING CAMPUS

864 Old Boerne Road
Bulverde, Texas, USA 78163

Phone: +1 830-980-9782

+1 830-438-8782

E-mail: info@futurex.com

EXCEPTIONAL SUPPORT

24x7x365

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

SOLUTIONS ARCHITECT

E-mail: solutions@futurex.com