MICROSOFT AD CS

Integration Guide

Applicable Devices:
KMES Series 3

TABLE OF CONTENTS

[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 Microsoft Active Directory Certificate Services' certificate authorities. For additional questions related to your KMES Series 3 device, see the relevant user guide.

[1.2] ABOUT MICROSOFT AD CS

Microsoft Active Directory Certificate Services (AD CS) provide management of certificates through a server that acts as a certificate authority (CA). With Futurex's support of AD CS, a network-connected KMES Series 3 can manage certificate authorities in a scalable manner and allow for secure storage, encryption, and signing via FXCL CNG.

[2] PREREQUISITES

Supported Hardware:

- KMES Series 3, 6.1.4.x and above

Supported Operating Systems:

- Windows 2012 R2 (6.3.9600) and above

Other:

- OpenSSL

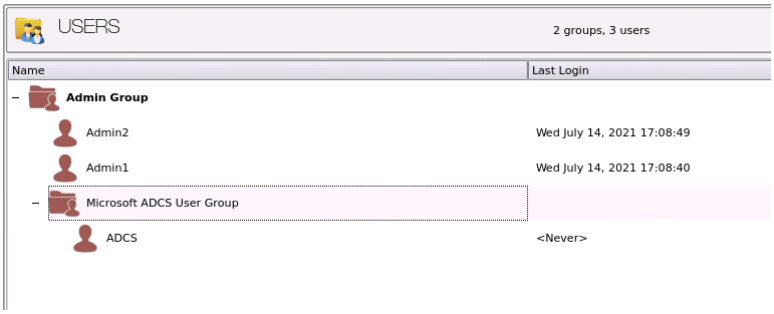
[3] KMES SERIES 3 CONFIGURATION

The first half of this section will cover general configurations that need to be made on the KMES Series 3 to allow Microsoft AD CS to integrate with the KMES to manage certificate authorities in a scalable manner and allow for secure storage, encryption, and signing via FXCL CNG. The second half of this section will cover the steps needed to configure TLS communication between the KMES and the AD CS instance.

[3.1] CREATE A USER FOR AD CS WITH THE REQUIRED PERMISSIONS

A new user group and user need to be created for AD CS on the KMES Series 3.

1. Log in to the KMES Series 3 application interface with the default Admin identities.
2. Go to the *Users* menu, expand the Admin user group, and click the **Add Group** button. This will pull up the *User Group Editor* dialog.
3. Specify a name for the user group, set the number of logins required to "1", and allow group members to authenticate 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:
    - Manage certificates -> Export
    - Manage keys -> Add
    - Perform cryptographic operations -> Sign
5. Click the **OK** button to finish creating the user group. The new user group should now be listed along with the other user groups that exist on the KMES Series 3.
6. Right-click on the newly created AD CS user group and select **Add** -> **User**.
7. In the *New User* dialog:
    a. Specify "ADCS" as the user name.
    b. Set a password.
    c. Leave all other fields as the default values and click the **OK** button to finish creating the user. The new user should now be listed inside of the AD CS user group.



[3.2] ENABLE THE HOST API COMMANDS REQUIRED FOR THE MICROSOFT AD CS OPERATION

Because FXCL CNG will be connecting to the Host API port on the KMES, users must define which Host API commands will be enabled for execution by FXCL CNG. To set the enabled commands, complete the following steps:

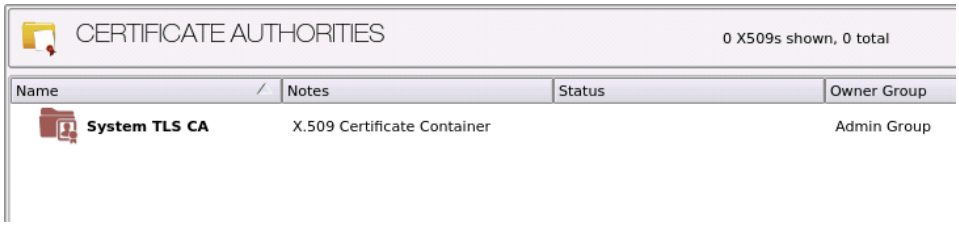
1. Log in to the KMES Series 3 application interface with the default Admin identities.
2. Go to *Configuration -> Host API Options*, enable the commands listed below, then click **Save**.

- **CLKY**: Manipulate application key (**NOTE:** Enable all CLKY subcommands.)
- **ECHO**: Communication Test/Retrieve Version
- **RKGP**: Export PKI keypair
- **RKGS**: Generate Signature
- **RKLN**: Lookup Objects
- **RKPK**: Pop Generated Key

[3.3] CONFIGURE TLS COMMUNICATION BETWEEN THE KMES SERIES 3 AND THE AD CS INSTANCE

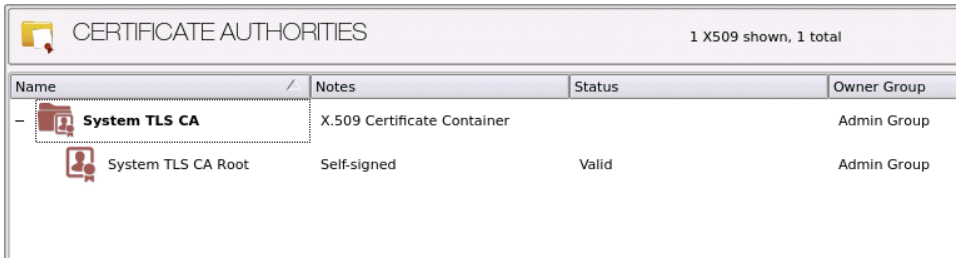
[3.3.1] Create a Certificate Authority (CA)

1. Log in to the KMES Series 3 application interface with the default Admin identities.
2. Select *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**.
4. The Certificate Container that was just created will be listed now in the Certificate Authorities menu.



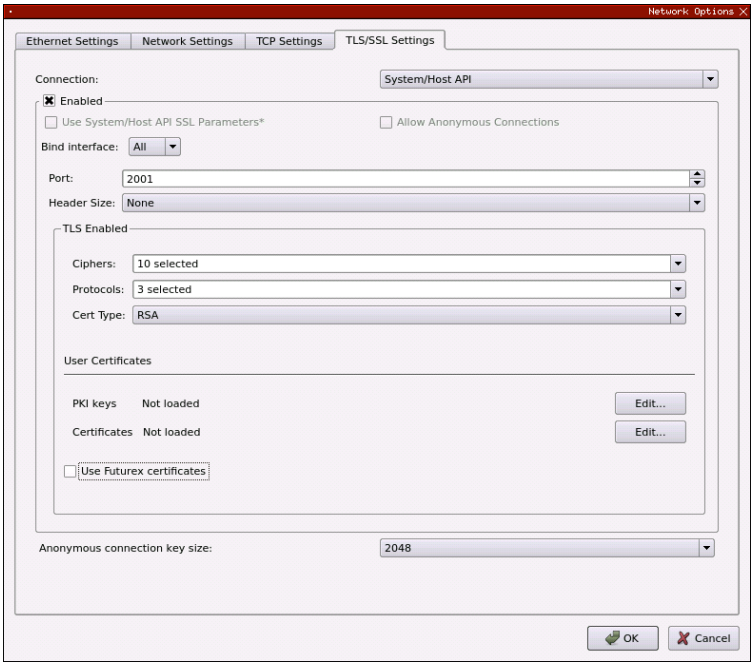
5. Right-click on the Certificate Container and select **Edit...**. In the *Certificate Authority* dialog, check the box that says, "Can be used for PKI authentication", then click **OK** to save.
6. Right-click on the Certificate Container again and select **Add Certificate -> New Certificate...**
7. In the *Subject DN* tab, set a Common Name for the certificate, such as "System TLS CA Root".
8. In the *Basic Info* tab, change the Major key to the **PMK**. All other settings can be left as the default values.

9. In the *V3 Extensions* tab, select the "Example Certificate Authority" profile, then click **OK**.
10. The root CA certificate will be listed now under the previously created Certificate Container.



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

1. Go to *Configuration -> Network Options*.
2. In the *Network Options* dialog, select the *TLS/SSL Settings* tab.
3. Under the **System/Host API** connection pair, uncheck "Use Futurex certificates", then click **Edit...** next to PKI keys in the User Certificates section.

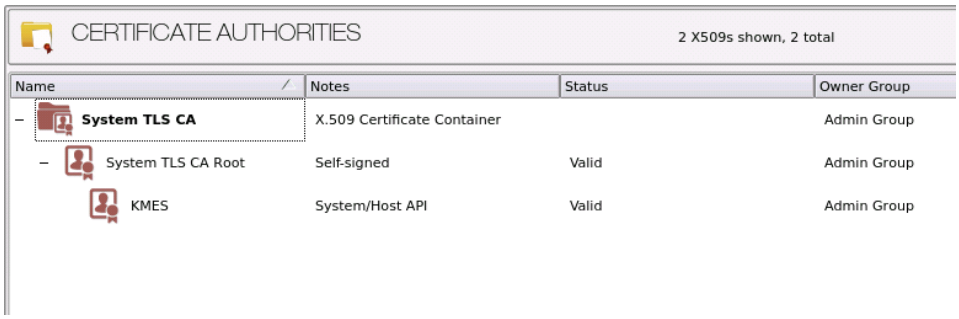


4. In the *Application Public Keys* dialog, click **Generate...**
5. There will be a warning stating that SSL will not be functional until new certificates are imported. Select **Yes** if you wish to continue.
6. In the *PKI Parameters* dialog, change the Encrypting key to the **PMK**, then change the Key Size to **2048** and click OK.

7. It should show that a PKI Key Pair is loaded now in the *Application Public Keys* dialog. If this is the case, click **Request...**
8. In the *Subject DN* tab, set a Common Name for the certificate, such as "KMES".
9. In the *V3 Extensions* tab, select the "Example TLS Server Certificate" profile.
10. In the *PKCS #10 Info* tab, select a save location for the CSR, then click **OK**.
11. There should be a message stating that the certificate signing request was successfully written to the file location that was selected. Click **OK**.
12. Click **OK** again to save the *Application Public Keys* settings.
13. In the main *Network Options* dialog, it should now say "Loaded" next to **PKI keys** for the System/Host API connection pair.

[3.3.3] Sign the System/Host API CSR

1. Go to the *Certificate Authorities* menu.
2. Right-click on the root CA certificate created in section 3.1.1, 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.



[3.3.4] Export the Root CA certificate

1. Go to the *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.

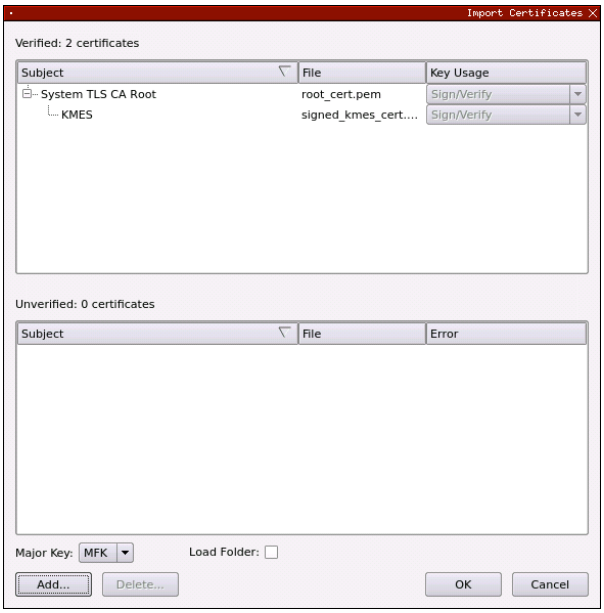
NOTE: The Root CA certificate will be configured later inside of the FXCL CNG configuration file.

[3.3.5] Export the signed System/Host API certificate

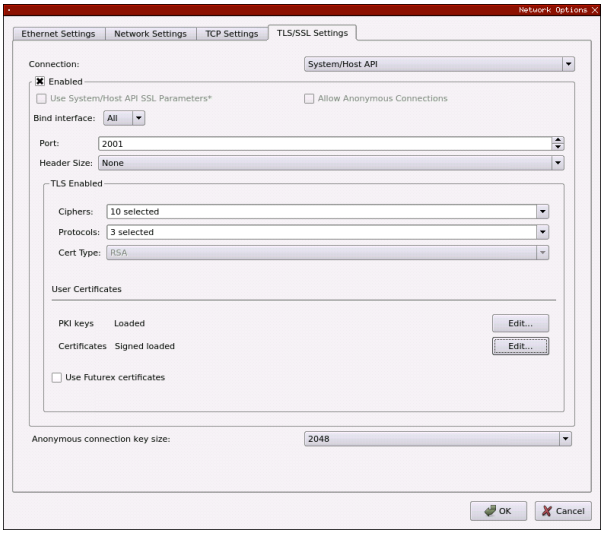
1. Go to the *Certificate Authorities* menu.
2. Right-click on the "KMES" certificate, then select **Export** -> **Certificate(s)...**
3. In the *Export Certificate* dialog, change the encoding to "PEM", then click **Browse...**
4. In the file browser, navigate to the location where you want to save 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.

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

1. Go to *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:



7. 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:



8. Click **OK** to save and exit the Network Options dialog.

[3.3.7] Issue a client certificate for AD CS

NOTE: The client certificate that is being created for AD CS will be configured later inside of the FXCL CNG configuration file.

1. Go to the *Certificate Authorities* menu.
2. Right-click on the **System TLS CA Root** certificate and select **Add Certificate** -> **New Certificate...**.
3. In the *Subject DN* tab, set "ADCS" as the Common Name for the certificate.

   NOTE: It is important that the Common Name of the certificate matches the name of the user created in section 3.1.
4. All settings in the *Basic Info* tab should be left as the default values.
5. In the *V3 Extensions* tab, select the "Example TLS Client Certificate" profile, then click **OK**.
6. The **ADCS** certificate will be listed now under the **System TLS CA Root** certificate.

[3.3.8] Export the ADCS 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.

1. Go to the *Certificate Authorities* menu.
2. Right-click on the **ADCS** certificate, then select **Export** -> **PKCS12...**

3. Make sure that the "Export Tree" 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**.

   NOTE: The P12 file password will be configured later inside of the FXCL CNG configuration file.
5. Click **Finish** to initate the export.

NOTE: The **ADCS** certificate and the Root CA certificate that was exported in section 3.4.4 both need to be moved to the computer where AD CS is running. In the next section, they will be configured and used for TLS communication with the KMES Series 3.

[3.4] GRANT THE AD CS USER GROUP "USE" PERMISSIONS ON THE CA TREE

1. Go to the *Certificate Authorities* menu.
2. Right-click on the CA container that was created in section 3.3.1, then select **Permission...**.
3. Grant the AD CS user group the "Use" permission, select "Apply to children recursively", then click **OK** to save.

[3.5] CONFIGURE PKI AUTHENTICATION FOR THE ADCS USER

1. Go to the Users menu.
2. Right-click on the ADCS user and select **Edit...**.
3. Go to the *PKI Auth* tab and click the **Add Trusted Certificate Authority** button next to System/Host API.
4. Select the CA container created in section 3.3.1, then click **OK**. It should say "Registered" now next to System/Host API.
5. Click **OK** in the main dialog to save.

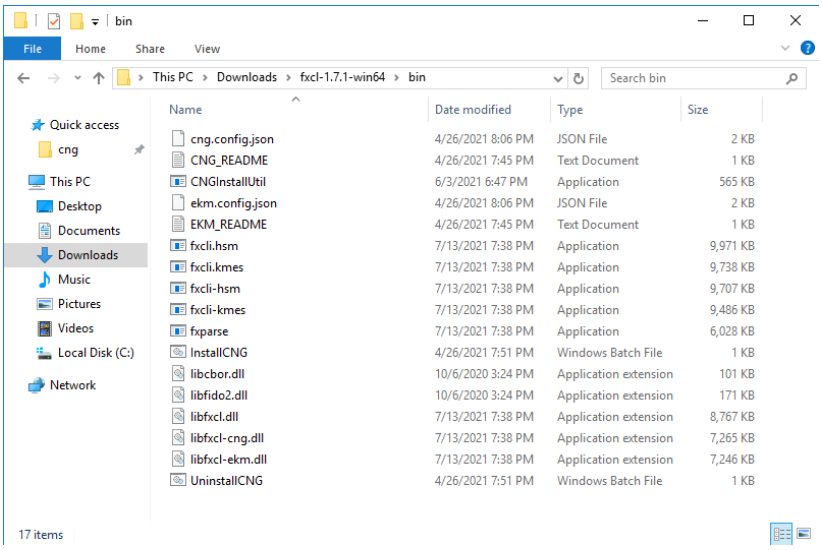
[4] INSTALL AND CONFIGURE FUTUREX CLIENT LIBRARY (FXCL) CNG

The Futurex Client Library, or FXCL, is a set of functions, offered using either Java (Java Native Interface) or C++, used by applications to access cryptographic processing and key management functionality.

[4.1] INSTALLING FXCL CNG

NOTE: To maintain system security, it is important to only install and operate copies of FXCL that are obtained directly from Futurex. These files will either be provided directly by a member of the Solutions Architect team or made available for download on the Futurex Portal or equivalent Futurex-operated file distribution platform.

1. Download or copy the `fxcl-x.x.x-win64.zip` file to the computer/server that will be running the Microsoft AD CS instance.
2. Unzip the file in any directory, then navigate into the `fxcl-x.x.x-win64\bin` folder. There you will see the following files:



3. Run the `InstallCNG.bat` file to install FXCL CNG. If the installation fails, copy all of the files in the `bin\` folder to `C:\Program Files\Futurex\fxcl\kmes\cng\` and change the `cng.config.json` file's name to `config.json`.

[4.2] CONFIGURING FXCL CNG

1. Create a `Certs\` directory in `C:\` (i.e., `C:\Certs`) and copy all of the TLS connection certificates to the `Certs\` folder.
2. Create a `Futurex\` directory in `C:\` (i.e., `C:\Futurex`). The FXCL CNG configuration file will be configured to output the FXCL CNG logs to the `Futurex\` directory.

3. Edit the `config.json` file to point to the TLS connection certificates and network-connected KMES Series 3 device. An example `config.json` file is shown below:

```
{
    // Enables output via DebugOutputString
    // (default: false)
    // Note that regardless of this setting, output is
    // placed in the debug view while loading the config.
    "enable_debug_view": false,

    // A file to place logs into. Optional.
    // If not provided, no log file is made.
    "log_file": "C:\\Futurex\\fxcl.log",

    // Level of logging to emit. Case insensitive.
    // possible values: None, Error, Info, Debug, Traffic (default: Info)
    "log_level": "traffic",

    // What kind of key storage unit is this?
    // possible values: kmes (default: kmes)
    // Not currently used, it always uses kmes.
    "driver": "kmes",

    // The host to connect to. Required.
    "host": "10.0.8.22:2001",

    // A PEM file containing a list of trusted CA certificates. Required.
    "ca": "C:\\Certs\\tls_ca.pem",

    // A P12 file containing leaf certificate and key. Required.
    "p12": "C:\\Certs\\PKI.p12",

    // Password to unlock the P12 file. Optional.
    // If not given, assumes it doesn't need a password.
    "p12_pass": "safest"
}
```

NOTE: The `tls_ca.pem` file is the Root CA certificate exported in section 3.3.4 and the `PKI.p12` file is the AD CS certificate exported as a PKCS #12 file in section 3.3.8.

[5] INSTALL ACTIVE DIRECTORY CERTIFICATE SERVICES

Install AD CS, unless you wish to set up a standalone CA. In order to install AD CS:

1. Click **Start**, **Administrative Tools**, **Server Manager**, and then **Manage**. Click **Add roles and feature**. The *Before You Begin* box will open. Click **Next**.
2. Choose the installation type: Role-based or feature-based installation. Press **Next**.
3. The *Server Selection* page will open. Select the server from the domain (or local machine) on which to install AD CS. Press **Next**.
4. On the *Server Roles* page, check the box next to **Active Directory Certificate Services**. Press **Next**. Press **Add Features**.
5. The *Features* page will open. Press **Next**.
6. The *AD CS* page will open. Press **Next**.
7. In the *Role Services* page, select **Certificate Authority**. Press **Next**.
8. On the *Confirmation* page, press **Install**.
9. Once installation is complete, press **Close**.

[6] CONFIGURE ACTIVE DIRECTORY CERTIFICATE SERVICES

A new installation of AD CS needs to be configured with a Public Key Infrastructure (PKI).

NOTE: If Active Directory is not already installed, please do so before proceeding, unless this is a standalone CA.

1. Click **Start**, **Administrative Tools**, and then **Server Manager**. Select the flag icon to the left of **Manage**.
2. Select **Configure Active Directory Certificate Services** on the destination.
3. The *Credentials* page will open. Ensure your login meets the displayed requirements. Press **Next**.
4. The *Select Role Services* page will open. Select **Certification Authority** to enable the management and issuance of certificates. Click **Next**.
5. The *Specify Setup Type* page will open. The type designates the kind of certificate authority server, and is dependent on your requirements as a business. Select either **Enterprise** or **Standalone**. Enterprise CAs are integrated with Active Directory, while standalone CAs conduct operations offline.
6. The *Specify CA Type* page will open. Click **Root** or **Subordinate**. Select **Root** if you have not yet created a PKI. Select **Subordinate** if you are integrating with an existing PKI. Click **Next**.
7. The *Set Up Private Key* page will open. Select **Use existing private key** or **Create a new private key**.
    - Select **Use existing private key** if you have integrated this CA with the Futurex hardware previously and the private key already exists on the KMES Series 3 (i.e. this is a reinstallation of the CA server). Then, choose **Select an existing private key on this computer**.
    - If this is a new CA, select **Create a new private key**.
8. If **Create a new private key** was selected:
    - The *Configure Cryptography for CA* window will open. Choose **Futurex FXCL KMES CNG** from the drop-down menu.
    - Select a **key character length**: 2048, 3072, or 4096.
    - Select a **hash algorithm** from the drop-down menu: SHA-1, SHA-256, or SHA-512. Checking **Allow administrator interaction when the private key is accessed by the CA** will have no effect.
    - Select **Next**.
9. If **Use existing private key** was selected:
    - The *Existing Key* window will open. **Change** the **Cryptographic provider** to **Futurex FXCL KMES CNG**.
    - Clear the **common name** field. Click **Search**. Locate the key you want to use from the search results.
    - Checking **Allow administrator interaction when the private key is accessed by the CA** will have no effect.
    - Select **Next**.
10. The *CA Name* page will open. Configure your PKI names. Click **Next**.
11. If **Root CA** was selected in step 6, the *Set the Certificate Validity Period* page will open. Designate the default validity for the root CA. Click **Next**.
12. If **Subordinate CA** was selected in step 6, The *Certificate Request* page will open.
    - You can choose a **parent CA** instance of AD CS on your domain to issue you a certificate.
    - You may save a **certificate request** to file and have it signed by an external CA.
13. The *Certificate Database* page will open. Click **Next**.

14. The *Confirmation* page will open. Press **Configure**.
15. To confirm that the root CA was installed successfully, enter this command in a command prompt:

```
$ certutil -csptest -csp "Futurex FXCL KMES CNG" RSA
```

A successful response to this command should contain:

```
STATE: 4  RUNNING
```

For more information on installing and configuring Active Directory Certificate Services, refer to Microsoft's documentation.

[7] VIEW CERTIFICATE STORE

The following command can be used to view the CA's certificate store. The LDAP URI will vary depending on your organization's Active Directory domain (IE: fx.futurex.com) and CA name (IE: fx-FXCA).

```
certutil -viewstore "ldap:///CN=fx-FXCA,CN=Certification Authorities,
CN=Public Key Services,CN=Services,CN=Configuration,DC=fx,
DC=futurex,DC=com?cACertificate?base?objectClass=certificationAuthority"
```

Between tests you may choose to clear the certificate store using a command similar to the following:

```
certutil -delstore "ldap:///CN=fx-FXCA,CN=Certification Authorities,
CN=Public Key Services,CN=Services,CN=Configuration,DC=fx,
DC=futurex,DC=com?cACertificate?base?objectClass=certificationAuthority" fx-FXCA
```

[8] SIGN CERTIFICATE USING THE KMES SERIES 3

The following steps will demonstrate one way to test using the KMES Series 3 to sign a certificate for the CA server.

1. Open the **Certificate Manager** on the CA server
2. Right-click on **Personal** -> **All Tasks** -> **Request New Certificate…**
3. The *Certificate Enrollment* dialog will open. Press **Next**.
4. The *Certificate Enrollment Policy* page will open. Choose a certificate enrollment service associated with the CA server, e.g. **Active Directory Enrollment Policy** for an Enterprise CA. Press **Next**.
5. The *Request Certificates* page will open. Choose a certificate template. Press **Enroll**.
6. If the KMES is connected you will receive a success message. If the KMES is offline you will receive an error.
7. To locate the certificate we just issued:
    - Open the **Active Directory Certificate Authority** tool from the Server Manager.
    - Expand the node associated with your CA common name.
    - Click **Issued Certificates**.
    - A certificate matching your request should be found on this page.

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 will help do 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 cannot be found 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

XCEPTIONAL SUPPORT

24x7x365

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

SOLUTIONS ARCHITECT

E-mail: solutions@futurex.com