



PURE STORAGE FLASHARRAY

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] OVERVIEW OF THE PURE STORAGE FLASHARRAY / KMES SERIES 3 KMIP INTEGRATION	3
[1.1] ABOUT PURE STORAGE FLASHARRAY	3
[1.2] WHAT IS KMIP?	3
[1.3] PURPOSE OF THE INTEGRATION	3
[2] PREREQUISITES	4
[3] DATA-AT-REST ENCRYPTION AND RAPID DATA LOCKING (RDL)	5
[3.1] RAPID DATA LOCKING (RDL)	5
[4] INITIAL SETUP	7
[4.1] CREATE A FLASHARRAY CERTIFICATE AND CONSTRUCT A CERTIFICATE SIGNING REQUEST (CSR)	7
[4.2] KMES SERIES 3 CONFIGURATION STEPS	8
[4.3] CONFIGURE CERTIFICATES IN THE FLASHARRAY CLI	19
[5] ENABLE RAPID DATA LOCKING (RDL)	21
[6] ONGOING RDL OPERATION	22
[6.1] GENERAL NOTES FOR KMIP CONFIGURATIONS	22
[6.2] HOW TO BLOCK ACCESS TO THE FLASHARRAY	22
APPENDIX A: XCEPTIONAL SUPPORT	23

[1] OVERVIEW OF THE PURE STORAGE FLASHARRAY / KMES SERIES 3 KMIP INTEGRATION

[1.1] ABOUT PURE STORAGE FLASHARRAY

From Pure Storage's documentation: "Pure Storage, with a continuous emphasis on simplicity, has implemented rigorous security measures including AES- 256 bit encryption, data erasure, rapid data locking technologies, key management, and a robust encrypt/decrypt process. These features meet or exceed internationally recognized security standards such as FIPS 140-2, NIAP/ Common Criteria and PCI-DSS. Coupled with comprehensive organizational security measures, FlashArray can help customers meet security requirements and data compliance regulations around the world – including the recently updated GDPR. We have achieved this without compromise in product serviceability, performance, or our industry leading data reduction capabilities."

[1.2] WHAT IS KMIP?

The Key Management Interoperability Protocol (KMIP) is an extensible communication protocol that defines message formats for the manipulation of cryptographic keys on a key management server. This facilitates data encryption by simplifying encryption key management. Keys may be created on a server and then retrieved, possibly wrapped by other keys. Both symmetric and asymmetric keys are supported, including the ability to sign certificates. KMIP also allows for clients to ask a server to encrypt or decrypt data, without needing direct access to the key.

[1.3] PURPOSE OF THE INTEGRATION

Pure Storage's Rapid Data Locking (RDL) feature makes it possible for a FlashArray device to create a secondary user-controllable key on a KMIP server (i.e., the KMES Series 3) via the KMIP protocol. The key that is created on the KMES Series 3 will subsequently be used for unlocking the array's flash modules. This makes it possible to quickly and completely lock down an array simply by revoking the remote key and powering off the FlashArray.

[2] PREREQUISITES

Supported Hardware:

- KMES Series 3, version 6.1.3.11 and above, with the *KMIP* license enabled

[3] DATA-AT-REST ENCRYPTION AND RAPID DATA LOCKING (RDL)

To understand how the **Rapid Data Locking (RDL)** feature fits in, it is helpful to know how **Data-At-Rest Encryption** works on the Pure Storage FlashArray device. For information about Data-At-Rest Encryption, please refer to the *wp-flasharray-data-security-and-compliance.pdf* document, which is contained in the Pure Storage FlashArray folder on the SharePoint.

[3.1] RAPID DATA LOCKING (RDL)

Some environments require external key management for locking down an array that is forward deployed. Pure Storage FlashArray's KMIP RDL solution makes it possible to use the KMES Series 3 for this purpose.

[3.1.1] KMIP RDL

With KMIP RDL, a secondary user-controllable key is introduced that allows for unlocking the array's flash modules. The KMIP keys are remotely accessed from a KMIP server (i.e., KMES Series 3). Without access to the server, the flash modules cannot be unlocked on power-on.

Data Encryption at Rest

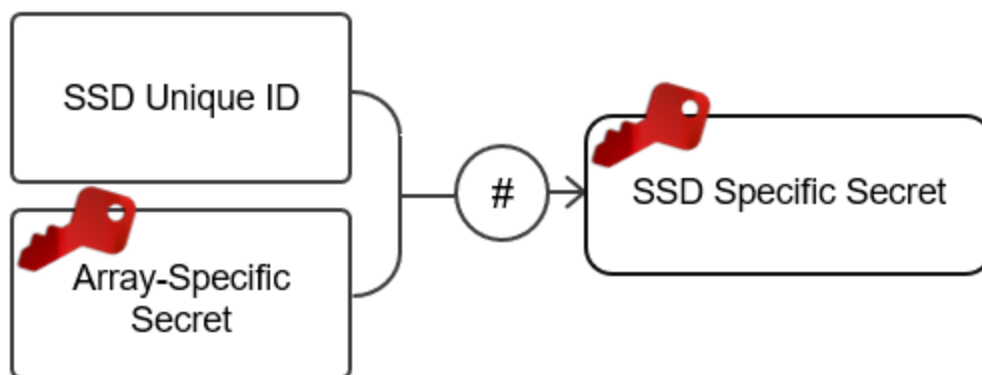


FIGURE 4. KMIP REMOTE ACCESS

Data Encryption at Rest with Rapid Data Locking enabled

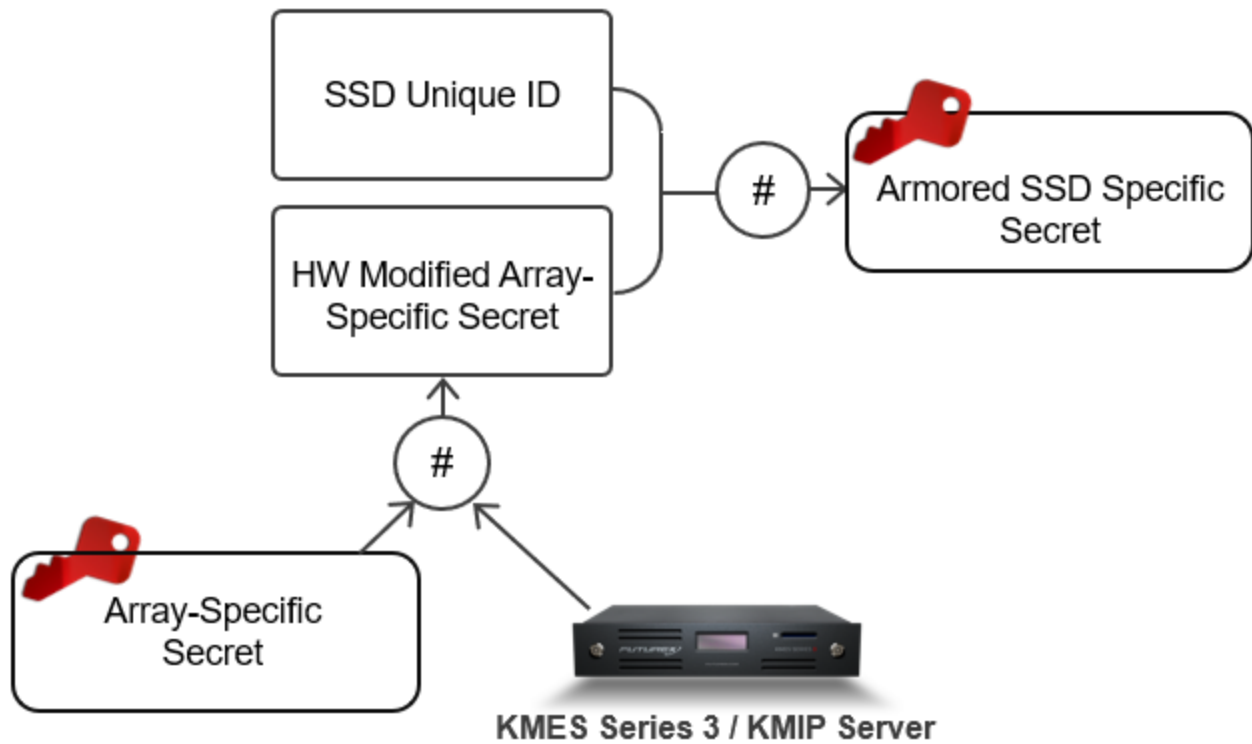


FIGURE 5. KMIP REMOTE ACCESS WITH RDL

NOTE: RDL can be enabled during installation, or at any time thereafter. Once enabled, RDL is permanent. It applies to all of an array's SSDs, including those added afterward.

[4] INITIAL SETUP

Before RDL is enabled on the FlashArray, the array and the KMES Series 3 must establish a mutual trust relationship by validating their respective digitally signed certificates.

In the subsections that follow, certificates will be generated and signed for both the FlashArray and the KMIP connection pair on the KMES Series 3. The FlashArray and the KMES Series 3 will register both certificates, and use them thereafter each time they establish a TCP/IP session secured by TLS.

Notes about certificates:

- Certificates used on the FlashArray must be PEM formatted (Base64 encoded).
- Intermediary certificates are not supported for use with KMIP.
- Using Purity's internal management certificate for KMIP configuration is not supported.

[4.1] CREATE A FLASHARRAY CERTIFICATE AND CONSTRUCT A CERTIFICATE SIGNING REQUEST (CSR)

NOTE: The steps in this subsection will be completed using the FlashArray Command Line Interface (CLI).

[4.1.1] Create a FlashArray certificate

Use the `purecert create` CLI command to create a self-signed certificate.

```
pureuser@purefa-ct0:# purecert create cert_1 --self-signed --common-name purefa
```

Display the certificate with the `purecert list` command. (Copy the displayed certificate for use in a later step.)

```
pureuser@purefa-ct0:# purecert list cert_1 --certificate
```

[4.1.2] Construct a Certificate Signing Request (CSR)

```
pureuser@purefa-ct0:# purecert construct cert_1 --certificate-signing-request
```

Copy the displayed CSR and paste it into a file editor. Save the file with either the `.pem` or `.csr` extension. Then, move the file via SFTP or other means to the external storage device configured on the KMES Series 3.

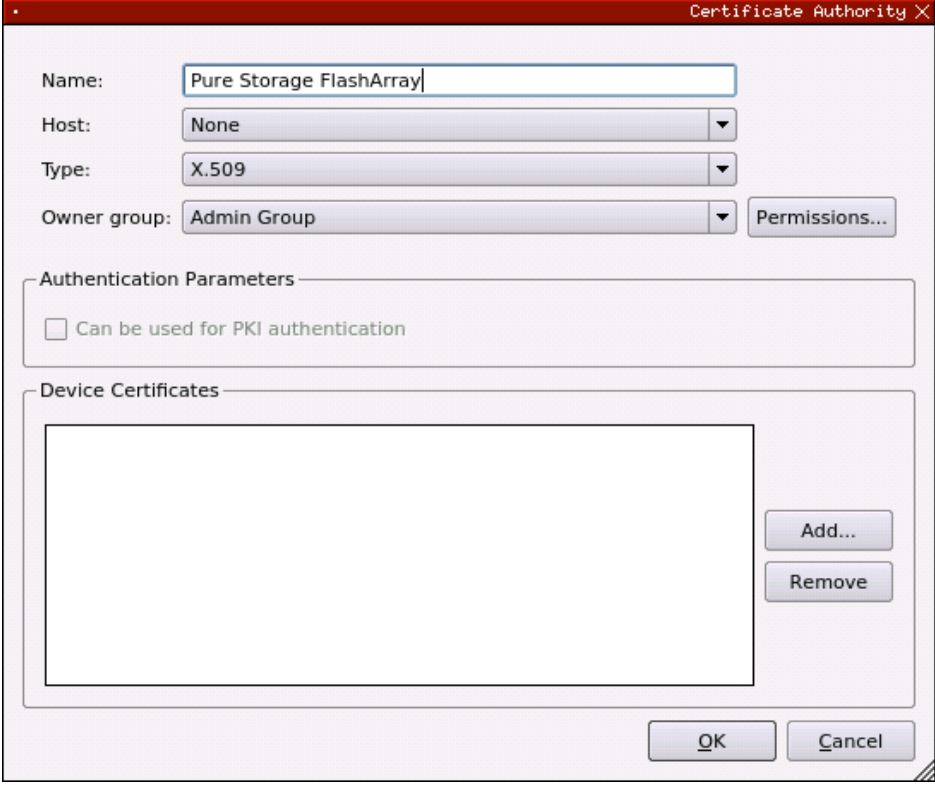
[4.2] KMES SERIES 3 CONFIGURATION STEPS

Log in to the KMES Series 3 application interface with the default Admin users.

[4.2.1] Create a new Certificate Authority (CA)

Navigate to the *Certificate Authorities* menu, then click the **Add CA...** button.

Specify a name for the CA, then click **OK**.

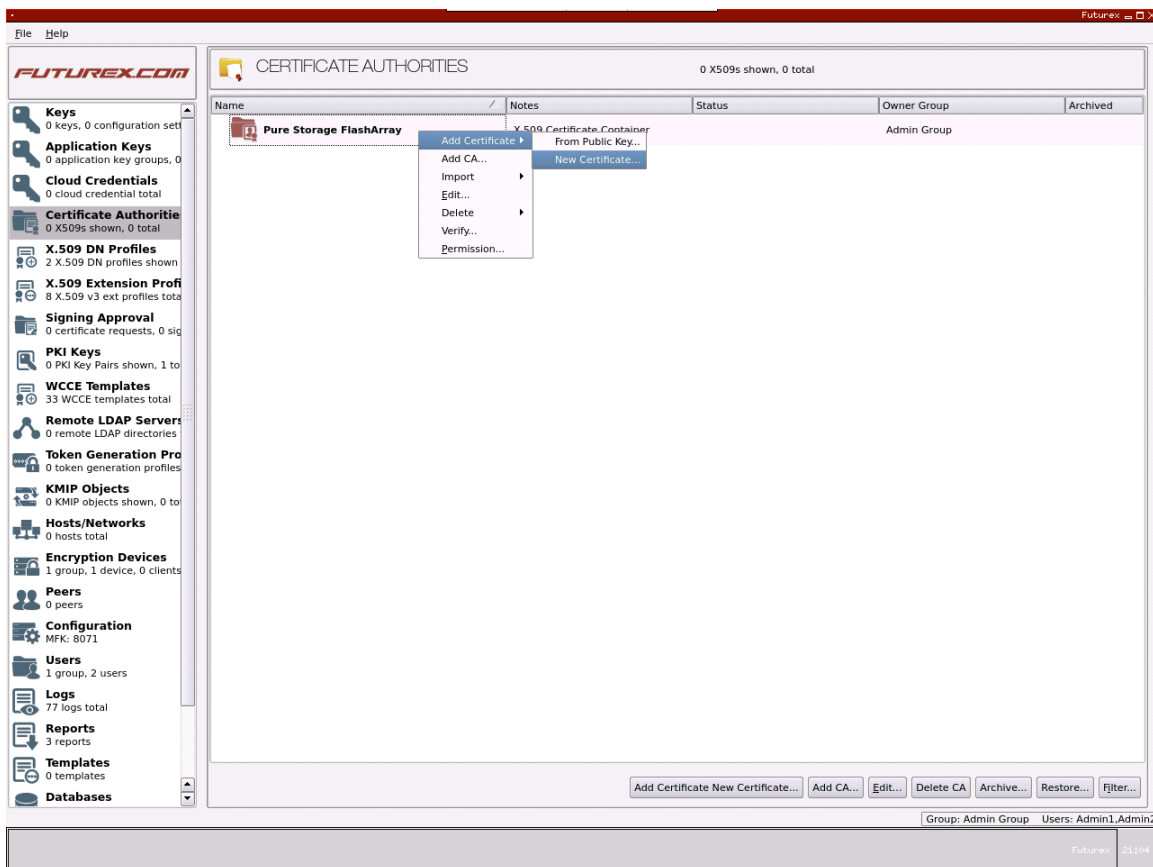


The screenshot shows a "Certificate Authority" dialog box with the following fields and options:

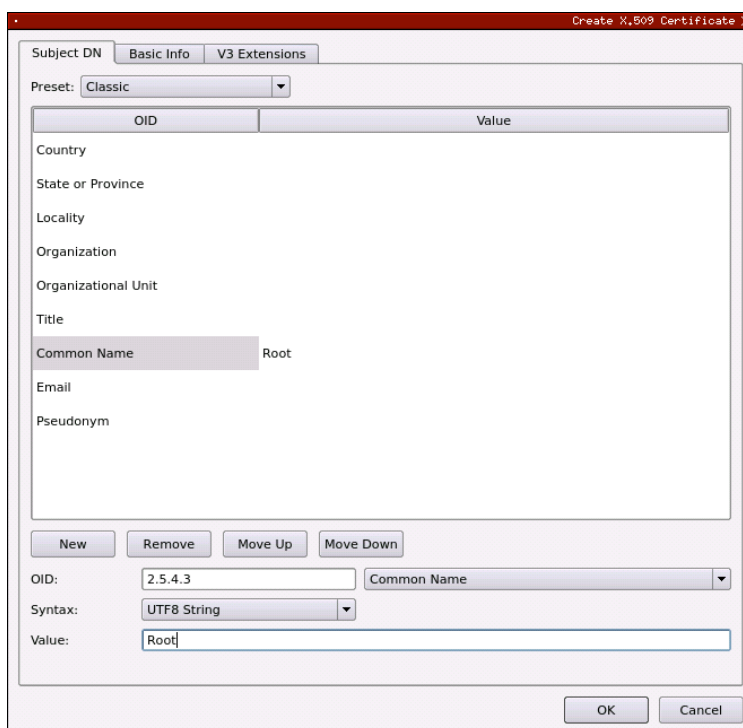
- Name:** A text box containing "Pure Storage FlashArray".
- Host:** A dropdown menu set to "None".
- Type:** A dropdown menu set to "X.509".
- Owner group:** A dropdown menu set to "Admin Group".
- Permissions...** button.
- Authentication Parameters:** A section containing a checkbox labeled "Can be used for PKI authentication", which is currently unchecked.
- Device Certificates:** A large empty rectangular box for listing certificates.
- Add...** and **Remove** buttons next to the Device Certificates box.
- OK** and **Cancel** buttons at the bottom right.

Right-click on the newly created "Pure Storage FlashArray" CA and select **Edit**. In the Certificate Authority dialog, check the box that says, "Can be used for PKI authentication", then click **OK** to save.

Right-click again on the "Pure Storage FlashArray" CA, then select **Add Certificate -> New Certificate....**



Change the **Preset** dropdown to "Classic", then set the **Common Name** value to "Root".



In the *Basic Info* tab, change the **Major key** to the "PMK". All other settings can be left as the default values.

In the *V3 Extensions* tab, set the **Profile** to "Example Certificate Authority", then click **OK** to save.

[4.2.2] Sign the FlashArray CSR

Right-click on the Root CA certificate, then select **Add Certificate** -> **From Request....**

In the file browser, find and select the FlashArray CSR. The certificate information should populate in the window.

Subject DN Basic Info V3 Extensions CSR Upload

Preset: None

OID	Value
Organizational Unit	Pure Storage, Inc.
Common Name	purefa
Organization	Pure Storage, Inc.

New Remove Move Up Move Down

OID: 2.5.4.11 Organizational Unit

Syntax: UTF8 String

Value: Pure Storage, Inc.

OK Cancel

Leave all of the settings as-is and click **OK** (Note that the **Common Name** of the certificate is "purefa").

The signed FlashArray certificate should now be listed under the Root certificate.

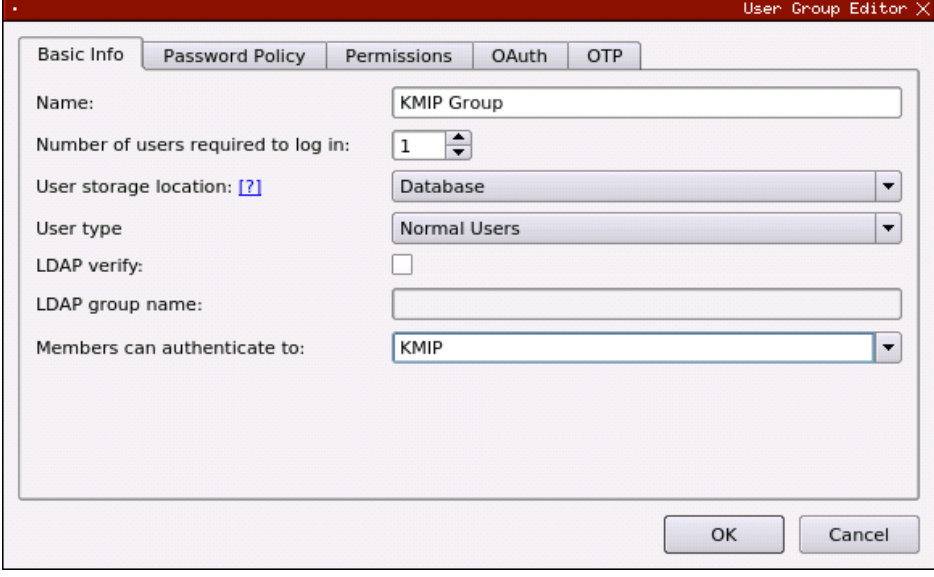
CERTIFICATE AUTHORITIES			
		2 X509s shown, 2 total	
Name	Notes	Status	Owner Group
- Pure Storage FlashArray - Root - purefa	- X.509 Certificate Container - Self-signed - No Private Key	- Valid - Valid	- Admin Group - Admin Group - Admin Group

[4.2.3] Create a new user for FlashArray

In this step we'll create a new user on the KMES Series 3. The name of this user needs to match what is set as the "Common Name" for the signed FlashArray certificate. This is how the KMES Series 3 authenticates the FlashArray device that is connecting via KMIP.

Navigate to the *Users* menu, then click the **Add Group...** button.

In the *Basic Info* tab, set the fields to how they are shown below (**NOTE:** The name of the group can be anything.)



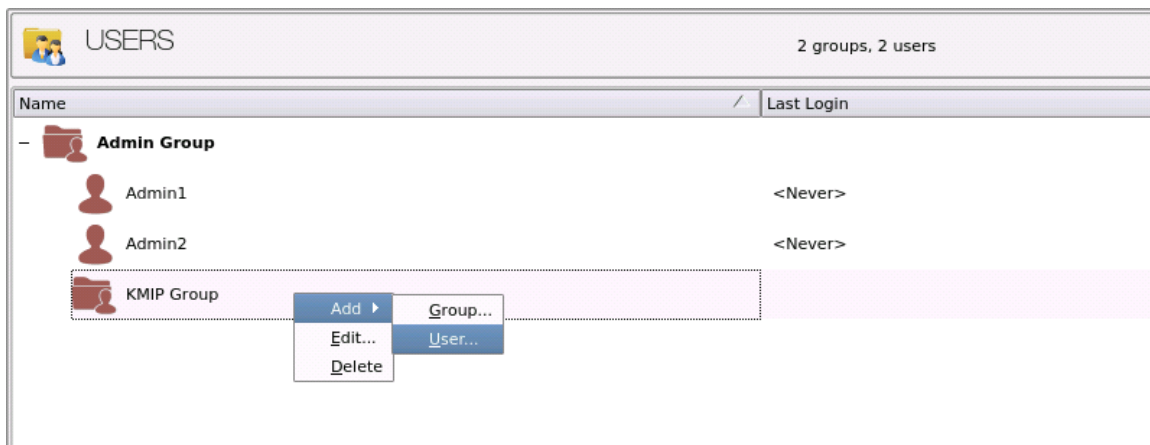
The image shows the 'User Group Editor' dialog box with the 'Basic Info' tab selected. The fields are as follows:

Field	Value
Name:	KMIP Group
Number of users required to log in:	1
User storage location:	Database
User type:	Normal Users
LDAP verify:	☐
LDAP group name:	
Members can authenticate to:	KMIP

Buttons: OK, Cancel

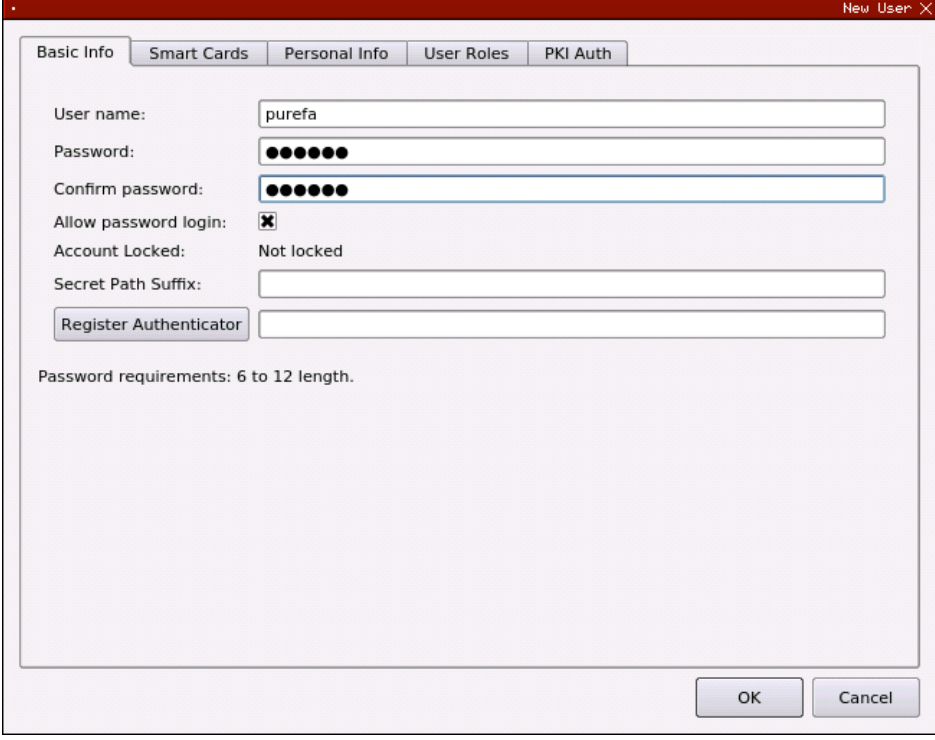
Go straight to the *Permissions* tab and enable all permissions for the group.

Click **OK** to save.



Right-click on the newly created User Group, then select **Add -> User...**

Set "purefa" as the user name (to match the Common Name of the FlashArray certificate), then set a password.

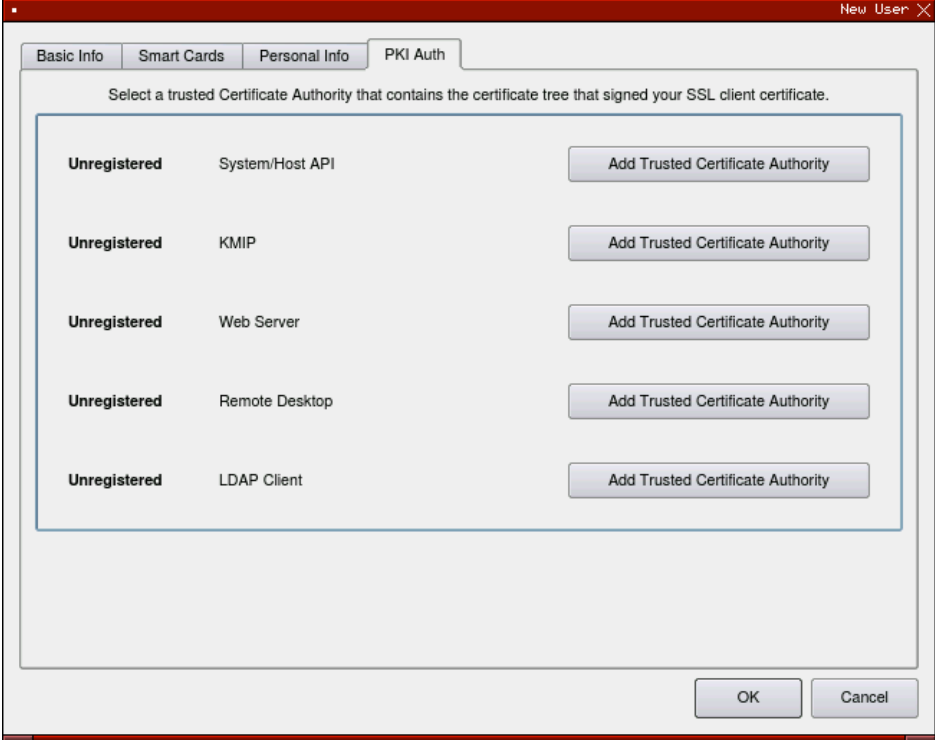


The screenshot shows the 'New User' dialog box with the 'Basic Info' tab selected. The 'User name' field contains 'purefa'. The 'Password' and 'Confirm password' fields are masked with dots. The 'Allow password login' checkbox is checked. The 'Account Locked' status is 'Not locked'. The 'Secret Path Suffix' field is empty. There is a 'Register Authenticator' button and an empty field next to it. At the bottom, there are 'OK' and 'Cancel' buttons. A note at the bottom states: 'Password requirements: 6 to 12 length.'

User name:	purefa
Password:	••••••
Confirm password:	••••••
Allow password login:	☒
Account Locked:	Not locked
Secret Path Suffix:	
Register Authenticator	

Password requirements: 6 to 12 length.

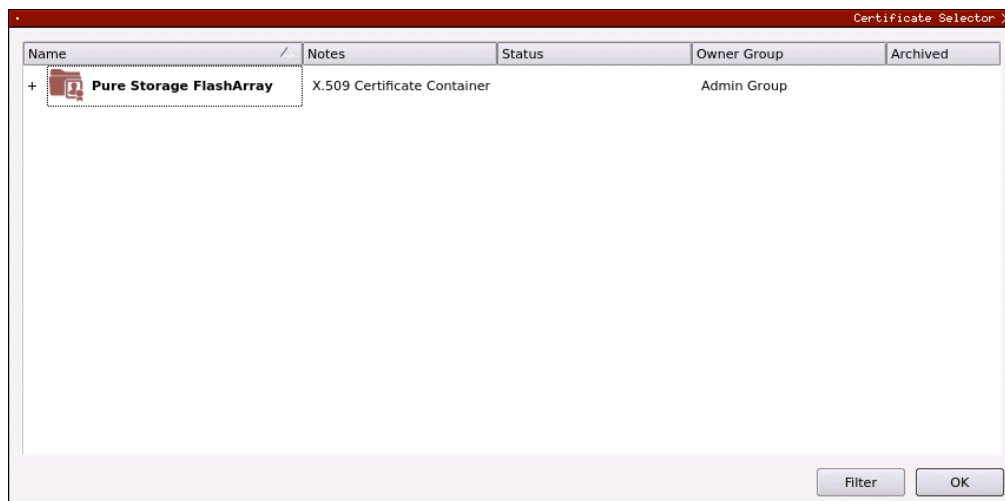
Navigate to the *PKI Auth* tab, then click the **Add Trusted Certificate Authority** button next to KMIP.



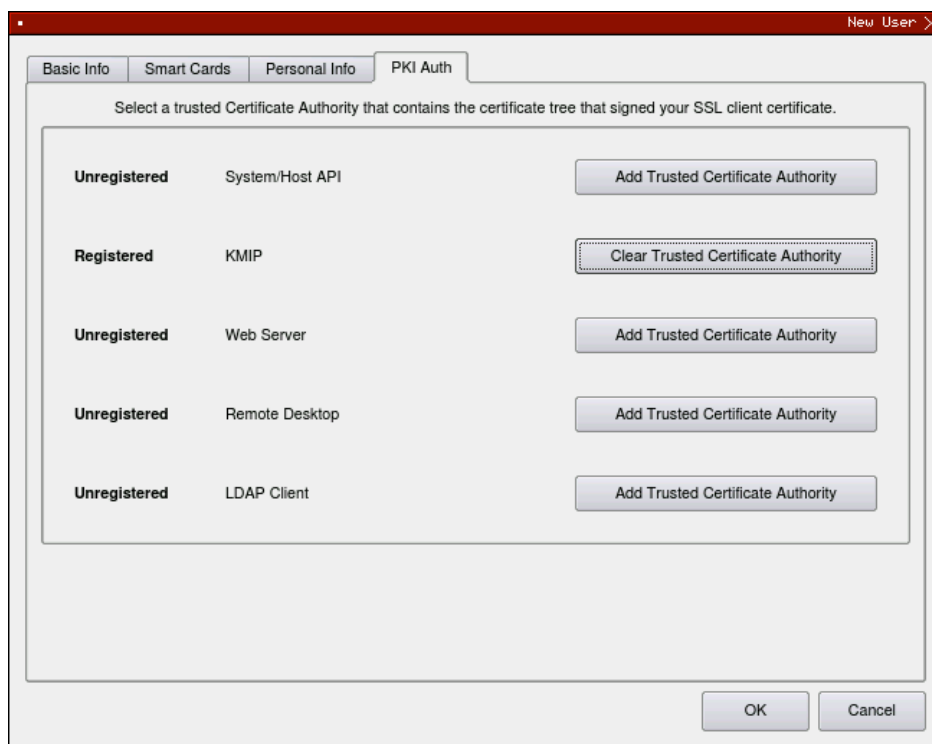
The screenshot shows the 'New User' dialog box with the 'PKI Auth' tab selected. The instruction reads: 'Select a trusted Certificate Authority that contains the certificate tree that signed your SSL client certificate.' Below this, there is a table with five rows, each representing a different system and having an 'Add Trusted Certificate Authority' button next to it. The 'KMIP' row is highlighted with a blue border. At the bottom, there are 'OK' and 'Cancel' buttons.

Status	System/Host API	Action
Unregistered	System/Host API	Add Trusted Certificate Authority
Unregistered	KMIP	Add Trusted Certificate Authority
Unregistered	Web Server	Add Trusted Certificate Authority
Unregistered	Remote Desktop	Add Trusted Certificate Authority
Unregistered	LDAP Client	Add Trusted Certificate Authority

Select the Pure Storage FlashArray CA, then click **OK**.



It should show "Registered" next to KMIP now. Click **OK** to save.



[4.2.4] Configure TLS certificate for the KMIP server connection pair

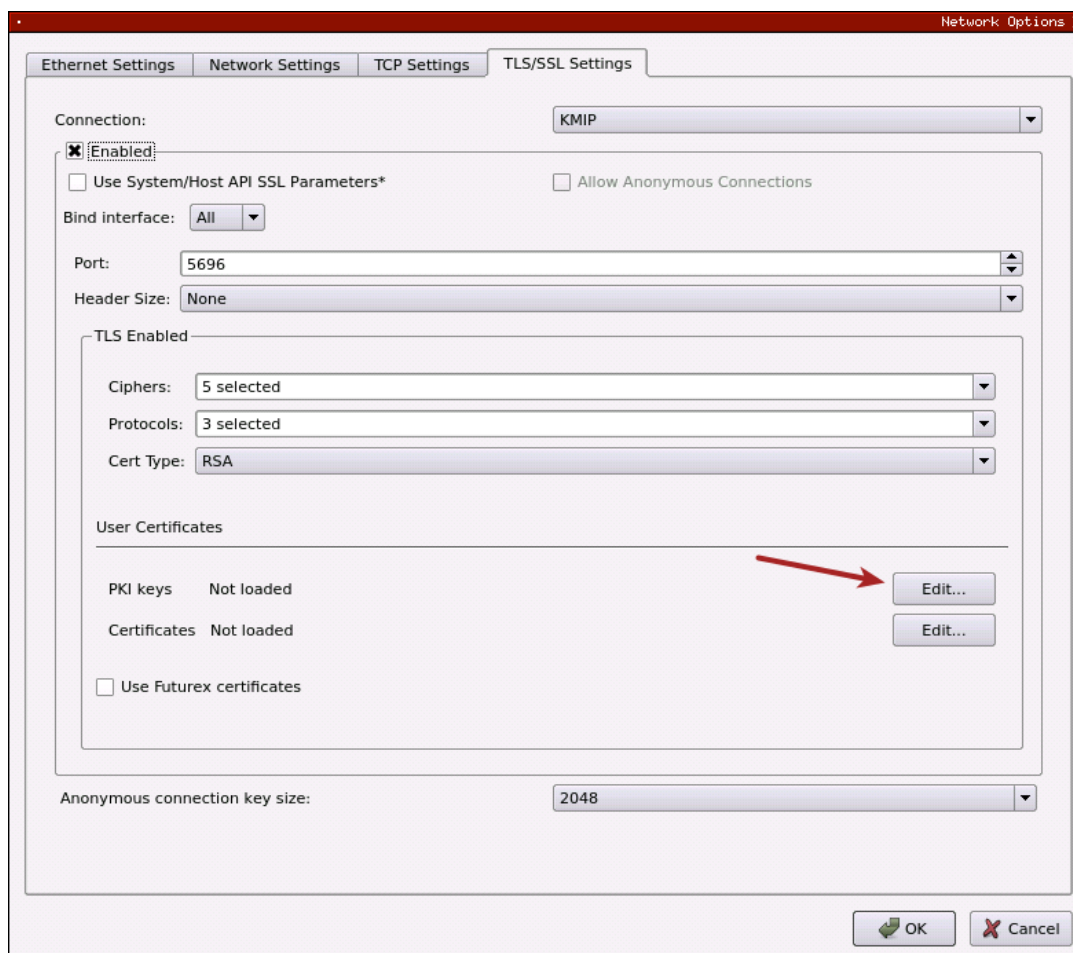
[4.2.4.1] Generate a new PKI key pair and CSR for the KMIP connection pair

Navigate to the *Configuration* menu, then double-click on *Network Options*. Under the *TLS/SSL Settings* tab, click the **Connection** dropdown and select the **KMIP** connection pair.

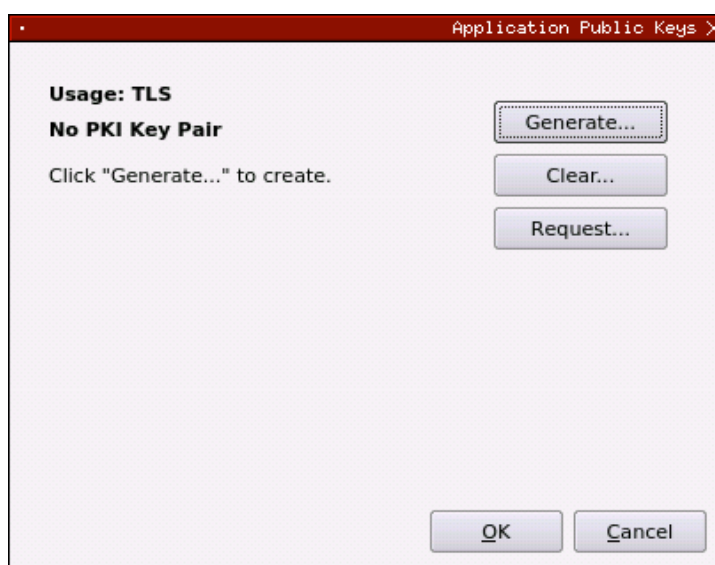
Enable the KMIP connection pair if it is not already enabled.

Uncheck **Use System/Host API SSL Parameters** if it is selected.

In the User Certificates section, click the **Edit...** button next to PKI keys.

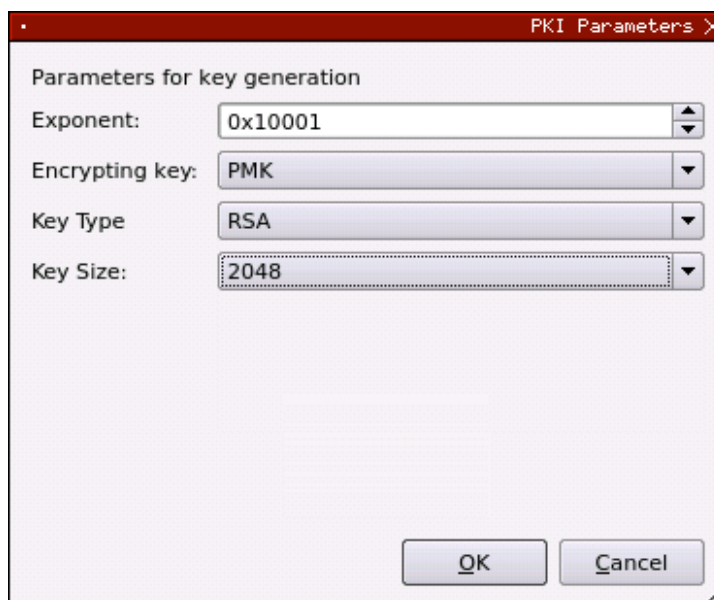


Click the **Generate...** button to create a new PKI Key Pair.



Click **Yes** and bypass the warning about SSL not being functional until new certificates are imported.

This will open the *PKI Parameters* dialog. Set the **PMK** as the Encrypting key, then change the Key Size to **2048**. Click **OK**.



The *Application Public Keys* dialog should now show that the PKI Key Pair is **Loaded**. If this is the case, click **Request....**



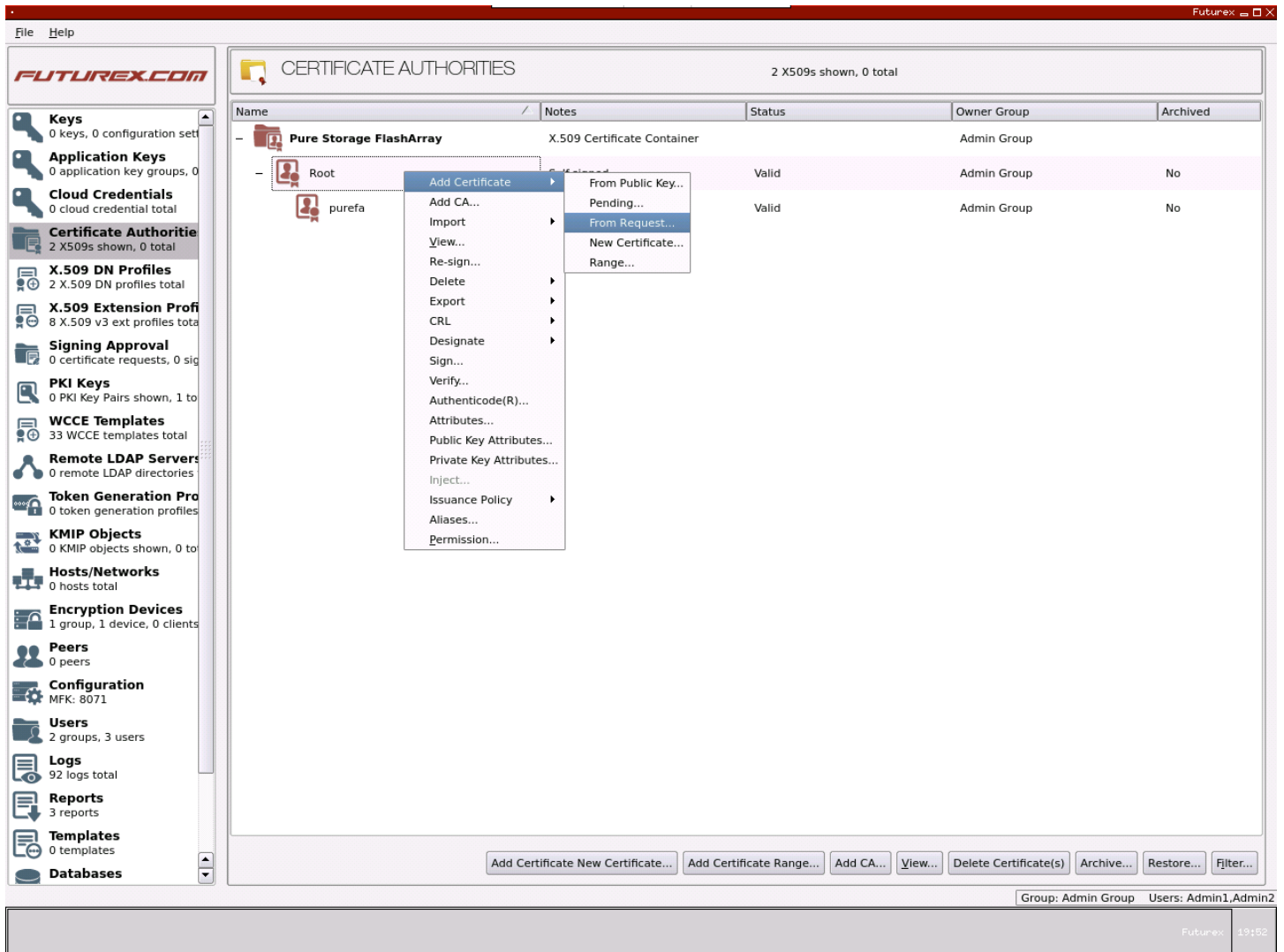
The values in the *Subject DN* tab can be left as default. In the *V3 Extensions* tab, set the profile to **Example TLS Server Certificate**. In the *PKCS #10 Info* tab, specify a save location and name for the CSR file, then click **OK**.

A message box should appear saying that the certificate signing request was successfully written to the specified location. Click **OK** in this box.

Click **OK** in the *Application Public Keys* dialog, then click **OK** once more in the main *Network Options* dialog.

[4.2.4.2] Sign the KMIP connection pair CSR

Navigate to the *Certificate Authorities* menu. Right-click on the Root CA certificate under the Pure Storage FlashArray CA, then select **Add Certificate -> From Request...**



In the file browser, find and select the KMIP connection pair CSR. Certificate information should populate in the *Create X.509 From CSR* window.

Leave all settings exactly as they are and click **OK** to save.

The signed KMIP server certificate should be under the Root CA certificate in the Pure Storage FlashArray CA tree now.

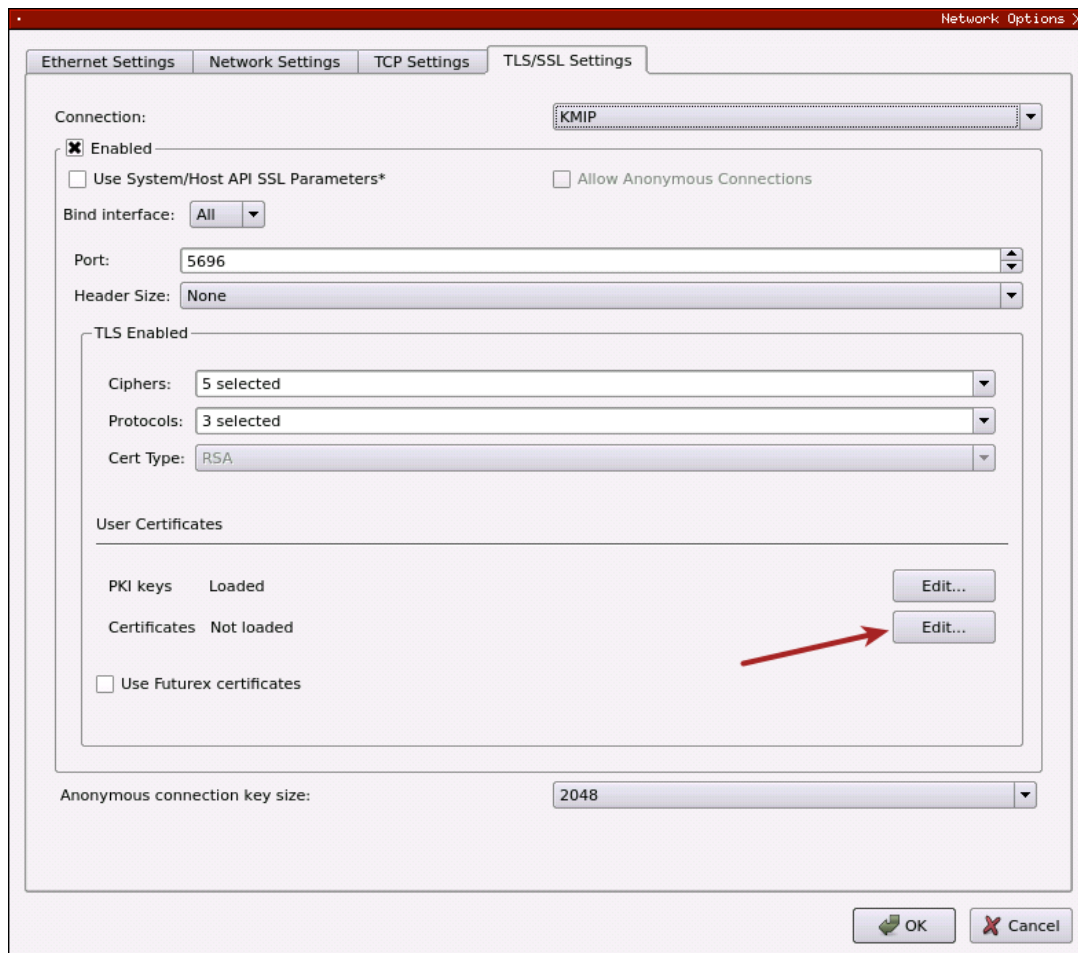
[4.2.4.3] Export all of the certificates in the Pure Storage FlashArray certificate tree

For each of the certificates in the Pure Storage FlashArray certificate tree, right-click on them and select **Export - > Certificate(s)...** In the *Export Certificate* dialog for each of them, change the encoding to **PEM**, then specify a save location for the file.

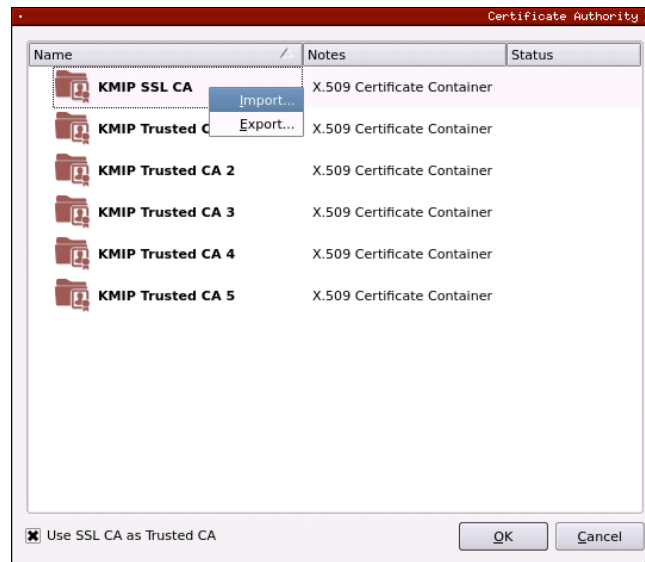
[4.2.4.4] Import the signed KMIP connection pair certificate

Navigate to the *Configuration* menu, then double-click on *Network Options*. Under the *TLS/SSL Settings* tab, click the **Connection** dropdown and select the **KMIP** connection pair.

In the User Certificates section, click the **Edit...** button next to Certificates.

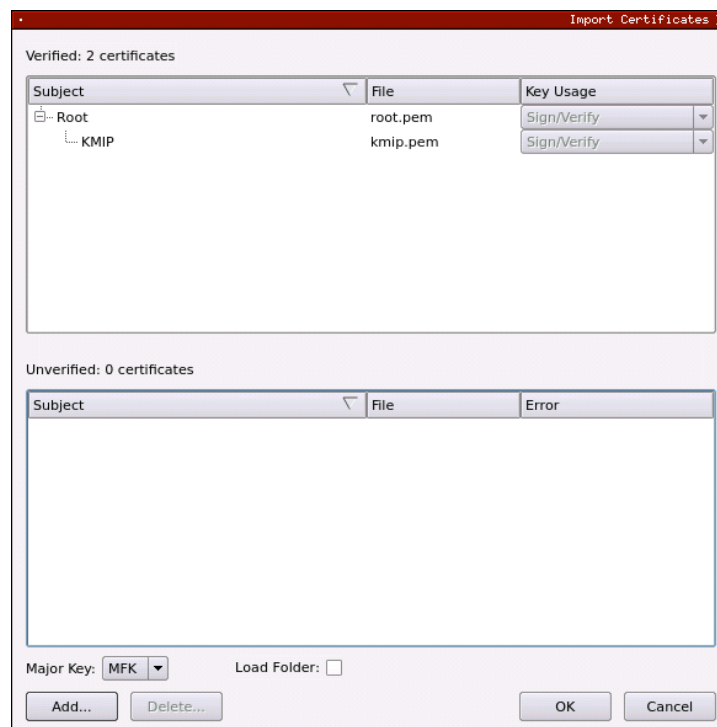


In the *Certificate Authority* dialog, right-click on the **KMIP SSL CA** X.509 Certificate Container, then select **Import....**



In the *Import Certificates* dialog, click the **Add...** button at the bottom of the window. In the file browser, select both the root CA certificate and the signed KMIP server certificate and click **Open**.

The certificates should now be listed in the "Verified" section of the *Import Certificates* dialog.



Click **OK** to save.

It should now say **Signed loaded** next to "Certificates" in the User Certificates section of the *Network Options* dialog. Click **OK** to save.

[4.3] CONFIGURE CERTIFICATES IN THE FLASHARRAY CLI

NOTE: In the previous section, all of the **Pure Storage FlashArray** CA tree certificates were exported to the storage medium (USB Device or FTP Server) that is configured on the KMES Series 3. It will be necessary to copy these files' contents to your computer's clipboard for use in the FlashArray CLI commands that follow.

[4.3.1] Define the KMIP Server and Import the KMIP Server's CA certificate

The `purekmp create` command allows for the creating of a KMIP Server and provides a way for importing the CA certificate for the KMIP server (i.e., the root CA certificate in the Pure Storage FlashArray certificate tree). After executing the command, you are prompted to paste in the KMIP server's CA certificate. Be sure to copy the entire certificate including “-----BEGIN” and “-----END” lines.

NOTE: In the "uri" field, the IP or hostname of the KMES Series 3 and the KMIP port number needs to be specified.

```
pureuser@purefa-ct0:~# purekmp create kmp_srvr --uri 10.0.5.127:5696 --certificate
cert_1 --ca-certificate

Please enter CA certificate followed by Enter and then Ctrl-D:
-----BEGIN CERTIFICATE-----
MIIDEjCCAfoCCQD5SRlGfudwrzANBgkqhkiG9w0BAQsFADBLMRswGQYDVQQQLDBJQ
---pasted lines omitted---
8mMBeuA8IYYihHIqd6nj03k0aESMtA==
-----END CERTIFICATE-----
```

If the command is successful, there will be output showing the name and URI of the KMIP Server, the name of the FlashArray certificate associated with it, and a boolean of True or False for whether the CA certificate is configured.

[4.3.2] Import the signed FlashArray certificate

The `purecert setattr` command will be used to import the signed FlashArray certificate. After executing the command, you are prompted to paste in the signed FlashArray certificate. Be sure to copy the entire certificate including “-----BEGIN” and “-----END” lines.

```
pureuser@purefa-ct0:~# purecert setattr --certificate cert_1

Please enter certificate followed by Enter and then Ctrl-D:
-----BEGIN CERTIFICATE-----
MIIDPDCCAisSgAwIBAgIIANgThwAAAIcwDQYJKoZIhvcNAQELBQAwDzENMAsGA1UE
---pasted lines omitted---
sQPNMlbdTlC7DN4yP0PK7g==
-----END CERTIFICATE-----
```

If the command is successful, the output will list the certificate's name, and the "Status" field will show imported.

[4.3.3] Test connection and authentication to the KMIP Server on the FlashArray

The `purekmip test` command will be used to verify that the specified credentials successfully contact and authenticate with the KMIP port on the KMES Series 3.

```
pureuser@purefa-ct0:~# purekmip test kmip_srvr
```

If the command is successful, the output will list the name of the KMIP server, and the "Status" field will show **OK**.

IMPORTANT: Be sure to run the `purekmip test` step to test the server-array communication path before enabling RDL.

[5] ENABLE RAPID DATA LOCKING (RDL)

CAUTION: Once RDL has been enabled, disabling it will obliterate all data stored in the array.

[5.0.1] Enable RDL using KMIP

The `purearray enable security-token` command will be used to enable RDL using the KMIP server.

```
pureuser@purefa-ct0:~# purearray enable security-token --kmip kmip_srvr
```

The new security-token can be listed with the following command:

```
pureuser@purefa-ct0:~# purearray list --security-token
```

[5.0.2] Test the security-token

The `purearray test security-token` command will be used to test the security-token with RDL enabled.

NOTE: Allow up to 30 minutes for the `purearray test` command to accurately reflect the configuration.

```
pureuser@purefa-ct0:~# purearray test security-token
```

The "Status" column reports success or failure:

- **OK:** A TLS connection could be established with the KMIP server and a basic KMIP Locate request is successful.
- **Fail:** Failure can be due to two main categories of error:
 - `Cannot connect and authenticate with the server`
For example, the KMIP server URI is not reachable, or the certificate is not in the correct format, not a complete certificate, or not a certificate file.
 - `Server is not ready for KMIP operations`
For example, the certificate cannot be authenticated by the KMIP server, or the KMIP server cannot successfully respond to the Locate request.

[6] ONGOING RDL OPERATION

[6.1] GENERAL NOTES FOR KMIP CONFIGURATIONS

- A certificate can only be deleted when it is no longer in use with a KMIP server. Being in use must be determined through the KMIP server (i.e., KMES Series 3). The `purecert` command does not include information on whether a certificate is in use.
- Currently, it is not supported to rename a KMIP server or a certificate used with a KMIP server.

[6.2] HOW TO BLOCK ACCESS TO THE FLASHARRAY

If you should require to block access to FlashArray data immediately, take one of the following steps and then either **power down the FlashArray** or **restart Purity**:

- On the KMIP server (i.e., KMES Series 3), revoke the TLS certificate used for communication with the FlashArray. It is possible to recover later by redoing the certificate setup steps.
- On the KMIP server (i.e., KMES Series 3), delete the secret key used for communication with the FlashArray. FlashArray data is not recoverable after this step. **Use only to make the array's data permanently inaccessible.**

IMPORTANT: These steps do not block data availability until Purity is restarted (or the array is powered off).

NOTE: All data on the FlashArray may become inaccessible if any of the following happen after RDL is enabled on the array. An alert is seen, but data remains accessible until the next Purity restart or failover.

- The KMIP server is removed or is not accessible.
- The certificate used with the KMIP server expires.

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