# Pure Storage FlashArray

6.8.5

# Integration Guide

# ESKM

8.54.0

utimaco®

## Imprint


| | |
|---|---|
| Copyright 2025 | Utimaco IS GmbH |
| | Germanusstr. 4 |
| | D-52080 Aachen |
| | Germany |
| Phone | AMERICAS +1-844-UTIMACO (+1 844-884-6226) |
| | EMEA +49 800-627-3081 |
| | APAC +81 800-919-1301 |
| Internet | https://support.hsm.utimaco.com/ |
| e-mail | support@utimaco.com |
| Document Version | 1.0.0 |
| Date | 2025-09-26 |
| Status | PUBLISHED |
| Document No. | IG-2025-0056 |

# Table of Contents

# 1 Introduction

## 1.1 About This Guide

This guide provides step-by-step instructions for integrating the ESKM with Pure Storage FlashArray to enable external key management, configure secure communication, and validate encryption key operations.

## 1.2 Target Audience

This guide is intended for Pure Storage FlashArray and Utimaco ESKM administrators.

## 1.3 Purpose of the Integration

This integration allows Pure Storage FlashArray to leverage Utimaco ESKM as an external KMIP-compliant key manager, enabling the secure generation, storage, and management of encryption keys used by the array.

## 1.4 Abbreviations

| Abbreviation | Meaning |
|---|---|
| ESKM | Enterprise Security Key Manager |
| KMIP | Key Management Interoperability Protocol |
| KMS | Key Management Service |
| CSR | Certificate Signing Request |
| CLI | Command Line Interface |
| CA | Certificate Authority |

| Abbreviation | Meaning |
|---|---|
| FA | Flash Array |
| URI | Uniform Resource Identifier |
| RDL | Rapid Data Locking |
| FIPS | Federal Information Processing Standards |

Table 1: Abbreviations

## 1.5 Document Conventions

The following conventions are used in this guide:

| Convention | Use | Example |
|---|---|---|
| **Bold** | Items of the Graphical User Interface (GUI), e.g., menu options | Press **OK** |
| `Monospaced` | Code that is given for explanation or as an example, file paths | `chsm-create` |
| *Italic* | References and important terms | See *Sample Chapter* in the *CryptoServer - Sample Manual* |

Table 2: Document Conventions

We use special icons to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message marks the result expected after the successful execution of an instruction.

# 2 Product Overview

## 2.1 Overview of Pure Storage FlashArray

Pure Storage FlashArray is an enterprise-class, all-flash storage platform with high performance, low latency, and consistent availability for business-critical workloads. It provides block storage services with built-in data reduction, snapshots, replication, and encryption. FlashArray is commonly deployed in data centers to support virtual machines, databases, containers, and cloud-native applications.

It also offers native encryption-at-rest. When integrated with an external key manager such as Utimaco ESKM via the KMIP protocol, FlashArray can securely manage encryption keys outside the array for enhanced security and centralized key lifecycle management.

## 2.2 Overview of ESKM

ESKM is a centralized key management solution that securely stores, distributes, and manages encryption keys throughout their lifecycle. It supports industry standards, including the KMIP, enabling integration with various enterprise applications and storage systems.

In the Pure Storage FlashArray integration, ESKM functions as the external key management server, allowing the FlashArray to obtain and validate encryption keys used for data-at-rest encryption securely.

## 2.3 Joint Value Proposition

Integrating Pure Storage FlashArray with ESKM delivers a unified solution combining enterprise-grade storage performance with robust, standards-based key management. FlashArray provides always-on data-at-rest encryption with no impact on performance, while ESKM centrally manages and secures the encryption keys throughout their lifecycle.

Together, they enable organizations to:

- Simplify compliance with industry and regulatory requirements through centralized key management.
- Enhance data security by separating key ownership from data storage.
- Maintain operational efficiency with seamless, transparent encryption that requires minimal administrative effort.

- Ensure flexibility and interoperability through support of KMIP standards.

This joint solution offers a secure, scalable, and efficient way to protect sensitive data while reducing complexity in enterprise environments.

# 3 Integration Requirements and Prerequisites

## 3.1 Tested Versions

| Operating System | Pure Storage FlashArray version | Utimaco ESKM Version |
|---|---|---|
| Purity//FA | 6.8.5 | 8.54.0 |

Table 3: Tested Versions

## 3.2 Supported Platforms

- Utimaco ESKM hardware appliance.
- Utimaco ESKM virtual/cloud appliance.

## 3.3 Hardware and Software Requirements

| Software | Software Requirements |
|---|---|
| Utimaco ESKM | 8.54.0 |
| Purity//FA | 6.8.5 |

Table 4: Hardware and Software Requirements

## 3.4 Prerequisites

1. Utimaco ESKM version 8.54.0 or later.
2. Admin access to Pure Storage FlashArray.
3. Admin access to Utimaco ESKM.

# 4 Installation and Configuration

The following section outlines the procedures required to configure ESKM.

## 4.1 Setting Up ESKM

The initial phase involves configuring ESKM before proceeding to PureStorage FlashArray.
For detailed configuration steps, refer to the *"ESKM_Installation and Replacement_Guide_8.54.0"*.

After successful installation and configuration, log in to ESKM.

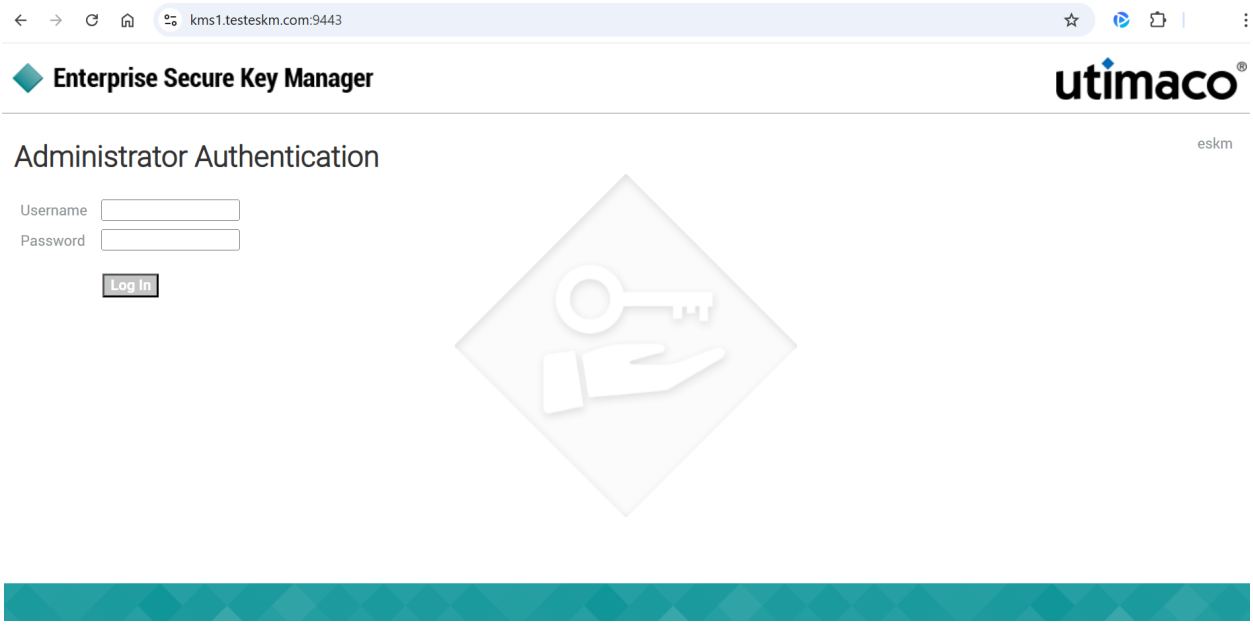



Figure 1 : ESKM Login Page

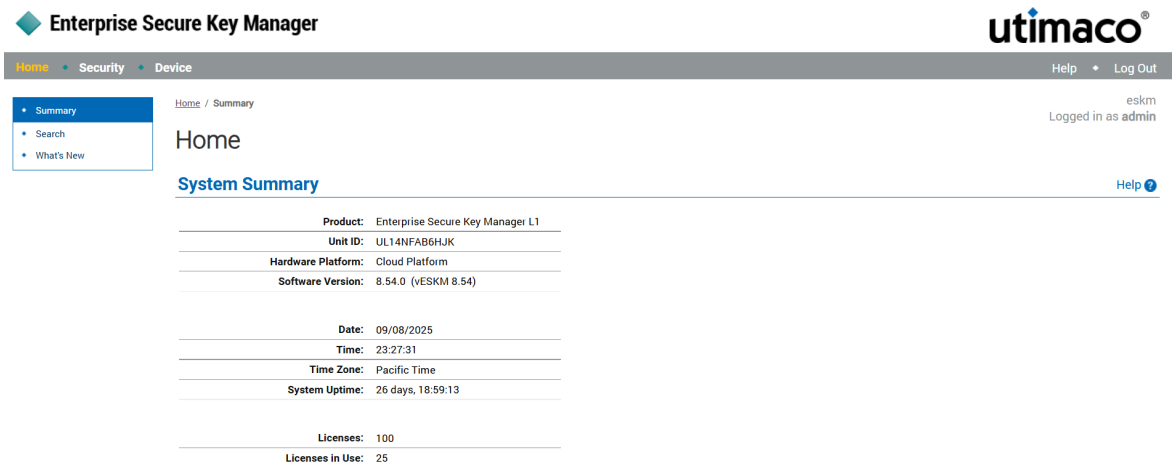



Figure 2 : ESKM Home Page

## 4.2 Setting Up Pure Storage FlashArray

Verify that you have administrative access to the Pure Storage FlashArray through the FlashArray CLI, which is required to configure security settings and perform integration steps.

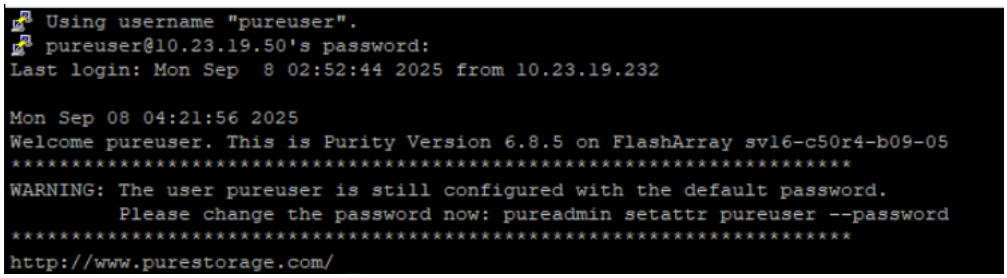



Figure 3 : Pure Storage FlashArray CLI

# 5 Integration Steps

## 5.1 Configuration on Utimaco ESKM

It is essential to configure Utimaco ESKM to ensure secure and efficient key management. This section guides you through the necessary steps to configure ESKM for Pure Storage FlashArray integration.

### 5.1.1 Create a Local CA

The local CA signs and verifies the server certificate and may also sign client certificate requests. Follow these steps to create and install a local CA.

1. Go to the **Security** tab.
2. Click on the **Certificates** option listed under **Certificates & CAs**.
3. Scroll down to the **Create Certificate** section.
4. Enter a **Certificate Authority Name** and a **Common Name**. These may have the same value, such as ESKMLocalCA.
5. Enter your **Organizational information**.
6. Select the **Algorithm** (for example, RSA-2048).
7. Select **Self-signed Root CA** and enter the **CA Certification Duration** and **Maximum User Certificate Duration**. These values determine when the certificate must be renewed and should be set in accordance with your company's security policies. The default value for both is 3650 days or 10 years.
8. Click on **Create**.


Figure 4 : Create Local CA

### 5.1.2 Create a Server Certificate

You must create an ESKM certificate to enable secure communication between Pure Storage FlashArray and the ESKM.

To create an ESKM server certificate, perform the following steps:

1. In the **ESKM Management** console, go to **Security** > **Certificates and CAs** and click **Certificates**.
2. Enter **Certificate Name**, **Country Name**, **State or Province Name**, **Locality Name**, **Organization Name,** and **Organizational Unit Name**.
3. Select **RSA-2408** from the **Algorithm** dropdown list.
4. Select the previously created CA certificate name from the **Local CA** dropdown list.
5. Select **Server** from the **Certificate Purpose** dropdown list.
6. Click **Create**.

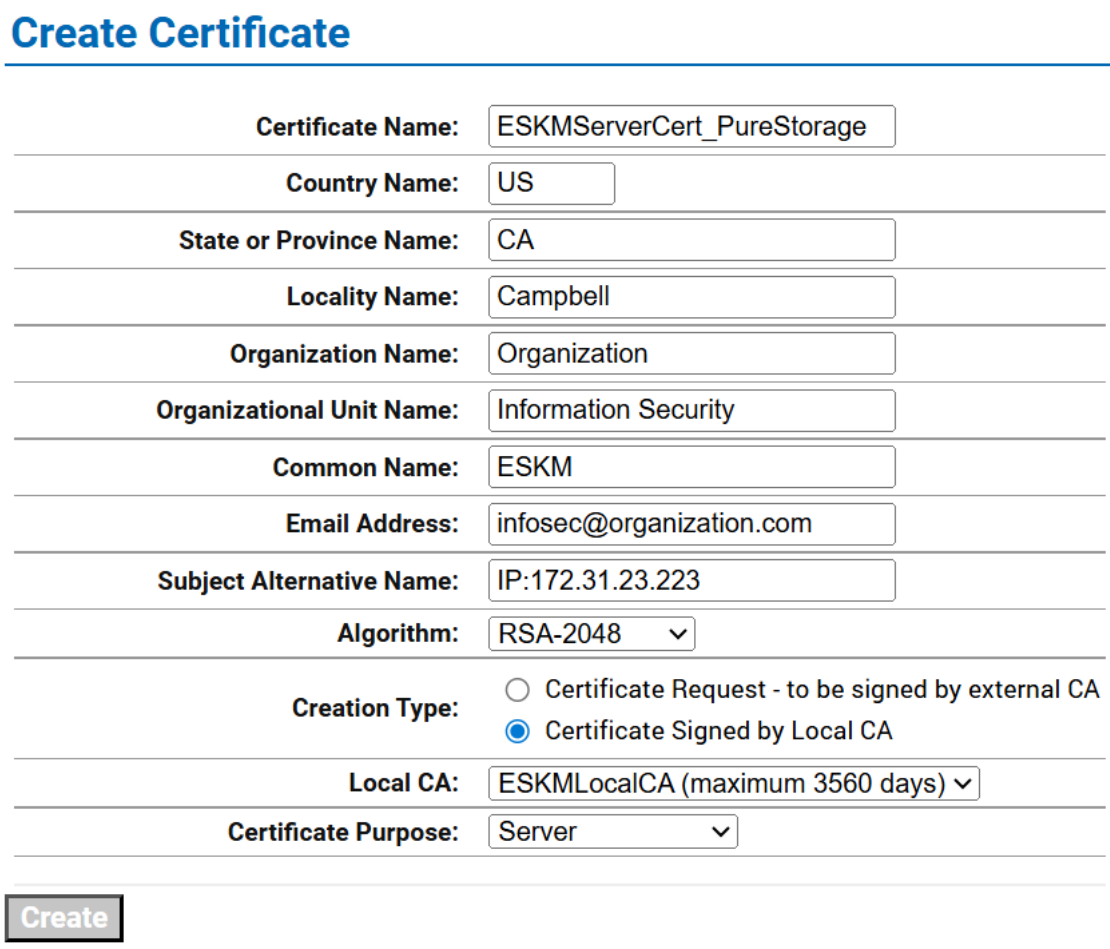



Figure 5 : Create Certificate

### 5.1.3 Configure the KMIP Server

1. In the **ESKM Management** console, go to **Device** > **KMIP Server** > **KMIP Server**.
2. Select the relevant KMIP Port.
3. Select the created server certificate as the **Server Certificate** for the KMIP server.
4. Select the created Local CA from the dropdown list.
5. Click **Save.**

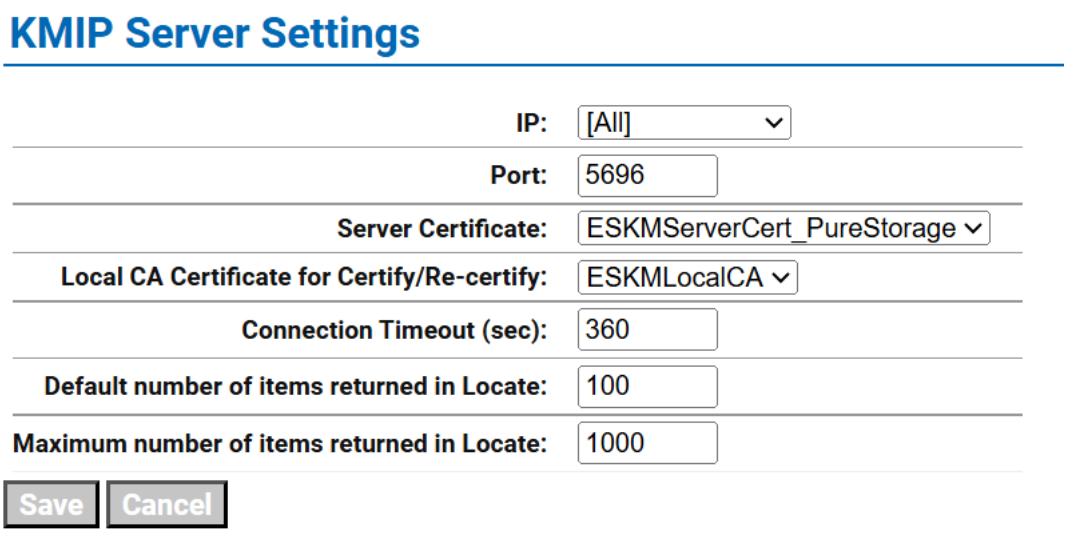



Figure 6 : KMIP Server Configuration

### 5.1.4 Sign the host certificate using ESKM

See *Client Certificate Creation* and generate a CSR in FlashArray CLI before you proceed with the steps below.

1. Copy the generated CSR from Pure Storage FlashArray CLI and submit it to ESKM for signing by the ESKMLocalCA as a client certificate.

```
pureuser@sv16-c50r4-b09-05> purecert construct eskm-kmip-cert --certificate-signing-request
-----BEGIN CERTIFICATE REQUEST-----
MIIC5DCCAcwCAQAwXDEgMB4GA1UEAwwXcHVyZXN0b3JhZ2Uta2lpcCljbGllbnQx
GzAZBgNVBAsMElBlcmUgU3RvcmFnZSwgSW5jLjEbMBkGA1UECgwSUHVyZSBTdG9y
YWdlLCBJbmMuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtrTCEO81
2JchBm4QsrFXzI+K98tI+DdpHcjl/THz0RtXqUhnCZmlPWfgIDud4fWLeRQwAeMq
AtBNP/DFyqp+Etpk9rM60A0MC0ftpzYTkpgwS9pc6Rwla+7Pt3VniErN7QltCwQT
pfUS2UHc5rISZWYh75421912VMtsMI5gyoAlClfgmUiLaUb35AUeFPZ5f/NXTKUU
8JOtvkEEEs3ijLuu4aJPfMBftRfG2l/dEAHAcIysYe/pHouvXho05iE5vp59OvoK
Y+X+dHNg6uuujvCEzDhViIH9YVG9uTqDRsWmlfk6nYsGiOLIXXOSyJnjYnlP7egq
ZQpV/qcESNbm+wIDAQABoEMwQQYJKoZIhvcNAQkOMTQwMjAiBgNVHREEGzAZghdw
dXJlc3RvcmFnZSlrbWlwLWNsaWVudDAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEB
CwUAA4IBAQB79QPYIK+5Z04eFMj9OnHlJCApbsgclE6zZdldvV7pIisItsgfe2Ao
pXAeZxlAYlPh3gMXnt0/8wu7ii3K0ixbKsovx7vEY90RIFE6EKdCkxDDtV5vQM2D
DAgAwkMLt5lluNoNjvZZOFR5UjnpB+xVgFE/PhblkSha2ydxQ4qTGX5Oc+gj4FzD
8CRLqBV9Vf3h4RHL9aPUc0PmGqd9uywDV+A57IooDRH+XIIrixuXcqPr5xgIVzOj
y6WmlOSOoy+cf4Y7OeQnA0ZJI5rFE8kl4Wj7alRNT+7Ks99Ck0zo2eCaxKGcWsd8
Vt4eLYD7XCuCfD3wsFAfNskGkVkVTCs8
-----END CERTIFICATE REQUEST-----
```

Figure 7 : Generated CSR in Pure Storage FlashArray CLI

2. Go to ESKM Management Console > Security > Certificates & CAs > Local CAs.

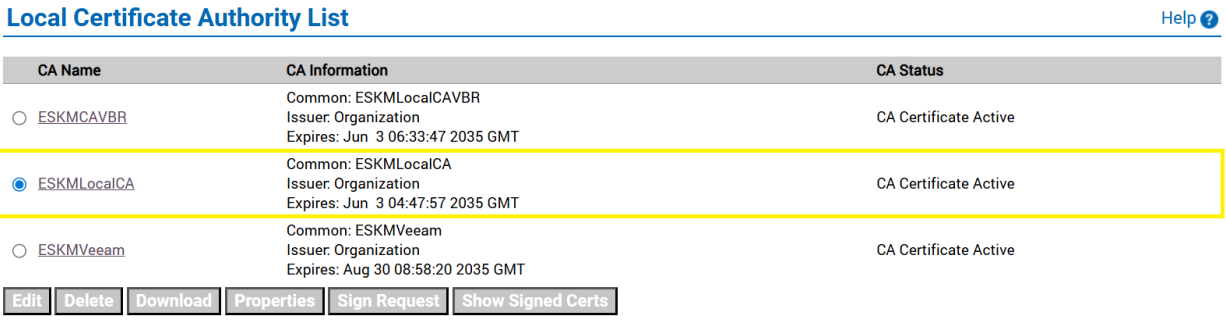



Figure 8 : Local CA

3. Select the created CA and click Sign Request.

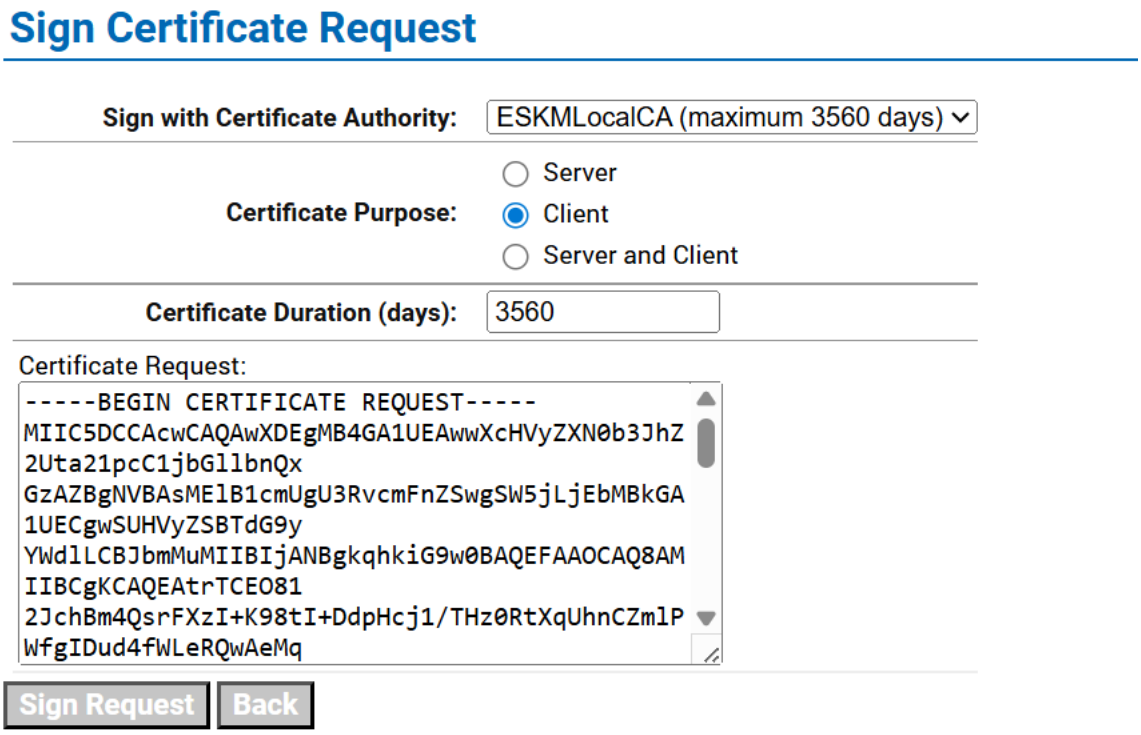
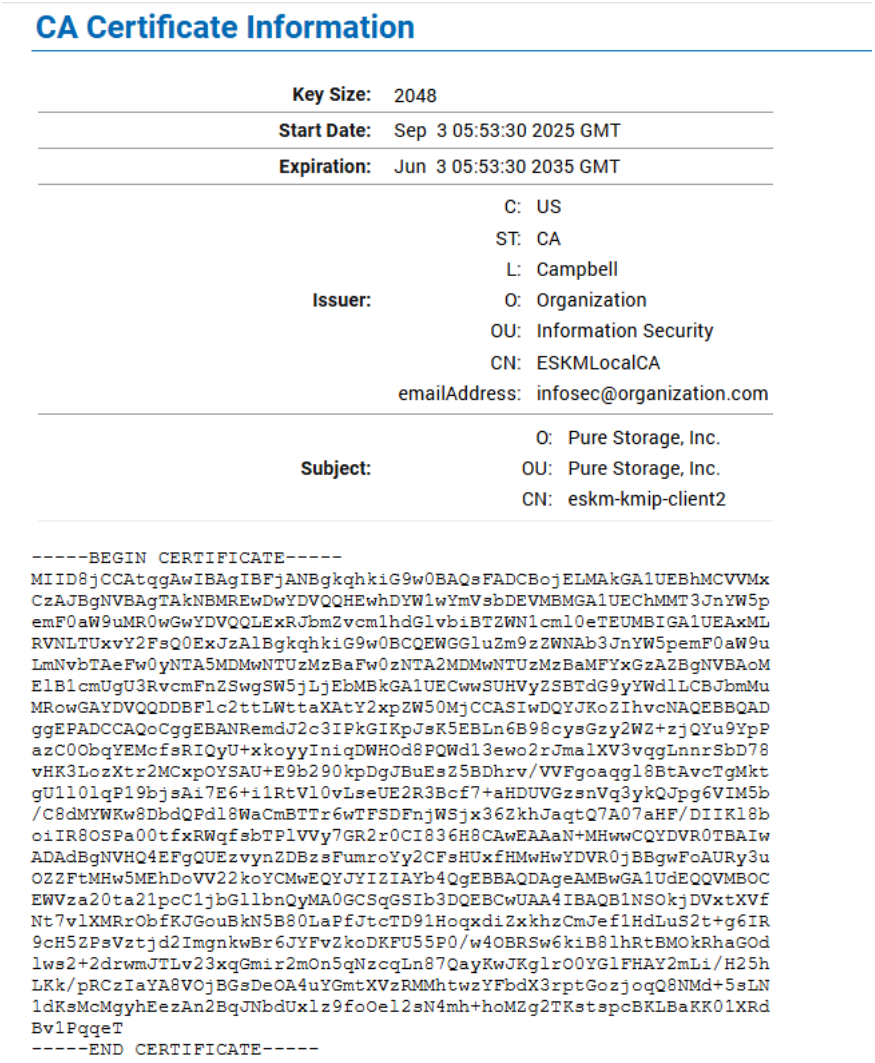



Figure 9 : Sign Certificate Request

4. Select the previously created CA certificate name from the Sign with Certificate Authority dropdown list.

5. Select Client in the Certificate Purpose section.

6. Copy the host certificate content to the **Certificate Request** box and click **Sign Request**.



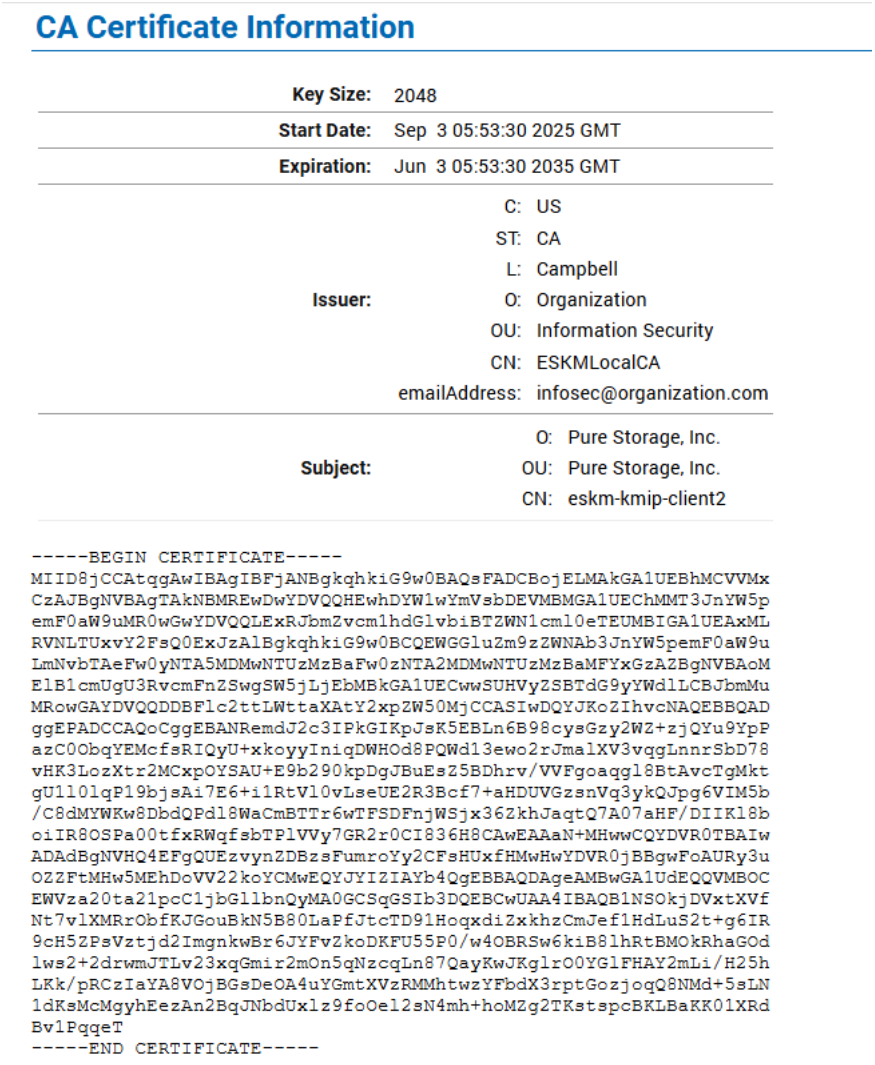
**CA Certificate Information**

| | | |
|---|---|---|
| **Key Size:** | 2048 | |
| **Start Date:** | Sep 3 05:53:30 2025 GMT | |
| **Expiration:** | Jun 3 05:53:30 2035 GMT | |
| **Issuer:** | C: | US |
| | ST: | CA |
| | L: | Campbell |
| | O: | Organization |
| | OU: | Information Security |
| | CN: | ESKMLocalCA |
| | emailAddress: | infosec@organization.com |
| **Subject:** | O: | Pure Storage, Inc. |
| | OU: | Pure Storage, Inc. |
| | CN: | eskm-kmip-client2 |

```
-----BEGIN CERTIFICATE-----
MIID8jCCAtqgAwIBAgIBFjANBgkqhkiG9w0BAQsFADCBojELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEVMBMGA1UEChMMT3JnYW5p
emF0aW9uMR0wGwYDVQQLExRJbmZvcm1hdGlvbiBTZWN1cml0eTEUMBIGA1UEAxML
RVNLTUxvY2FsQ0ExJzAlBgkqhkiG9w0BCQEWGGluZm9zZWNAb3JnYW5pemF0aW9u
LmNvbTAeFw0yNTA5MDMwNTUzMzBaFw0zNTA2MDMwNTUzMzBaMFYxGzAZBgNVBAoM
ElBlcmUgU3RvcmFnZSwgSW5jLjEbMBkGA1UECwwSUHVyZSBTdG9yYWdlLCBJbmMu
MRowGAYDVQQDDBFlc2ttLWttaXAtY2xpZW50MjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBANRemdJ2c3IPkGIKpJsK5EBLn6B98cysGzy2WZ+zjQYu9YpP
azC0ObqYEMcfsRIQyU+xkoyyIniqDWHOd8PQWd13ewo2rJmalXV3vqgLnnrSbD78
vHK3LozXtr2MCxpOYSAU+E9b290kpDgJBuEsZ5BDhrv/VVFgoaqgl8BtAvcTgMkt
gUll0lqP19bjsAi7E6+i1RtVl0vLseUE2R3Bcf7+aHDUVGzsnVq3ykQJpg6VIM5b
/C8dMYWKw8DbdQPdl8WaCmBTTr6wTFSDFnjWSjx36ZkhJaqtQ7A07aHF/DIIKl8b
oiIR8OSPa00tfxRWqfsbTPlVVy7GR2r0CI836H8CAwEAAaN+MHwwCQYDVR0TBAIw
ADAdBgNVHQ4EFgQUEzvynZDBzsFumroYy2CFsHUxfHMwHwYDVR0jBBgwFoAURy3u
OZ2FtMHw5MEhDoVV22koYCMwEQYJYIZIAYb4QgEBBAQDAgeAMBwGA1UdEQQVMBOC
EWVza20ta21pcC1jbGllbnQyMA0GCSqGSIb3DQEBCwUAA4IBAQB1NSOkjDVxtXVf
Nt7vlXMRrObfKJGouBkN5B80LaPfJtcTD91HoqxdiZxkhzCmJef1HdLuS2t+g6IR
9cH5ZPsVztjd2ImgnkwBr6JYFvZkoDKFU55P0/w4OBRSw6kiB81hRtBMOkRhaGOd
lws2+2drwmJTLv23xqGmir2mOn5qNzcqLn87QayKwJKglrO0YGlFHAY2mLi/H25h
LKk/pRCzIaYA8VOjBGsDeOA4uYGmtXVzRMMhtwzYFbdX3rptGozjoqQ8NMd+5sLN
1dKsMcMgyhEezAn2BqJNbdUxlz9foOel2sN4mh+hoMZg2TKstspcBKLBaKK01XRd
Bv1PqqeT
-----END CERTIFICATE-----
```

Figure 10 : Signed Certificate Information

7. Copy the signed certificate and paste it into the Pure Storage FlashArray CLI.
8. Click **ESKMLocalCA** from **Local CAs**, copy the ESKMLocalCA certificate, and paste it into the Pure Storage FlashArray CLI.



CA Certificate Information

| | |
|---|---|
| Key Size: | 2048 |
| Start Date: | Sep 3 05:53:30 2025 GMT |
| Expiration: | Jun 3 05:53:30 2035 GMT |
| Issuer: | C: US<br>ST: CA<br>L: Campbell<br>O: Organization<br>OU: Information Security<br>CN: ESKMLocalCA<br>emailAddress: infosec@organization.com |
| Subject: | O: Pure Storage, Inc.<br>OU: Pure Storage, Inc.<br>CN: eskm-kmip-client2 |


```
-----BEGIN CERTIFICATE-----
MIID8jCCAtqgAwIBAgIBFjANBgkqhkiG9w0BAQsFADCBojELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEVMBMGA1UEChMMT3JnYW5p
emF0aW9uMR0wGwYDVQQLExRJbmZvcm1hdGlvbiBTZWN1cml0eTEUMBIGA1UEAxML
RVNLTUxvY2FsQ0ExJzAlBgkqhkiG9w0BCQEWGGluZm9zZWNAb3JnYW5pemF0aW9u
LmNvbTAeFw0yNTA5MDMwNTUzMzBaFw0zNTA2MDMwNTUzMzBaMFYxGzAZBgNVBAoM
ElBlcmUgU3RvcmFnZSwgSW5jLjEbMBkGA1UECwwSUHVyZSBTdG9yYWdlLCBJbmMu
MRowGAYDVQQDDBFlc2ttLWttaXAtY2xpZW50MjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBANRemdJ2c3IPkGIKpJsK5EBLn6B98cysGzy2WZ+zjQYu9YpP
azC0obqYEMcfsRIQyU+xkoyyIniqDWHOd8PQWd13ewo2rJmalXV3vqgLnnrSbD78
vHK3LozXtr2MCxpOYSAU+E9b290kpDgJBuEsZ5BDhrv/VVFgoaqgl8BtAvcTgMkt
gUll0lqP19bjsAi7E6+i1RtVl0vLseUE2R3Bcf7+aHDUVGzsnVq3ykQJpg6VIM5b
/C8dMYWKw8DbdQPdl8WaCmBTTr6wTFSDFnjWSjx362khJaqtQ7A07aHF/DIIKl8b
oiIR8OSPa00tfxRWqfsbTPlVVy7GR2r0CI836H8CAwEAAaN+MHwwCQYDVR0TBAIw
ADAdBgNVHQ4EFgQUEzvynZDBzsFumroYy2CFsHUxfHMwHwYDVR0jBBgwFoAURy3u
OZZFtMHw5MEhDoVV22koYCMwEQYJYIZIAYb4QgEBBAQDAgeAMBwGA1UdEQQVMBOC
EWVza20ta21pcC1jbGllbnQyMA0GCSqGSIb3DQEBCwUAA4IBAQB1NSOkjDVxtXVf
Nt7vlXMRrObfKJGouBkN5B80LaPfJtcTD91HoqxdiZxkhzCmJef1HdLuS2t+g6IR
9cH5ZPsVztjd2ImgnkwBr6JYFvZkoDKFU55P0/w4OBRSw6kiB8lhRtBMOkRhaGOd
lws2+2drwmJTLv23xqGmir2mOn5qNzcqLn87QayKwJKglrO0YGlFHAY2mLi/H25h
LKk/pRCzIaYA8VOjBGsDeOA4uYGmtXVzRMMhtwzYFbdX3rptGozjoqQ8NMd+5sLN
1dKsMcMgyhEezAn2BqJNbdUxlz9foOel2sN4mh+hoMZg2TKstspcBKLBaKK01XRd
BvlPqqeT
-----END CERTIFICATE-----
```


Figure 11 : CA Certificate Information

### 5.1.5 Create a KMIP User

1. In the **ESKM Management console**, go to **Security** > **Users & Groups** > **Local Users & Groups** > **Local Users**.
2. Click **Add**.
3. Enter the **Username** exactly as the common name specified during creating the host certificate.
4. Select **Enable KMIP**.
5. Select **KMIP** as **License Type**.

6. Provide the client certificate in KMIP Client Certificate that is produced by signing the CSR with ESKMLocalCA.

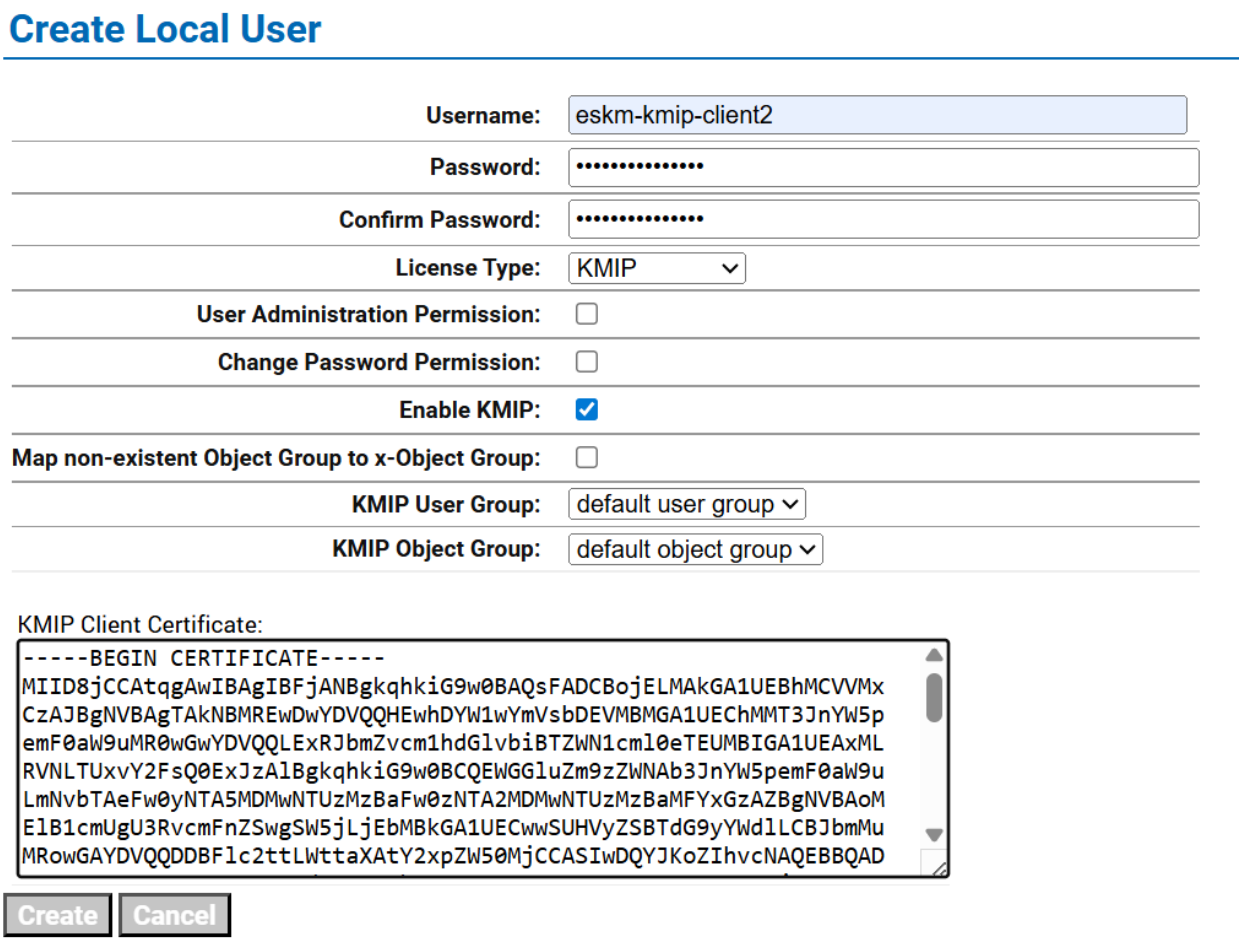



Figure 12 : Create KMIP a User

## 5.2 Configuration on Pure Storage FlashArray CLI

### 5.2.1 Create a Client Certificate

1. Create a self-signed certificate.

```
pureuser@sv16-c50r4-b09-05> purecert create eskm-kmip-cert --self-signed --common-name eskm-kmip-client2
Name           Type       Status       Key Algorithm  Key Size  Issued To          Issued By          Valid From
alid To                Subject Alt Names  Country  State/Province  Locality  Organization       Organizational Unit  E
mon Name
eskm-kmip-cert  appliance  self-signed  rsa            2048      eskm-kmip-client2  eskm-kmip-client2  2025-09-04 00:23:
035-09-02 00:23:21 PDT  eskm-kmip-client2  -        -               -         Pure Storage, Inc.  Pure Storage, Inc.   -
m-kmip-client2
```

Figure 13 : Create Self-Signed Certificate

2. Display the created self-signed certificate.

```
pureuser@sv16-c50r4-b09-05> purecert list eskm-kmip-cert --certificate
-----BEGIN CERTIFICATE-----
MIID2DCCAsCgAwIBAgIQcN/yr+MULVENnhF9Ij7X8DANBgkqhkiG9w0BAQsFADBW
MRowGAYDVQQDDBFlc2ttLWttaXAtY2xpZW50MjEbMBkGA1UECwwSUHVyZSBTdG9y
YWdlLCBJbmMuMRswGQYDVQQKDBJQdXJlIFN0b3JhZ2UsIEluYy4wHhcNMjUwOTA0
MDcyMzIxWhcNMzUwOTAyMDcyMzIxWjBWMRowGAYDVQQDDBFlc2ttLWttaXAtY2xp
ZW50MjEbMBkGA1UECwwSUHVyZSBTdG9yYWdlLCBJbmMuMRswGQYDVQQKDBJQdXJl
IFN0b3JhZ2UsIEluYy4wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC3
+sldUjI+YxjHpo0lpXQivWLTW+4Cvj8PE8O3UTyqONfdH9kUpw2semPHGjlqeNTr
MyJR7tf2qkCgsz3othnaf8L6kWdGkNQmp83QCBuGKbxpnLormko8oR7Rr4nk9IdO
ly0mGmu98vxZ+YHcVZvrYpKge8N3nyEOU59yUxLxOOFtE+8KxX3AZKve+FNsyxrN
tCL/oDAy6l5+pBjKsf04N/VRLFK9nVFKsfMfiSUvJzeN9cpvwcwYNsl8v7s7oOwQ
2kb2Bb6LEtsT73euG9cihfC3oD5XpqBAvztPAZp5m49uR4AYDMm28VmsHalIp3W+
+STr+fphPXZHwwYMoW27AgMBAAGjgaEwgZ4wHAYDVR0RBBUwE4IRZXNrbSlrbWlw
LWNsaWVudDIwHwYDVR0jBBgwFoAUCq/JSk7wJWK4JmZFnl5SE1V4NdkwHQYDVR0O
BBYEFAqvyUpO8CViuCZmRZ5eUhNVeDXZMAwGA1UdEwEB/wQCMAAwDgYDVR0PAQH/
BAQDAgKkMCAGA1UdJQEB/wQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG
9w0BAQsFAAOCAQEAaUBdOePf1SKgGiS7YSphFWs6lf2LPwKcDfhpMShAsrEbDTnv
PRhQ0xCKNMpNQ/ngVDfPqWmH8fLajH6ljGITYlORSceESCgKsnQEINOH8kFGj6nw
H3dKwLpGX2bOivDaxkKcVsmMnaKNixjrttkxreeQz8TfnyJpZ59Pgwn8viCLt+l+
j3IOMGbpKTH2NSzp+SdQwDj/i6uBJ+3tKKKPUrAU+WSbd/ATsplVZCcbDCmbmDHq
OvApDaXzSiOR9RZdtfoEgj7XLNO4hTSYn4khtA83lKV/+RXHgZnmeIa9v0CO6+Uq
/OUswgFijttUH0K74moNDD8JQ3xzm3LEtwvxNw==
-----END CERTIFICATE-----
```

Figure 14 : Display Self-Signed Certificate

3. Create a certificate signing request (CSR).

```
pureuser@sv16-c50r4-b09-05> purecert construct eskm-kmip-cert --certificate-signing-request
-----BEGIN CERTIFICATE REQUEST-----
MIIC2DCCAcACAQAwVjEaMBgGA1UEAwwRZXNrbS1rbW1wLWNsaWVudDIxGzAZBgNV
BAsMElB1cmUgU3RvcmFnZSwgSW5jLjEbMBkGA1UECgwSUHVyZSBTdG9yYWdlLCBJ
bmMuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1F6Z0nZzcg+QYgqk
mwrkQEufoH3xzKwbPLZZn7ONBi7lik9rMLQ5upgQxx+xEhDJT7GSjLIieKoNYc53
w9BZ3Xd7CjasmZqVdXe+qAueetJsPvy8crcujNe2vYwLGk5hIBT4Tlvb3SSkOAkG
4SxnkEOGu/9VUWChqqCXwG0C9xOAyS2BTWXSWo/XluOwCLsTr6LVGlWXS8ux5QTZ
HcFx/v5ocNRUbOydWrfKRAmmDpUgzlv8Lx0xhYrDwNtlA92XxZoKYFNOvrBMVIMW
eNZKPHfpmSElqqlDsDTtocX8MgggXxuiIhHw5I9rTSl/FFap+xtM+VVXLsZHavQI
jzfofwIDAQABoD0wOwYJKoZIhvcNAQkOMS4wLDAcBgNVHREEFTATghFlc2ttLWtt
aXAtY2xpZW50MjAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQBcqqf6
n3LqZP+vqCHKfU8rJbciqcsoswtDgvtc9H7WIrSMJrOxXLu8kKz+QCoJklup64KJ
b3nzi9tVfERCwgL/SFqlx7mBoA4tW3kosvNqjYPfQcH7iJCBnnzXGACcL6ybta7s
F/ZejD4jYklhhh/Rr3adjvqvbNgC+9+4uBsUFkl3H2VUbyH9+/zNvm5ljs45AlYO
NUXpJKtiyW82i/MIGstURDuBOgADacI4J2Wr/kPfuV7mXoC4l4ezZjo04lPlWxIS
6sR7wgd8ll5N7VS+dTZtiUwNYOR5ymlK8asmYluSkYRhq407mVwM/e+ZoFNfrElE
eGRsaed7KgGQjON2
-----END CERTIFICATE REQUEST-----
```

Figure 15 : Construct CSR

4. Copy the generated CSR and submit it to ESKM for signing by the ESKMLocalCA as a client certificate, see *Sign the host certificate using ESKM*.

5. Update the Pure Storage FlashArray certificate with the signed key details.
   When prompted, paste the client certificate from ESKM, see *Sign the host certificate using ESKM*.

```
pureuser@sv16-c50r4-b09-05> purecert setattr eskm-kmip-cert --certificate
Please enter certificate followed by Enter and then Ctrl-D:

-----BEGIN CERTIFICATE-----
MIID8jCCAtqgAwIBAgIBFjANBgkqhkiG9w0BAQsFADCBojELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEVMBMGA1UEChMMT3JnYW5p
emF0aW9uMR0wGwYDVQQLExRJbmZvcmlhdGlvbiBTZWN1cml0eTEUMBIGA1UEAxML
RVNLTUxvY2FsQ0ExJzAlBgkqhkiG9w0BCQEWGGluZm9zZWNAb3JnYW5pemF0aW9u
LmNvbTAeFw0yNTA5MDMwNTUzMzBaFw0zNTA2MDMwNTUzMzBaMFYxGzAZBgNVBAoM
ElBlcmUgU3RvcmFnZSwgSW5jLjEbMBkGA1UECwwSUHVyZSBTdG9yYWdlLCBJbmMu
MRowGAYDVQQDDBFlc2ttLWttaXAtY2xpZW50MjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBANRemdJ2c3IPkGIKpJsK5EBLn6B98cysGzy2WZ+zjQYu9YpP
azC0ObqYEMcfsRIQyU+xkoyyIniqDWHOd8PQWd13ewo2rJmalXV3vqgLnnrSbD78
vHK3LozXtr2MCxpOYSAU+E9b290kpDgJBuEsZ5BDhrv/VVFgoaqgl8BtAvcTgMkt
gUll0lqPl9bjsAi7E6+ilRtVl0vLseUE2R3Bcf7+aHDUVGzsnVq3ykQJpg6VIM5b
/C8dMYWKw8DbdQPdl8WaCmBTTr6wTFSDFnjWSjx36ZkhJaqtQ7A07aHF/DIIKl8b
oiIR8OSPa00tfxRWqfsbTPlVVy7GR2r0CI836H8CAwEAAaN+MHwwCQYDVR0TBAIw
ADAdBgNVHQ4EFgQUEzvynZDBzsFumroYy2CFsHUxfHMwHwYDVR0jBBgwFoAURy3u
OZZFtMHw5MEhDoVV22koYCMwEQYJYIZIAYb4QgEBBAQDAgeAMBwGA1UdEQQVMBOC
EWVza20ta2lpcCljbGllbnQyMA0GCSqGSIb3DQEBCwUAA4IBAQBlNSOkjDVxtXVf
Nt7vlXMRrObfKJGouBkN5B80LaPfJtcTD9lHoqxdiZxkhzCmJeflHdLuS2t+g6IR
9cH5ZPsVztjd2ImgnkwBr6JYFvZkoDKFU55P0/w4OBRSw6kiB8lhRtBMOkRhaGOd
lws2+2drwmJTLv23xqGmir2mOn5qNzcqLn87QayKwJKglrO0YGlFHAY2mLi/H25h
LKk/pRCzIaYA8VOjBGsDeOA4uYGmtXVzRMMhtwzYFbdX3rptGozjoqQ8NMd+5sLN
ldKsMcMgyhEezAn2BqJNbdUxlz9foOel2sN4mh+hoMZg2TKstspcBKLBaKK0lXRd
BvlPqqeT
-----END CERTIFICATE-----
```

Figure 16 : Update Client Certificate

### 5.2.2 Configure KMIP

Create the KMIP server configuration by specifying the ESKM hostname in the `--uri` parameter along with the KMIP port number. Provide the server certificate and CA certificate, see *Sign the host certificate using ESKM, for secure* communication.

```
pureuser@sv16-c50r4-b09-05> purekmip create ESKM-KMIP-Server --uri kms1.testeskm.com:5696 --certificate eskm-kmip-cert --ca-certificate
Please enter CA certificate followed by Enter and then Ctrl-D:

-----BEGIN CERTIFICATE-----
MIIEFDCCAvygAwIBAgIBADANBgkqhkiG9w0BAQsFADCBojELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhDYW1wYmVsbDEVMBMGA1UEChMMT3JnYW5p
emF0aW9uMR0wGwYDVQQLExRJbmZvcmlhdGlvbiBTZWN1cml0eTEUMBIGA1UEAxML
RVNLTUxvY2FsQ0ExJzAlBgkqhkiG9w0BCQEWGGluZm9zZWNAb3JnYW5pemF0aW9u
LmNvbTAeFw0yNTA2MDQwNDQ3NTdaFw0zNTA2MDMwNDQ3NTdaMIGiMQswCQYDVQQG
EwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBAcTCENhbXBiZWxsMRUwEwYDVQQKEwxP
cmdhbml6YXRpb24xHTAbBgNVBAsTFEluZm9ybWF0aW9uIFN1Y3VyaXR5MRQwEgYD
VQQDEwtFU0tNTG9jYWxDQTEnMCUGCSqGSIb3DQEJARYYaW5mb3N1Y0Bvcmdhbml6
YXRpb24uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzS4CUqBR
oFG6DZI8c6nCrxUleamMH12pbFTLSAq+xDkqL5xlsf7+QQUZm3WwBWkiMOMjy8ko
tVwa7FsZ2KRSM1J0tf64/+S5rxVsInqw8jMiuVUfTseh9aj5sUpXpsAXNntE2tlX
3OGa3reZyfpNBnq8xD4HCzq/BDJleja9ko+Hz+lDZXhhWIdTe/ZkWRQ6J3Sv7Zl1
8lkYOE1ySQGXEdVTMTbkBTPniPf0Ak2sjvgON1/99q7ThlFOoL0Ut3aGrPUlnvly
3uZ08JieV2UaVbFXdaRFsihnpOLsdeVUmEBcd48rIeXsxE5ing5w0QEfNZ4mV+5Q
yRm6OEigu9edFwIDAQABo1MwUTAdBgNVHQ4EFgQURy3uOZZFtMHw5MEhDoVV22ko
YCMwHwYDVR0jBBgwFoAURy3uOZZFtMHw5MEhDoVV22koYCMwDwYDVR0TAQH/BAUw
AwEB/zANBgkqhkiG9w0BAQsFAAOCAQEArOpObj/GhPm2icn4lZEEUl13ifCqYvVX
lzJqfiaol0ADFmvJGmZczw+TuTTj9HWX2+Etv+okKAVvJb5DJsik+AOk22zK3uAs
dle8fv4FsijnA3lpePUzZkBSEq9szW2b/3PjtBWvklVKt5Qa56+TTtr2jrfASObO
JBNScGAQaTrlerzlPLhn58qL36O/znffaJyC+aThaowhagIFryjgP3tU/eBETgPD
CV3py/+e8LIiIU2buMklKXgF0RcYMkmt6F+424cO9i/daWHafuGqCZcrjjBHsfJU
Ptgf6lvpcVMBNIyNqT3pHPGxNobaYSDCrqLtkPz3Bh9W9jtoo3Sdaw==
-----END CERTIFICATE-----
Name            URI                    Certificate     Ca Certificate Configured
ESKM-KMIP-Server  kms1.testeskm.com:5696  eskm-kmip-cert  True
```

Figure 17 : KMIP Server Configuration

### 5.2.3 Enable a Security Token

1. Test the KMIP connection, see *Functional Testing*, before enabling the security token.
2. Enable enhanced data security using the **ESKM-KMIP-Server**.

```
pureuser@sv16-c50r4-b09-05> purearray enable security-token --kmip ESKM-KMIP-Server
Enabled  Type  Signature                                                        Server
True     KMIP  eef5ab1d132729d21feb53c3496d5a92b5d0ffc64fc8d86bb034ae3f2256e2b9  ESKM-KMIP-Server
pureuser@sv16-c50r4-b09-05>
```

Figure 18 : Enable Security Token

3. List the security token.

```
pureuser@sv16-c50r4-b09-05> purearray list --security-token
Enabled  Status    Type  Signature                                                        Server
True     updating  KMIP  eef5ab1d132729d21feb53c3496d5a92b5d0ffc64fc8d86bb034ae3f2256e2b9  ESKM-KMIP-Server
```

Figure 19 : List Security Token

4. After enabling the security token, verify that the KMIP connection is active on the FlashArray, see *Functional Testing*, and confirm that a KMIP object is created on the ESKM, see *Verify KMIP Object*. Review the ESKM KMIP logs to ensure successful key validation and trust establishment, see *Verify ESKM KMIP Logs*.

# 6 Verification and Testing

In this chapter, we verify whether Utimaco ESKM and Pure Storage FlashArray integration works as expected. This involves validating the KMIP-based connection, confirming that the security token has been enabled on the FlashArray, and checking that the corresponding KMIP requests are logged and processed on the ESKM server.

## 6.1 Functional Testing

The `purekmip test` command was executed against the configured KMIP server to validate the functional connectivity. The test confirmed successful communication with the ESKM server and returned an OK status for the KMIP connection.

```
pureuser@sv16-c50r4-b09-05> purekmip test ESKM-KMIP-Server
Name               URI                      Status  Details
ESKM-KMIP-Server   kms1.testeskm.com:5696   OK
```

Figure 20 : Test KMIP Connection

## 6.2 Logs and Validation Steps

### 6.2.1 Verify ESKM KMIP Logs

Check the **LOCATE** and **MAC** requests in the Utimaco ESKM KMIP logs, which indicate that the FlashArray successfully located and validated the encryption key material via ESKM.

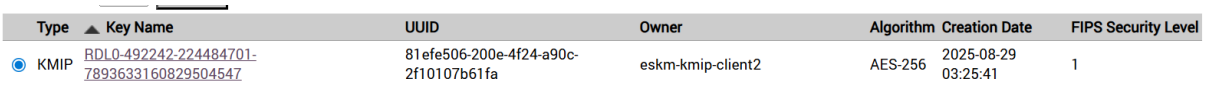
**KMIP Log:**

```
2025-08-31 03:12:05 [KMIP Server] [Authentication Success] User:[eskm-kmip-client2] From IP: 69.64.23.253
2025-08-31 03:12:05 [KMIP Server] [ClientOperation] User:[eskm-kmip-client2] UUID:[] Operation:[LOCATE] Result:[SUCCESS]
2025-08-31 03:12:05 [KMIP Server] [Authentication Success] User:[eskm-kmip-client2] From IP: 69.64.23.253
2025-08-31 03:12:05 [KMIP Server] [ClientOperation] User:[eskm-kmip-client2] UUID:[81efe506-200e-4f24-a90c-2f10107b61fa] Operation:[LOCATE] Result:[SUCCESS]
2025-08-31 03:12:06 [KMIP Server] [Authentication Success] User:[eskm-kmip-client2] From IP: 69.64.23.253
2025-08-31 03:12:06 [KMIP Server] [ClientOperation] User:[eskm-kmip-client2] UUID:[] Operation:[LOCATE] Result:[SUCCESS]
2025-08-31 03:12:06 [KMIP Server] [Authentication Success] User:[eskm-kmip-client2] From IP: 69.64.23.253
2025-08-31 03:12:06 [KMIP Server] [ClientOperation] User:[eskm-kmip-client2] UUID:[81efe506-200e-4f24-a90c-2f10107b61fa] Operation:[MAC] Object Type:[SYMMETRIC_KEY] Result:[SUCCESS]
2025-08-31 03:12:06 [KMIP Server] [Authentication Success] User:[eskm-kmip-client2] From IP: 69.64.23.253
2025-08-31 03:12:06 [KMIP Server] [ClientOperation] User:[eskm-kmip-client2] UUID:[81efe506-200e-4f24-a90c-2f10107b61fa] Operation:[MAC] Object Type:[SYMMETRIC_KEY] Result:[SUCCESS]
```

Figure 21 : Verify KMIP Log

### 6.2.2 Verify KMIP Object

1. After enabling the security token on the FlashArray, verify that a KMIP object has been created for the FlashArray client by navigating to the **ESKM Management Console** and clicking **Security** > **KMIP Objects**.



| Type | Key Name | UUID | Owner | Algorithm | Creation Date | FIPS Security Level |
|---|---|---|---|---|---|---|
| KMIP | RDL0-492242-224484701-7893633160829504547 | 81efe506-200e-4f24-a90c-2f10107b61fa | eskm-kmip-client2 | AES-256 | 2025-08-29 03:25:41 | 1 |

Figure 22 : KMIP Object

2. This confirms that the external key manager is supplying the root encryption key material used by the FlashArray.

# 7 Troubleshooting

## 7.1 Log locations and interpretation

You can verify the logs from Utimaco ESKM by following these steps:

1. In the **ESKM Management Console**, click **Device** > **Logs & Statistics** > **Log Viewer** > **KMIP**.
2. Review the logs for operations such as **LOCATE** and **MAC**, which confirm that the Pure Storage FlashArray successfully connected to ESKM and validated encryption keys.

**KMIP Log:**

```
2025-08-31 03:12:05 [KMIP Server] [Authentication Success] User:[eskm-kmip-client2] From IP: 69.64.23.253
2025-08-31 03:12:05 [KMIP Server] [ClientOperation] User:[eskm-kmip-client2] UUID:[] Operation:[LOCATE] Result:[SUCCESS]
2025-08-31 03:12:05 [KMIP Server] [Authentication Success] User:[eskm-kmip-client2] From IP: 69.64.23.253
2025-08-31 03:12:05 [KMIP Server] [ClientOperation] User:[eskm-kmip-client2] UUID:[81efe506-200e-4f24-a90c-2f10107b61fa] Operation:[LOCATE] Result:[SUCCESS]
2025-08-31 03:12:06 [KMIP Server] [Authentication Success] User:[eskm-kmip-client2] From IP: 69.64.23.253
2025-08-31 03:12:06 [KMIP Server] [ClientOperation] User:[eskm-kmip-client2] UUID:[] Operation:[LOCATE] Result:[SUCCESS]
2025-08-31 03:12:06 [KMIP Server] [Authentication Success] User:[eskm-kmip-client2] From IP: 69.64.23.253
2025-08-31 03:12:06 [KMIP Server] [ClientOperation] User:[eskm-kmip-client2] UUID:[81efe506-200e-4f24-a90c-2f10107b61fa] Operation:[MAC] Object Type:[SYMMETRIC_KEY] Result:[SUCCESS]
2025-08-31 03:12:06 [KMIP Server] [Authentication Success] User:[eskm-kmip-client2] From IP: 69.64.23.253
2025-08-31 03:12:06 [KMIP Server] [ClientOperation] User:[eskm-kmip-client2] UUID:[81efe506-200e-4f24-a90c-2f10107b61fa] Operation:[MAC] Object Type:[SYMMETRIC_KEY] Result:[SUCCESS]
```

Figure 23 : KMIP Log

# 8 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Germanusstr. 4
52080 Aachen
Germany

### RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

### Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

# 9 Appendices

## 9.1 References

| Title | Description | Document/Link |
|---|---|---|
| ESKM Installation Guide | Step-by-step guide for installing and configuring ESKM. | 2021-0047 Installation and Replacement Guide |
| FLASHARRAY SECURITY AND COMPLIANCE | Document describes the Pure Storage FlashArray data at rest encryption and RDL mechanisms. | *https://www.purestorage.com/content/dam/pdf/en/white-papers/wp-flasharray-data-security-and-compliance.pdf* |

Table 5: References

## 9.2 Command Summary

| Command Used | Purpose |
|---|---|
| `purecert create eskm-kmip-cert --self-signed --common-name eskm-kmip-client` | To create a self-signed client certificate for KMIP authentication |
| `purecert list eskm-kmip-client --certificate` | To list the details of the generated certificate |
| `purecert construct eskm-kmip-cert --certificate-signing-request` | To generate a CSR |
| `purecert setattr eskm-kmip-cert --certificate` | To associate the signed certificate with the client identity |

| Command Used | Purpose |
|---|---|
| `purekmip create ESKM-KMIP-Server --uri kms1.testeskm.com:5696 --certificate eskm-kmip-cert --ca-certificate` | To configure the ESKM KMIP server with URI, client cert and CA cert |
| `purekmip test ESKM-KMIP-Server` | To test connectivity and authentication with the KMIP server |
| `purekmip list ESKM-KMIP-Server` | To display available KMIP server details |
| `purearray enable security-token --kmip ESKM-KMIP-Server` | To enable security token and establish trust with the KMIP server |

Table 6: CLI Commands