Open PGP and Luna HSM Integration Guide

Document Information

Document Part Number	007-012381-001 (Rev B)
Release Date	November 2014

Trademarks

Limitations

This document does not include the steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA documentation for general Luna setup procedures.

Disclaimer

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Support Contacts

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

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Email	support@safenet-inc.com	

Contents

CHAPTER 1
Introduction

This document is intended to guide administrators through the steps for Open PGP and Luna HSM integration, and also covers the necessary information to install, configure and integrate Open PGP with SafeNet Luna Hardware Security Modules (HSMs).

The Luna HSMs integrates with the Open PGP to provide significant performance improvements by off-loading cryptographic operations from the Server to the Luna HSMs. In addition, the Luna HSMs provides extra security by protecting the private keys within a FIPS 140-2 certified hardware security module.

Understanding the OPEN PGP

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991.

PGP and similar software follow the Open PGP standard (RFC 4880) for encrypting and decrypting data.

Scope

This guide provides instructions for setting up a small test lab with Open PGP running with Luna HSM for securing the private keys. It explains how to install and configure the software that is required for setting up an Open PGP while storing private key on Luna HSM.

3rd Party Application Details

- Symantec Encryption Desktop Win32-10.3.0
- Symantec Encryption Desktop Win64-10.3.0
- PGP Command Line-10.3.0.214
- Symantec Encryption Desktop Win64-10.3.2
- PGP Command Line-10.3.2.12268

You can download the PGP Software's from Symantec Support site:

Supported Platforms

The following platforms are supported for Luna HSM:

Operating System	SafeNet Luna HSM	Encryption Desktop	PGP Command Line
Windows Server 2008 (32 bit)	Luna SA v5.1 (32 bit)	Win32-10.3.0	10.3.0.214 (32 bit)
Windows Server 2008 R2	Luna SA v5.1 (32 bit)	Win64-10.3.0	10.3.0.214 (32 bit)
Windows Server 2008 R2	Luna SA v5.2.1 (32 bit)	Win64-10.3.2	10.3.2.12268 (32 bit)

NOTE: We cannot use 64 bit PGP Command Line and 64 bit Symantec Encryption Desktop with Luna CSP because Encryption Desktop (both 64 and 32 bit) uses only 32 bit Luna CSP to create a key-ring that is accessible by 32 bit Command Line only. So we cannot use 64 bit Encryption Desktop and 64 bit Command Line together with Luna CSP.

HSM and Firmware Support

We did this integration with the following:

- Luna SA f/w 6.2.1 with Luna Client s/w v5.1 (32 bit)
- Luna SA f/w 6.10.1 with Luna Client s/w v5.2.1 (32 bit)

Prerequisites

Luna SA Setup

Please refer to the **Luna SA** documentation for installation steps and details regarding configuring and setting up the box on Windows operating systems. Before you get started ensure the following:

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

Open PGP Setup

You should familiarize yourself with Open PGP. Refer to the Symantec Encryption Desktop and PGP Command Line documentation for more information to install and pre-installation requirements.

Symantec Encryption Desktop and PGP Command Line must be installed on the target machine to carry on with the integration process. This guide will use to setup a small lab for testing purposes that uses the following:

- Windows machine, which will become a Domain Controller and Certification Authority.
- Windows machine, which is used to setup PGP.

NOTE: We can install the domain controller and CA on different machines depends upon the requirement. For testing purpose we installed the Domain Controller and CA on same machine. If you are installing PGP on different machine then it must be joined in to the domain.

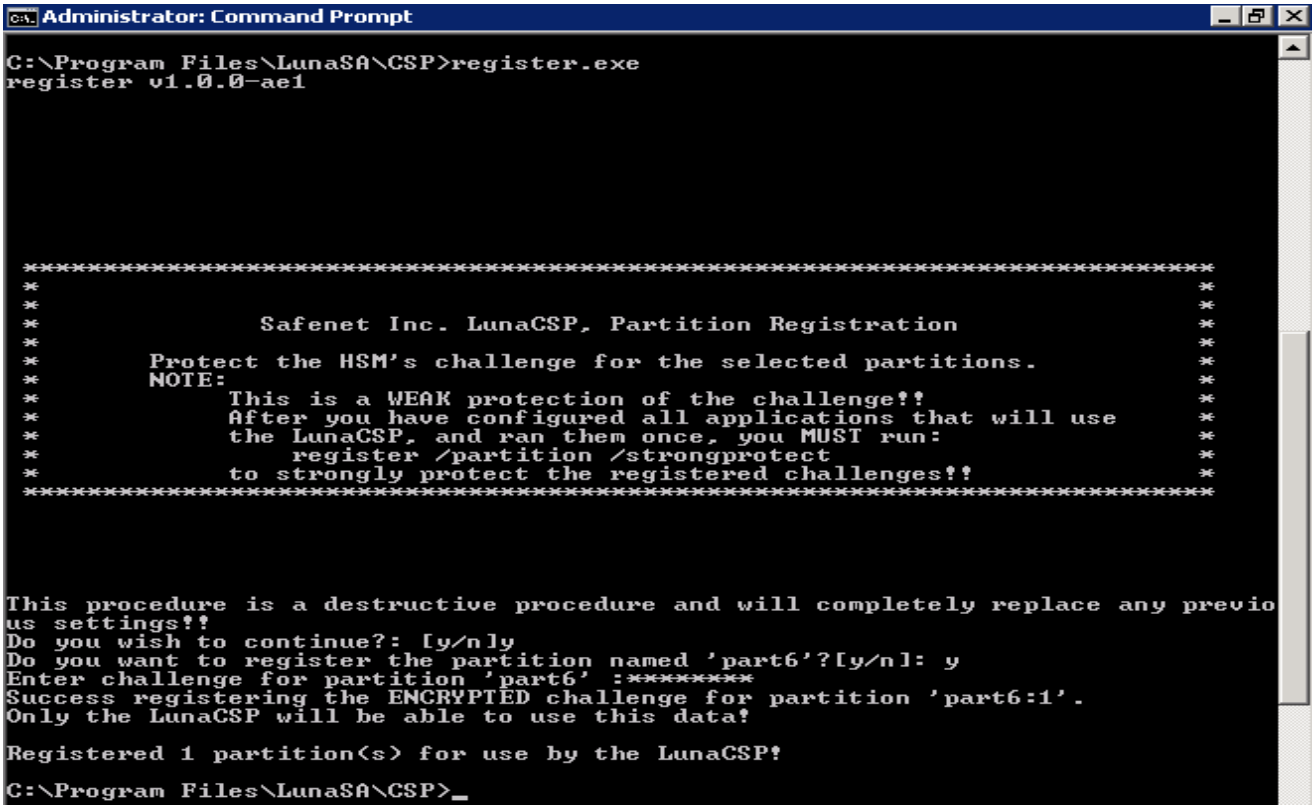
Before you install

1. CSP must be installed on the system in a separate step following completion of the main Luna SA Client software installation.
2. Open the command prompt and Traverse to

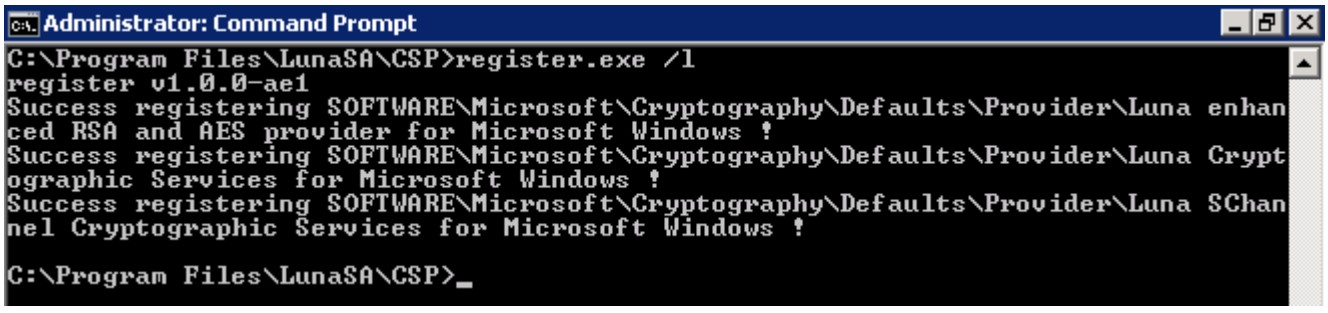
   C:\Program Files\LunaSA\CSP (for Luna Client 5.1)

   C:\Program File\SafeNet\LunaClient\win32\CSP (for Luna Client 5.2.1 onwards)

3. Run the register.exe and provide the Luna SA partition password when prompt, to register the partition to use with CSP.



4. Run the "register.exe /l" to list the Luna CSPs



CHAPTER 2
Integrating Open PGP with Luna (v5.1)

Setting up Luna with Open PGP

To set up Luna HSM for Symantec Encryption Desktop and PGP Command Line, kindly perform the following steps:

Setting up Luna SA for Active Directory Certificate Services

To set up Luna SA for Active Directory Certificate Services, kindly refer the Microsoft Active Directory Certificate Services Integration Guide with Luna SA.

1. Configuring the CA to issue PGP User Certificate

Configuring a CA to create a certificate template and issuing properties for PGP user certificate.

1.1 Configuring certificate templates for your test environment

a) Log on to system as a domain administrator.

b) From the Start menu, select Run.

c) In the Run dialog, type mmc and click OK.

d) In the mmc console that appears, select File > Add/Remove Snap-in…

e) In the Add or Remove Snap-Ins dialog box, find the Certificate Templates snap-in (under the Available snap-ins section) and select it.

f) Click Add, and then click OK.

g) Under Console Root, expand the Certificate Templates snap-in. Listed in the middle section will be all the available certificate templates that you can make your CA issue.

h) Scroll down the list until you locate the User template, right-click and click Duplicate Template.

i) Select Windows Server 2003 Enterprise and click OK.

j) In the pop-up dialog that appears, click the General tab.

k) Enter the Template Display Name for example PGP User here and select Publish Certificate in Active Directory.

l) Click the Request Handling tab.

m) Click on CSPs and select Request can use any CSP available on subject's computer.

n) Click OK to close the window.

o) Click the Subject Name tab.

p) Uncheck E-mail name in subject name and E-mail name check boxes.

q) Click the Security tab.

r) Add and provide the Read and Enroll permissions to the following:

- Authenticated Users
- Administrator

s) For Domain Admins and Enterprise Admins, make sure that Read, Write, and Enroll check boxes are ticked.

t) Click Apply and then OK.

1.2 Configuring the CA to support the PGP certificate template

a) Log on to system as a domain administrator.

b) From the Start menu select Control Panel > Administrative Tools > Certification Authority.

c) In the console tree (left-hand section), expand the CA. (It has a computer and a green tick next to it.)

d) In console tree of the Certification Authority snap-in, right-click Certificate Templates, and then click New Certificate Templates to Issue.

e) In Enable Certificates Templates, select the PGP User template and any other certificate templates you configured previously, and then click OK.

f) Open Certificate Templates in the Certification Authority and verify that the modified certificate templates appear in the list.

Creating a key and requesting a certificate

a) Log on to system as a domain administrator.

b) From the Start menu, select Run.

c) In the Run dialog, type certmgr.msc and click OK. If you are using 64 bit OS then open the certmgr.msc from the location “C:\Windows\SysWow64”.

d) In the mmc console that appears, right click on the Personal folder and select All Tasks -> Request New Certificate…

e) Click Next, Select Active Directory Enrollment Policy and then click Next. It will show you the certificate template you have configured, i.e. PGP User

f) Click on Details and then Properties.

g) Certificate Properties window will open and select the Subject tab.

h) Select Common Name under Subject Name and provide the fully qualified domain name for the computer on which you are installing the certificate in the Value field and click Add. Repeat the same step for adding more values.

i) Click on General tab and provide the Friendly Name. For example PGP User.

j) Click on Private Key tab, and verify that Luna Cryptographic Services for Microsoft Windows must be selected under the Cryptographic Service Provider.

k) Click on Certificate Authority tab, and make sure that Enterprise Root CA is selected.

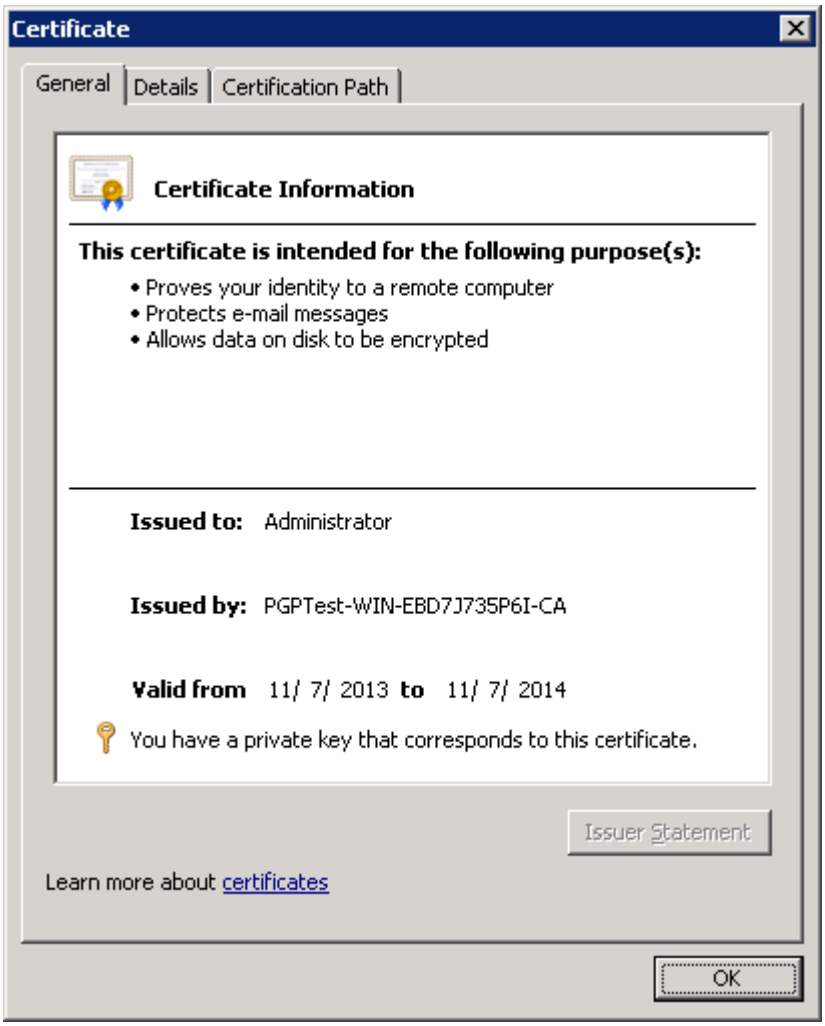
l) Click Apply and then OK.

m) Select PGP User certificate template or the certificate template you have configured, and click Enroll.

n) It will take some time to enroll, when enrollment succeeded, click Finish.

o) Make sure that certificate is now available in the Personal -> Certificate store.

p) Double click on the certificate and see that “You have a private key that corresponds to this certificate”.



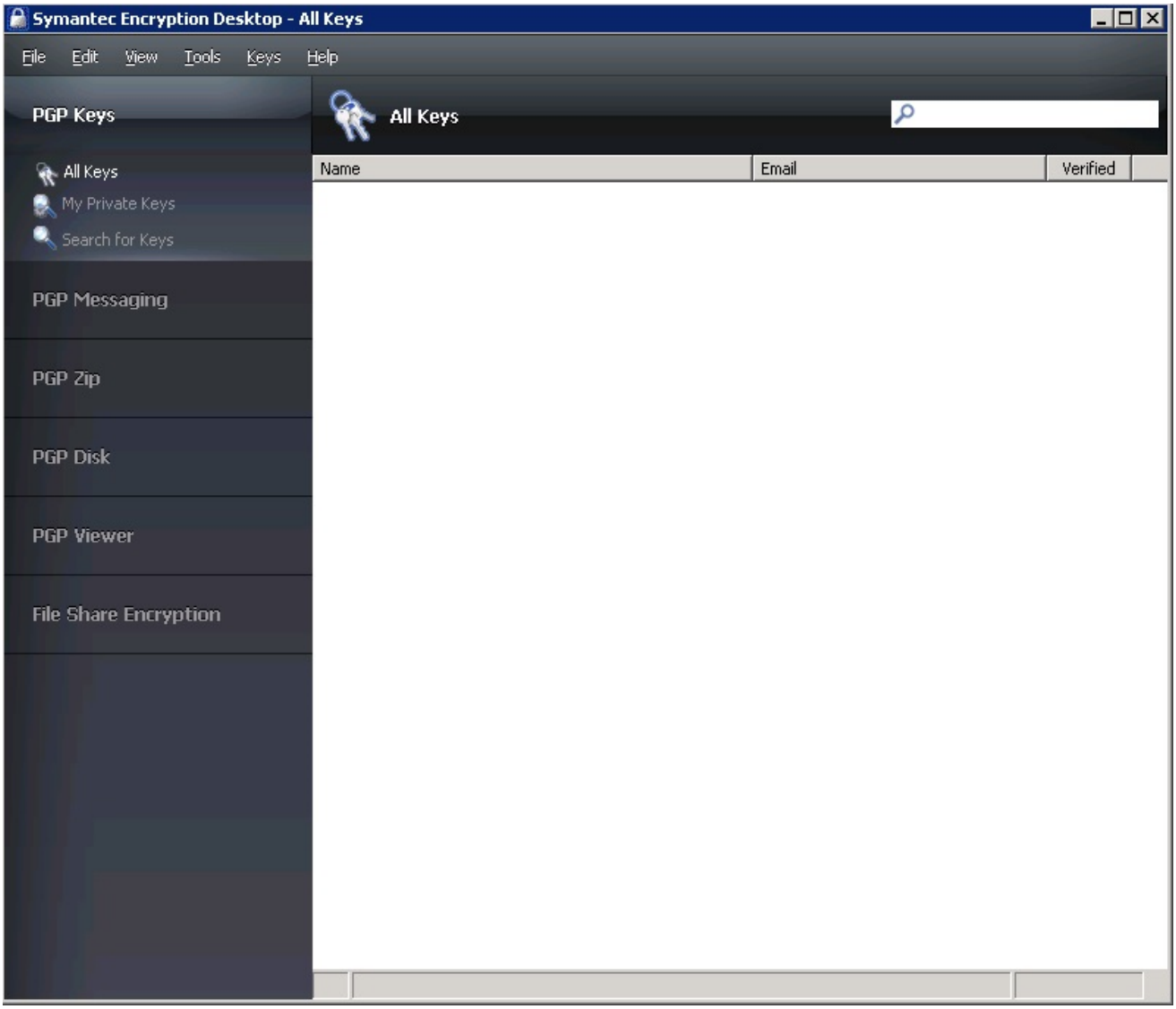
The keys for this certificate will be generated on Luna HSM box. You can see the contents on Luna SA box.

2. Configuring PGP applications to use available keys

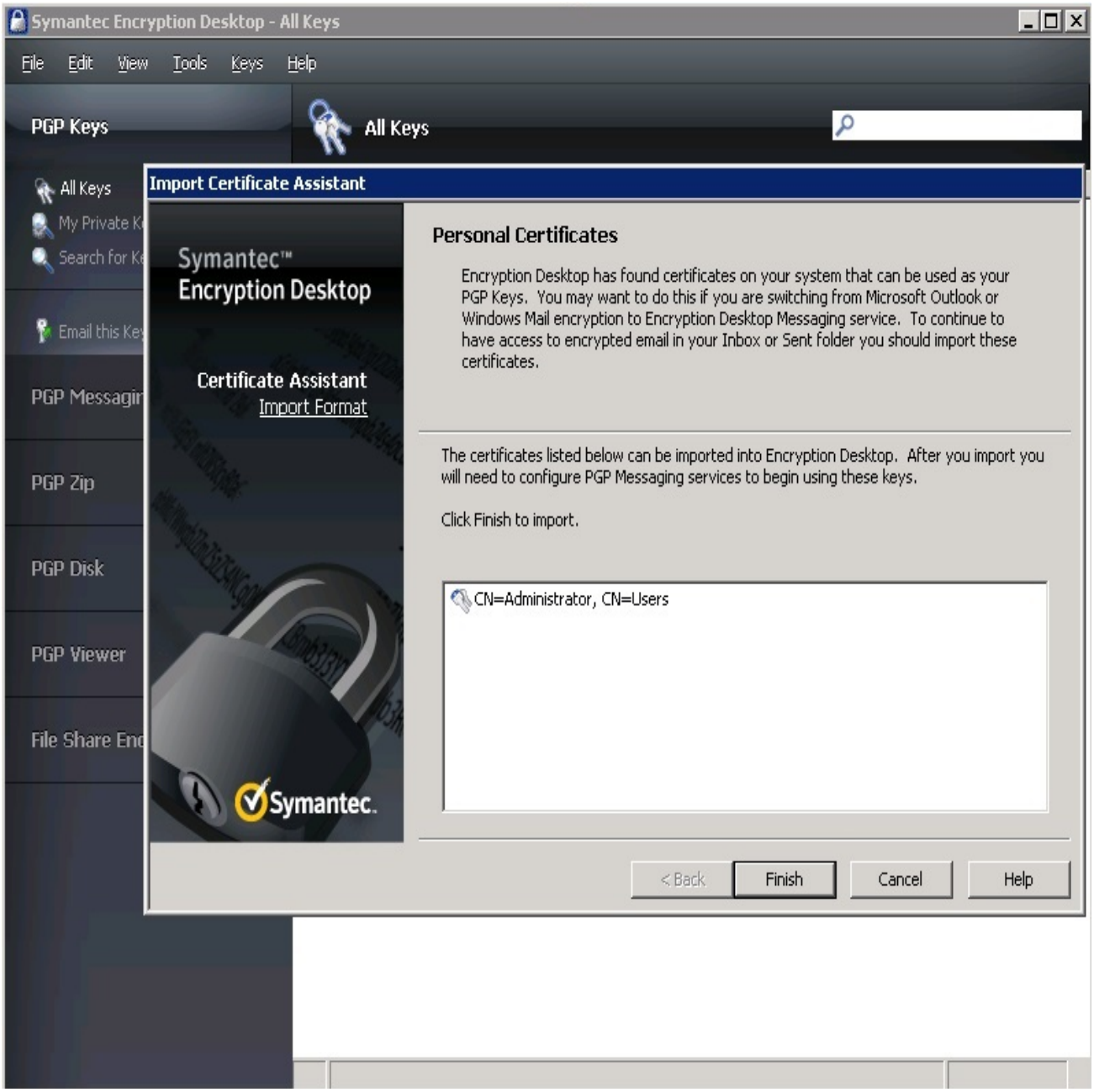
The first step to be able to use the keys protected by the HSM with PGP Applications is to import them in the current key ring files using Encryption Desktop.

2.1 Import the keys in Symantec Encryption Desktop

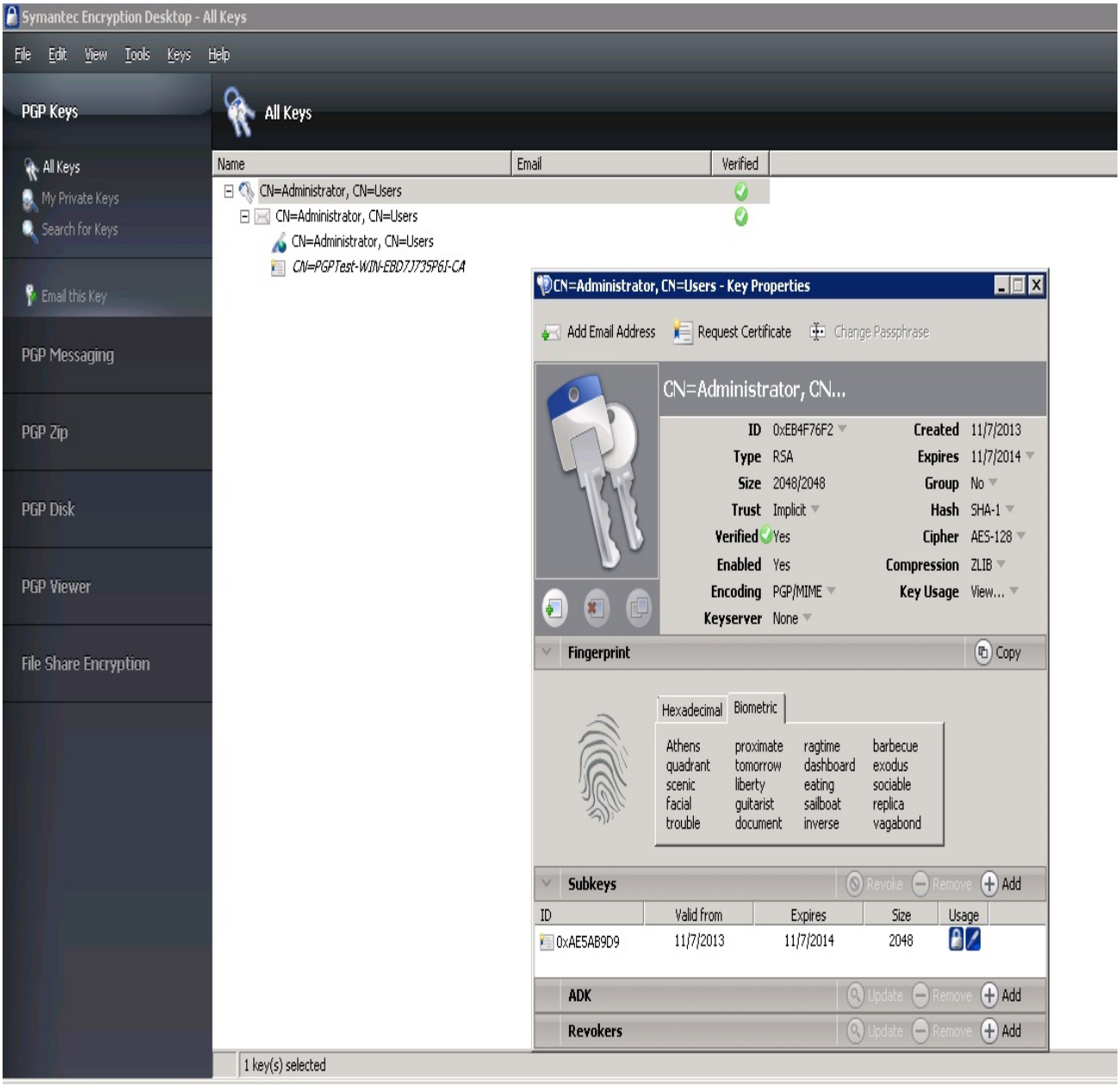
1. Open the Symantec Encryption Desktop and select PGP Keys on the left side of the window



2. From File menu choose “Import Personal Certificates“, click Finish.



3. Confirm the list of keys / certificates found to be imported into the PGP Key Ring. Double click to open the properties window to see the details.



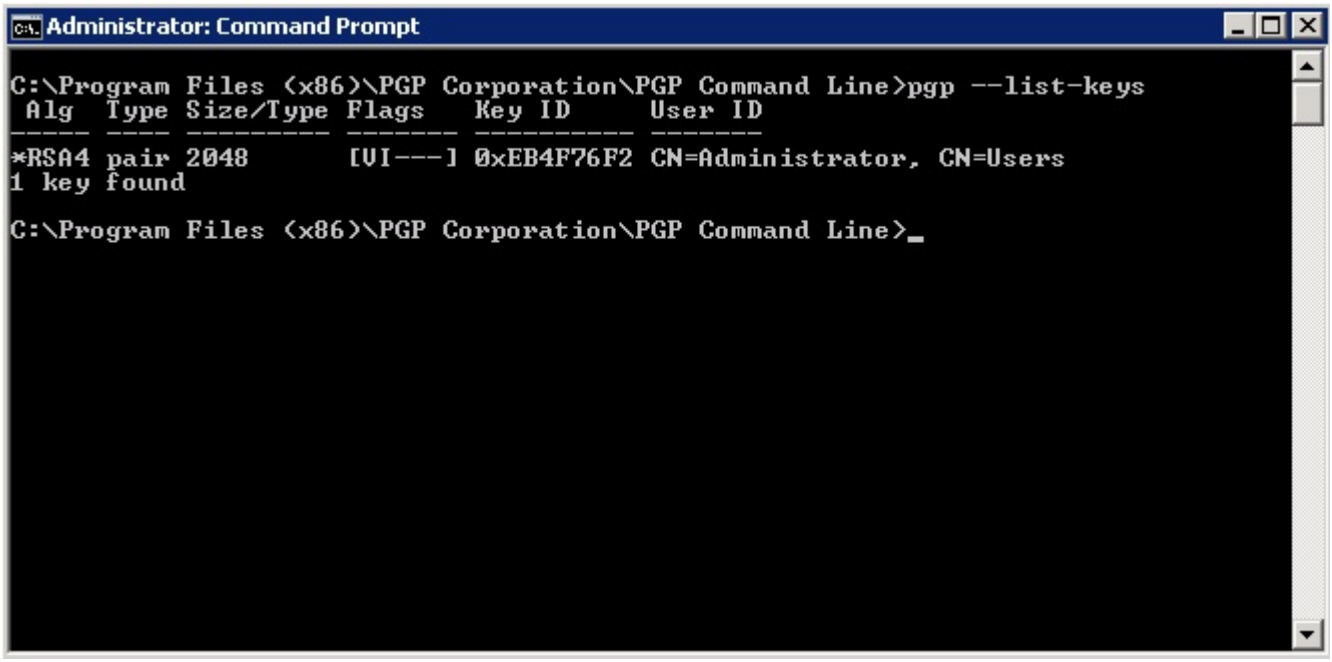
4. The certificate protected by the HSM can now be used in all PGP Applications.

2.2 List the keys using PGP Command Line

After the keys / certificates were imported into the key ring, these can now be listed with PGP Command Line. To list the keys execute:

```
pgp --list-keys
```

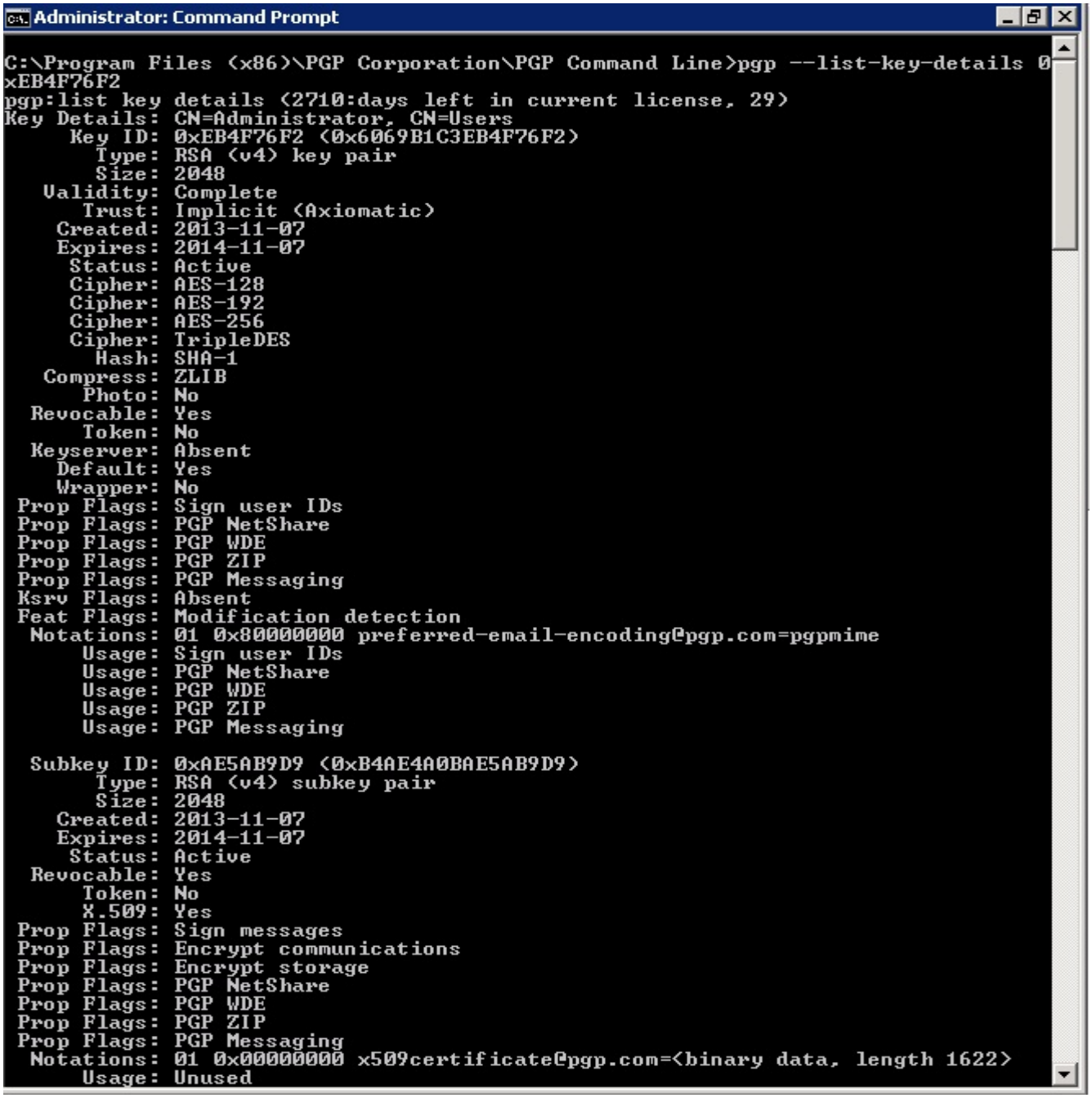
This will show you all available keys for PGP Command Line



The keys protect by the HSM will show up as key pair since public and private part is available for PGP Command Line

More details about a single key can be shown when executing:

```
pgp --list-key-details 0xEB4F76F2
```

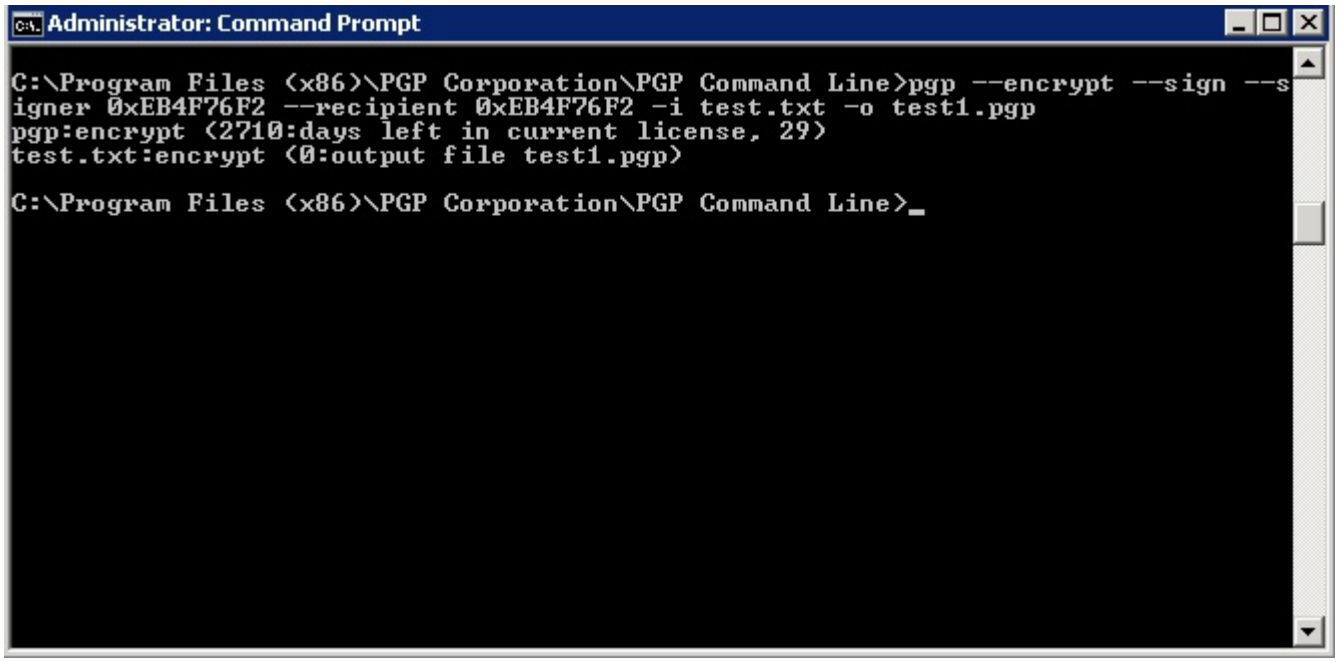


2.3 Using the keys with PGP Command Line

After these steps the keys protected by the HSM can be used in the same way as any other keys available in the PGP key ring.

To sign a file called “test.txt” with the key with ID 0xEB4F76F2 (stored on HSM) and encrypt it to a recipient with the key ID 0xXXXXXXXX execute the following command.

```
pgp --encrypt --sign --signer 0xEB4F76F2 --recipient 0xEB4F76F2 -i test.txt -o test1.pgp
```

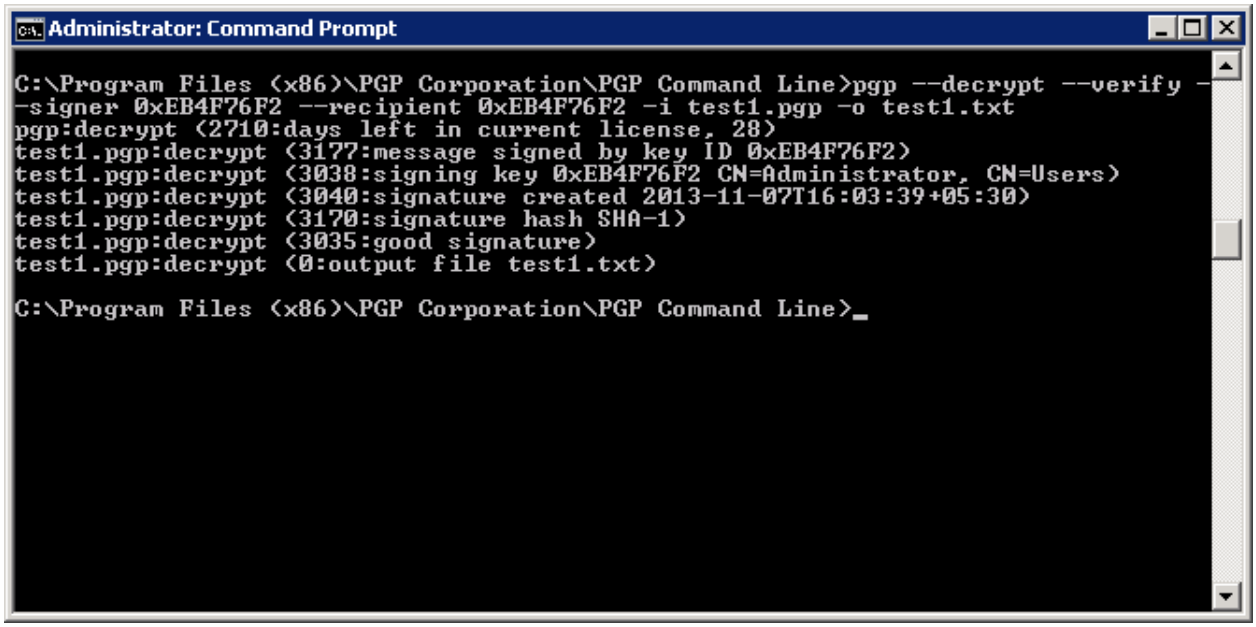


NOTE: We have used here same ID for signer and recipient both for test purpose.

It will create the encrypted test1.pgp file in the current directory.

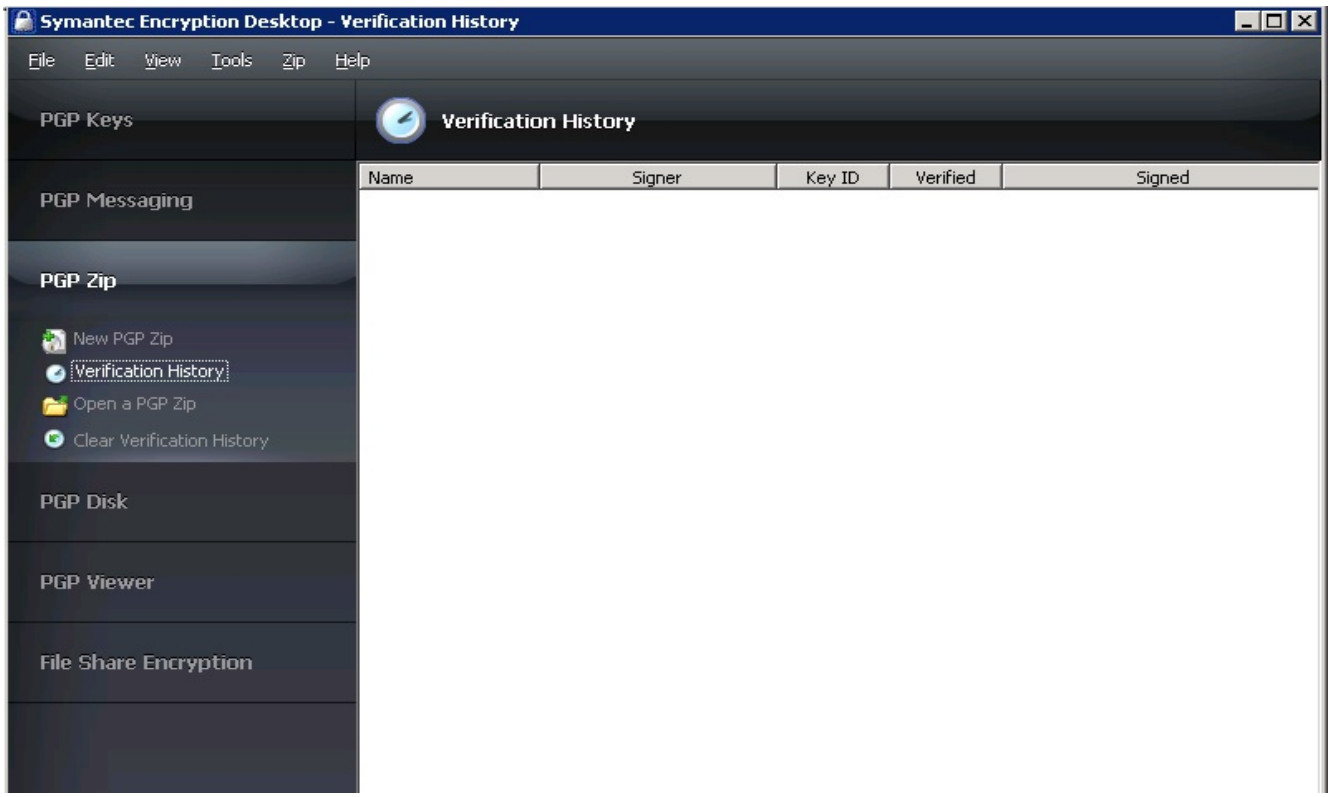
To verify an encrypted file called “test1.pgp” with the key with ID 0xEB4F76F2 (stored on HSM) and encrypt it to a recipient with the key ID 0xXXXXXXXX execute the following command.

```
pgp --decrypt --verify --signer 0xEB4F76F2 --recipient 0xEB4F76F2 -i test1.pgp -o test1.txt
```

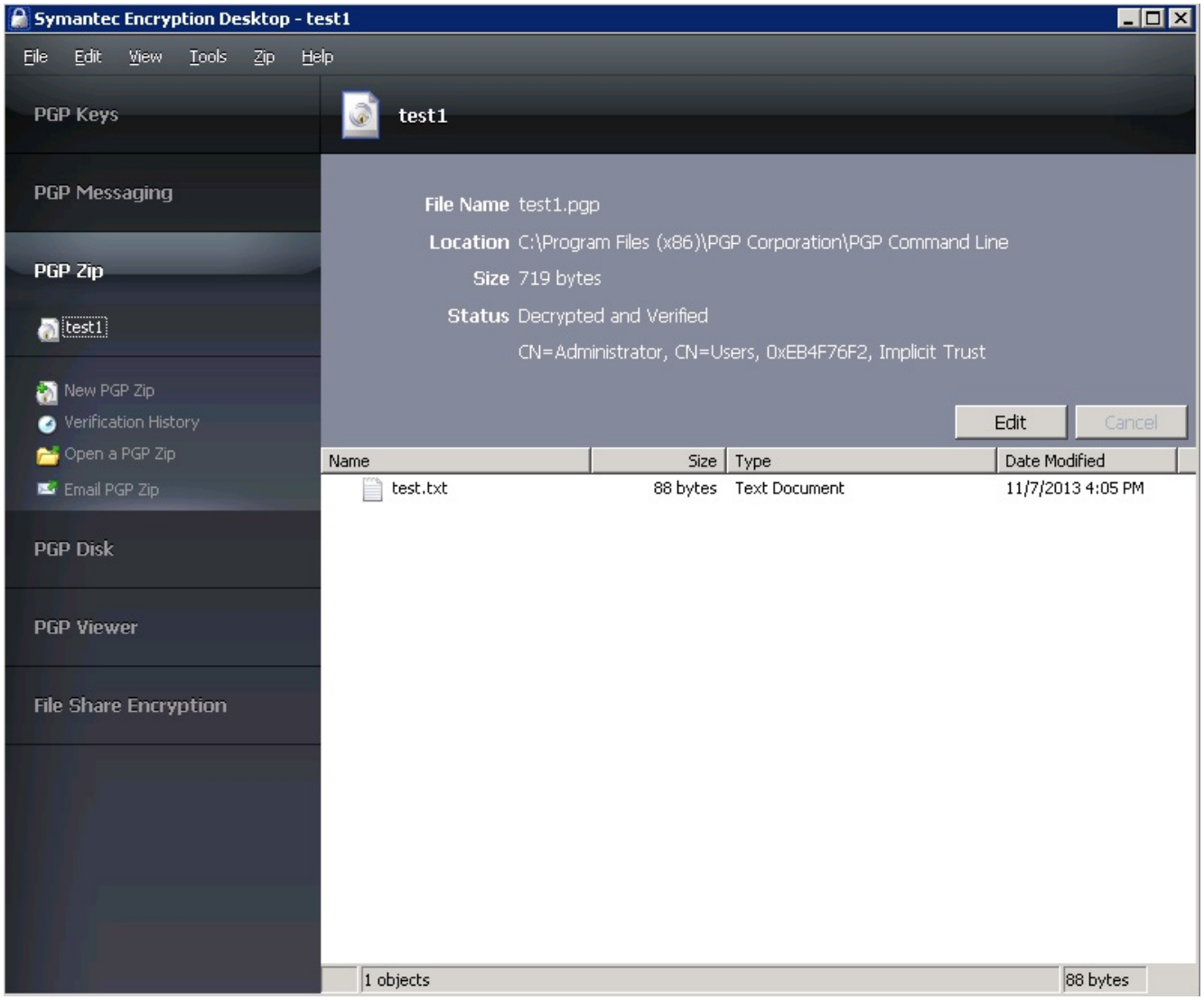


Verify the test1.txt and test.txt files contents which must be same. You can also use the Symantec Desktop Encryption for verifying the encrypted file using the PGP Zip option.

Open the Symantec Encryption Desktop and click on PGP Zip. Click on Open a PGP Zip



Browse the file test1.pgp and click Open. It will verify and decrypt the file using the keys available in key ring.



You can extract the file to verify the decrypted contents. It completes the PGP integration with Luna HSM.

CHAPTER 3
Integrating Open PGP with Luna (v5.2.1 or above)

Setting up Luna with Open PGP

To set up Luna HSM for Symantec Encryption Desktop and PGP Command Line, kindly perform the following steps:

Setting up Luna SA to use 32 bit CSP

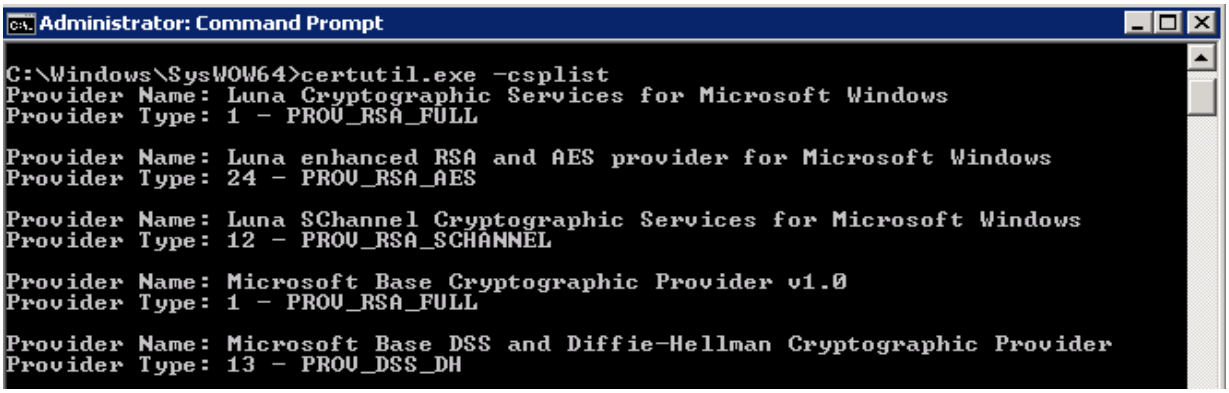
To set up Luna SA to use 32 bit CSP, perform the following steps on the system where you want to install the PGP:

1. Copy the “C:\Program Files\SafeNet\LunaClient\crystoki.ini” to “C:\Program Files\SafeNet\LunaClient\win32\crystoki.ini”
2. Edit the “C:\Program Files\SafeNet\LunaClient\win32\crystoki.ini” file and make the following changes:

   [Chrystoki2]

   LibNT=C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll
3. Click on Server Manger -> Change System Properties -> Advanced -> Environment Variables…
4. Under System Variables, select ChrystokiConfigurationPath and click Edit.
5. Enter the variable value as C:\Program Files\SafeNet\LunaClient\win32\ and click OK.
6. Click OK two more times to close the window.
7. Register the CSP as described in Before You Install section.
8. Run the following command to show that 32 bit CSP has been registered successfully.

   C:\Windows\SysWow64\certutil.exe -csplist



Setting up Luna SA for Active Directory Certificate Services

To set up Luna SA for Active Directory Certificate Services, kindly refer the Microsoft Active Directory Certificate Services Integration Guide with Luna SA. It is assumed that you have domain CA installed and the PGP machine is already joined this domain.

1. Configuring the CA to issue PGP User Certificate

Configuring a CA to create a certificate template and issuing properties for PGP user certificate.

1.1 Configuring certificate templates for your test environment

a) Log on to CA system as a domain administrator.

b) From the Start menu, select Run.

c) In the Run dialog, type mmc and click OK.

d) In the mmc console that appears, select File > Add/Remove Snap-in…

e) In the Add or Remove Snap-Ins dialog box, find the Certificate Templates snap-in (under the Available snap-ins section) and select it.

f) Click Add, and then click OK.

g) Under Console Root, expand the Certificate Templates snap-in. Listed in the middle section will be all the available certificate templates that you can make your CA issue.

h) Scroll down the list until you locate the User template, right-click and click Duplicate Template.

i) Select Windows Server 2003 Enterprise and click OK.

j) In the pop-up dialog that appears, click the General tab.

k) Enter the Template Display Name for example PGP User here and select Publish Certificate in Active Directory.

l) Click the Request Handling tab.

m) Click on CSPs and select Request can use any CSP available on subject's computer.

n) Click OK to close the window.

o) Click the Subject Name tab.

p) Uncheck E-mail name in subject name and E-mail name check boxes.

q) Click the Security tab.

r) Add and provide the Read and Enroll permissions to the following:

- Authenticated Users
- Administrator

s) For Domain Admins and Enterprise Admins, make sure that Read, Write, and Enroll check boxes are ticked.

t) Click Apply and then OK.

1.2 Configuring the CA to support the PGP certificate template

a) Log on to system as a domain administrator.

b) From the Start menu select Control Panel > Administrative Tools > Certification Authority.

c) In the console tree (left-hand section), expand the CA. (It has a computer and a green tick next to it.)

d) In console tree of the Certification Authority snap-in, right-click Certificate Templates, and then click New Certificate Templates to Issue.

e) In Enable Certificates Templates, select the PGP User template and any other certificate templates you configured previously, and then click OK.

f) Open Certificate Templates in the Certification Authority and verify that the modified certificate templates appear in the list.

Creating a key and requesting a certificate

a) Log on to PGP system as a domain administrator.

b) From the Start menu, select Run.

c) In the Run dialog, type cmd and click OK.

d) Type “C:\Winodws\SysWow64\certmgr.msc” and hit Enter.

e) In the mmc console that appears, right click on the Personal folder and select All Tasks -> Request New Certificate…

f) Click Next, Select Active Directory Enrollment Policy and then click Next. It will show you the certificate template you have configured, i.e. PGP User

g) Click on Details and then Properties.

h) Certificate Properties window will open and select the Subject tab.

i) Select Common Name under Subject Name and provide the fully qualified domain name for the computer on which you are installing the certificate in the Value field and click Add. Repeat the same step for adding more values.

j) Click on General tab and provide the Friendly Name. For example PGP User.

k) Click on Private Key tab, and verify that Luna Cryptographic Services for Microsoft Windows must be selected under the Cryptographic Service Provider.

l) Click on Certificate Authority tab, and make sure that Enterprise Root CA is selected.

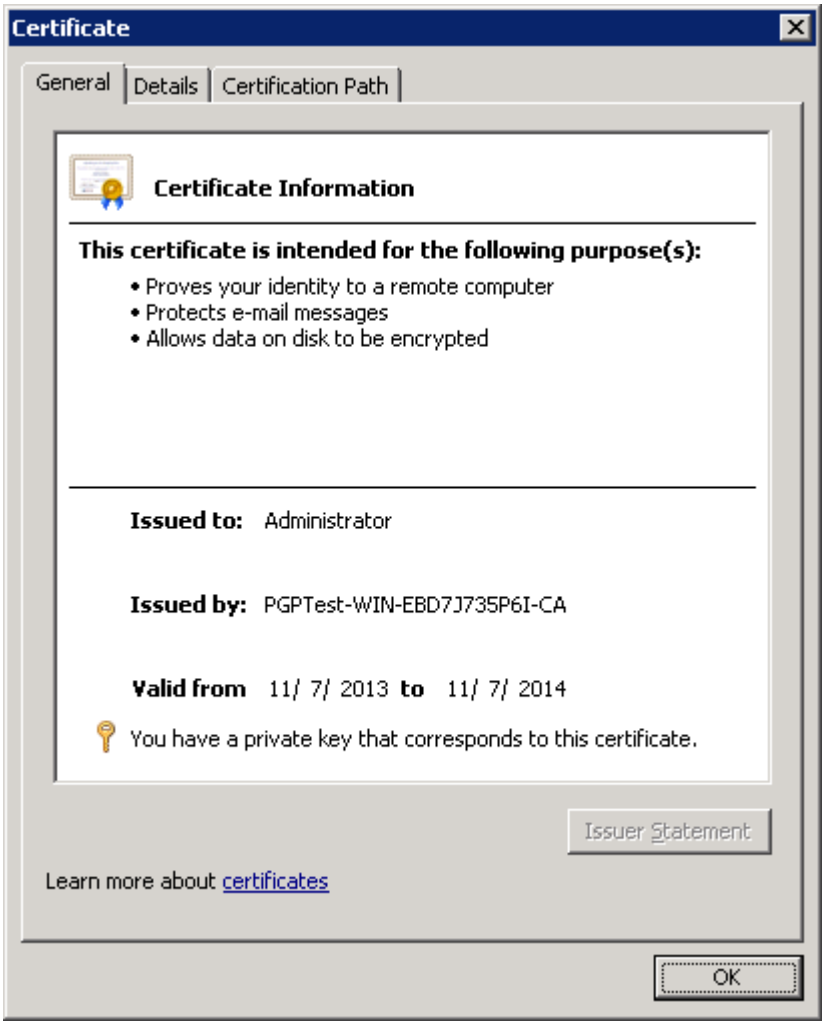
m) Click Apply and then OK.

n) Select PGP User certificate template or the certificate template you have configured, and click Enroll.

o) It will take some time to enroll, when enrollment succeeded, click Finish.

p) Make sure that certificate is now available in the Personal -> Certificate store.

q) Double click on the certificate and see that “You have a private key that corresponds to this certificate”.



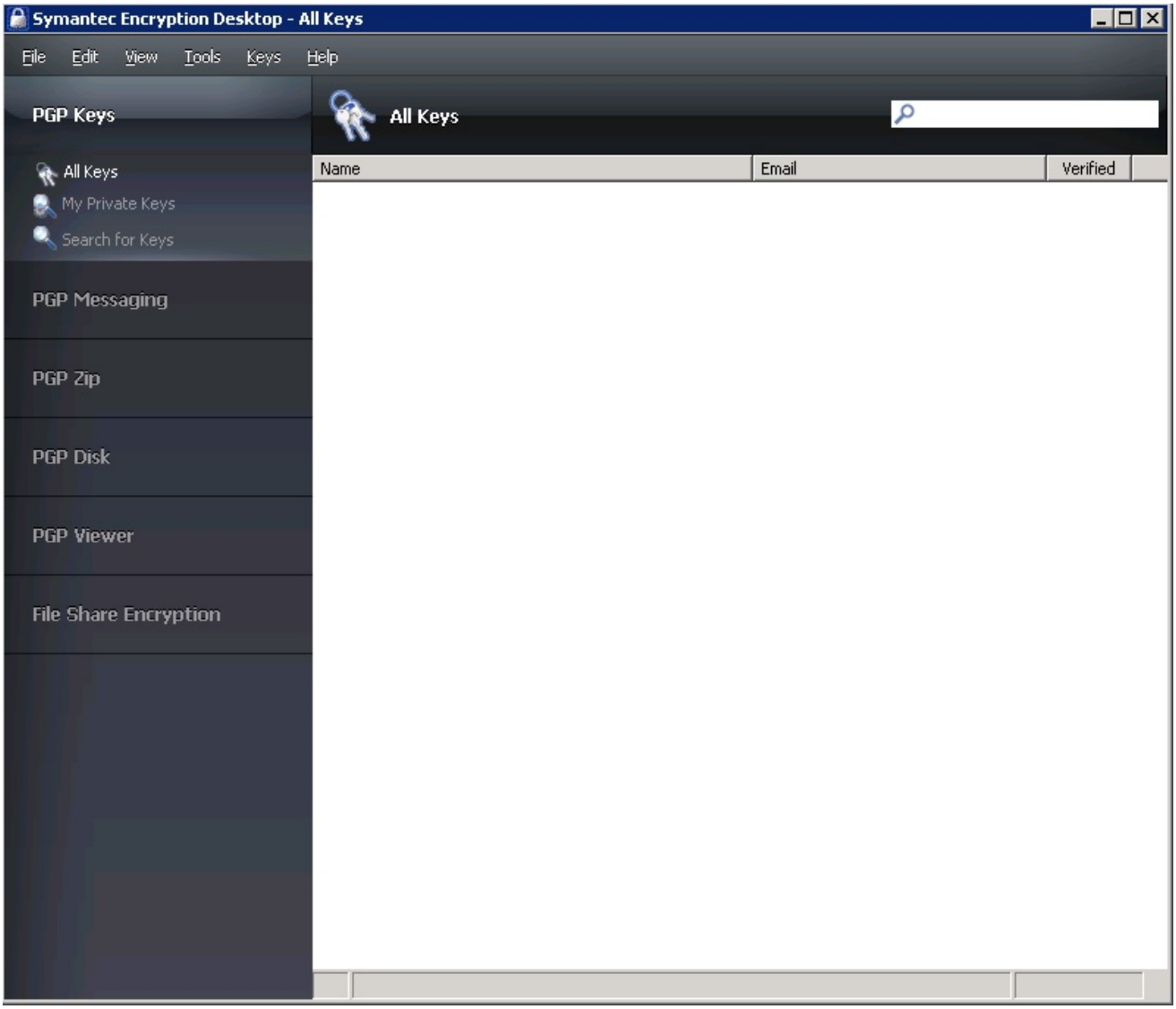
The keys for this certificate will be generated on Luna HSM box. You can see the contents on Luna SA box.

2. Configuring PGP applications to use available keys

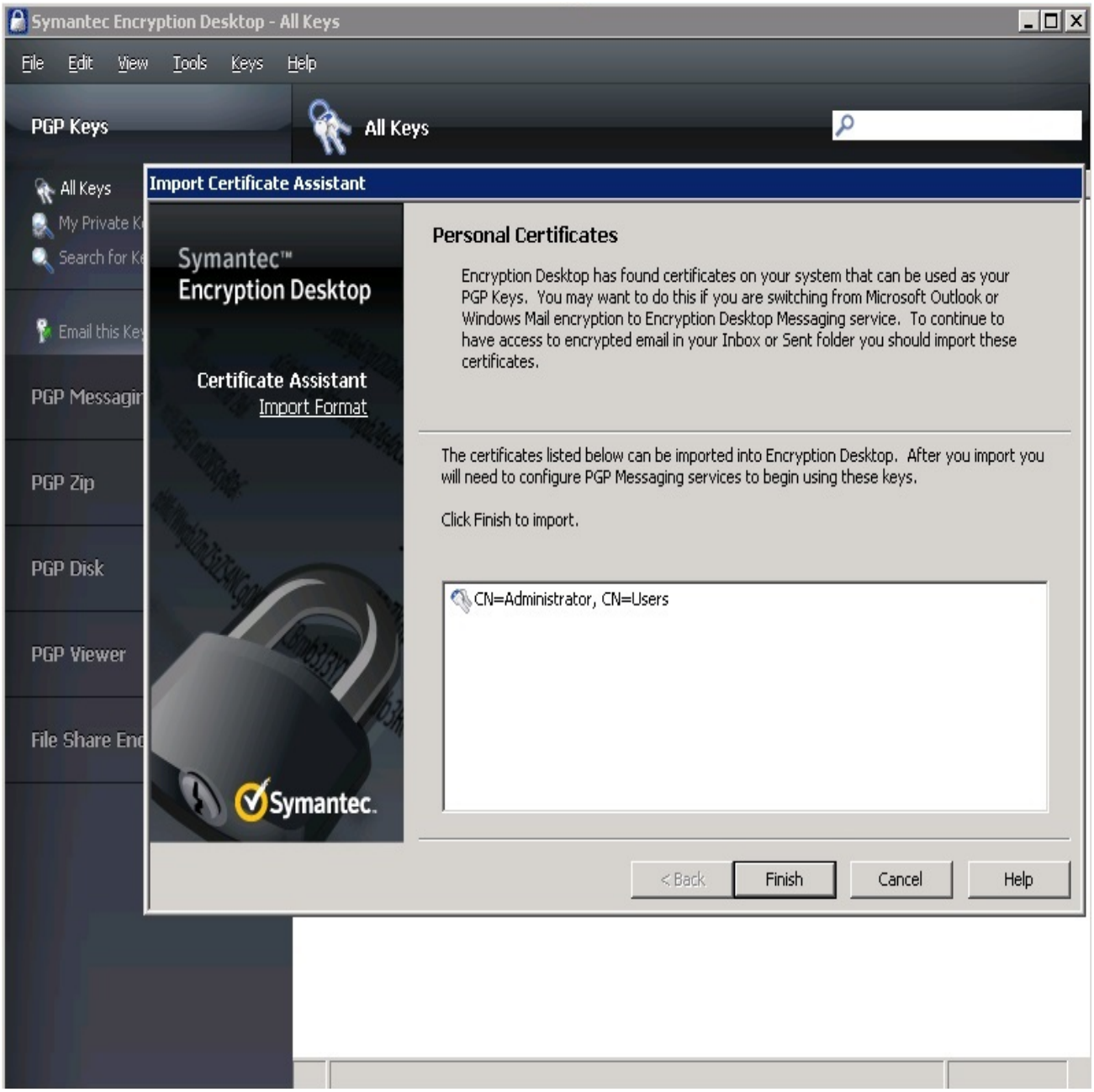
The first step to be able to use the keys protected by the HSM with PGP Applications is to import them in the current key ring files using Encryption Desktop.

2.1 Import the keys in Symantec Encryption Desktop

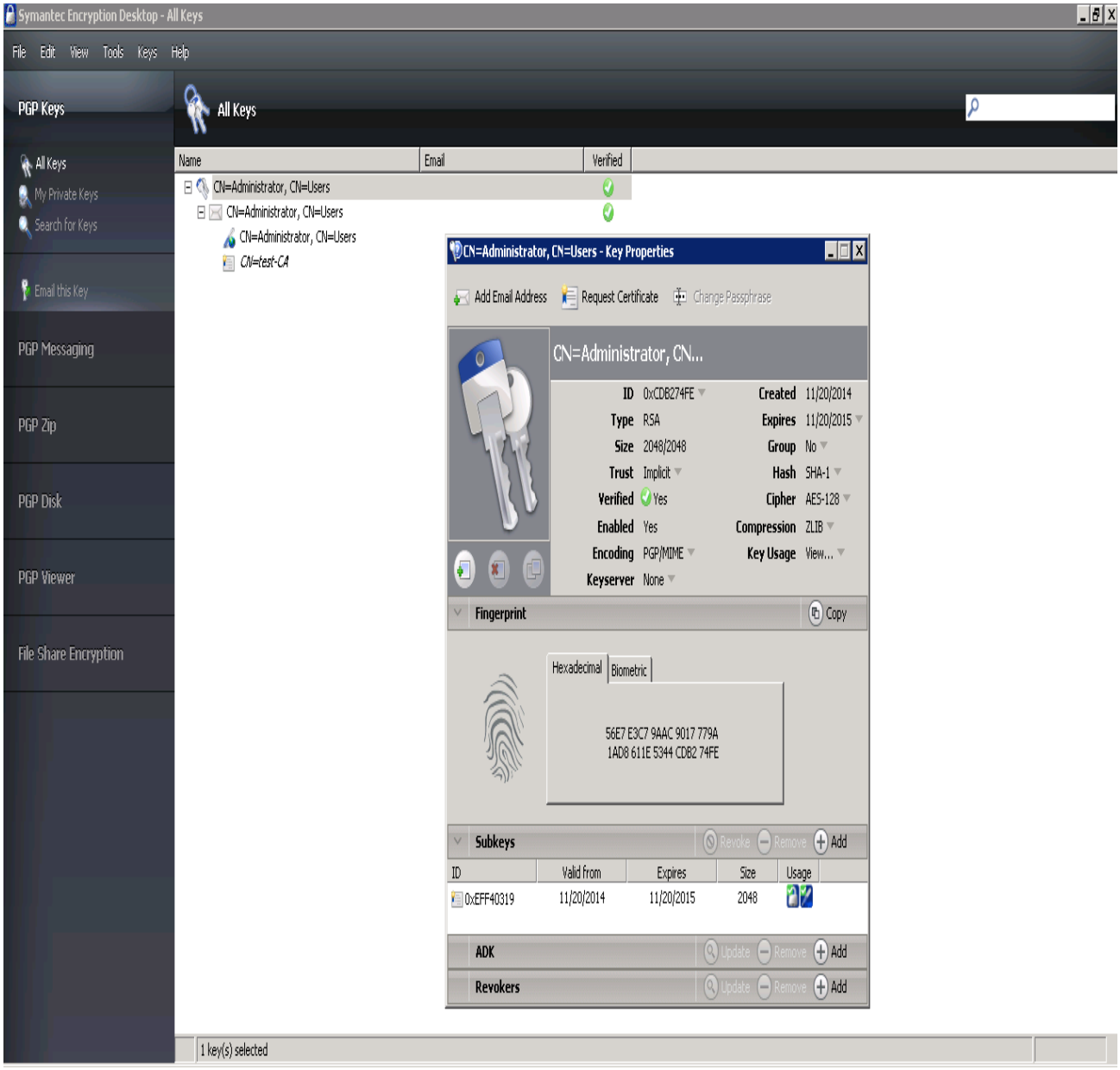
1. Open the Symantec Encryption Desktop and select PGP Keys on the left side of the window



2. From File menu choose “Import Personal Certificates“, click Finish.



3. Confirm the list of keys / certificates found to be imported into the PGP Key Ring. Double click to open the properties window to see the details.



4. The certificate protected by the HSM can now be used in all PGP Applications.

2.2 List the keys using PGP Command Line

After the keys / certificates were imported into the key ring, these can now be listed with PGP Command Line. To list the keys execute:

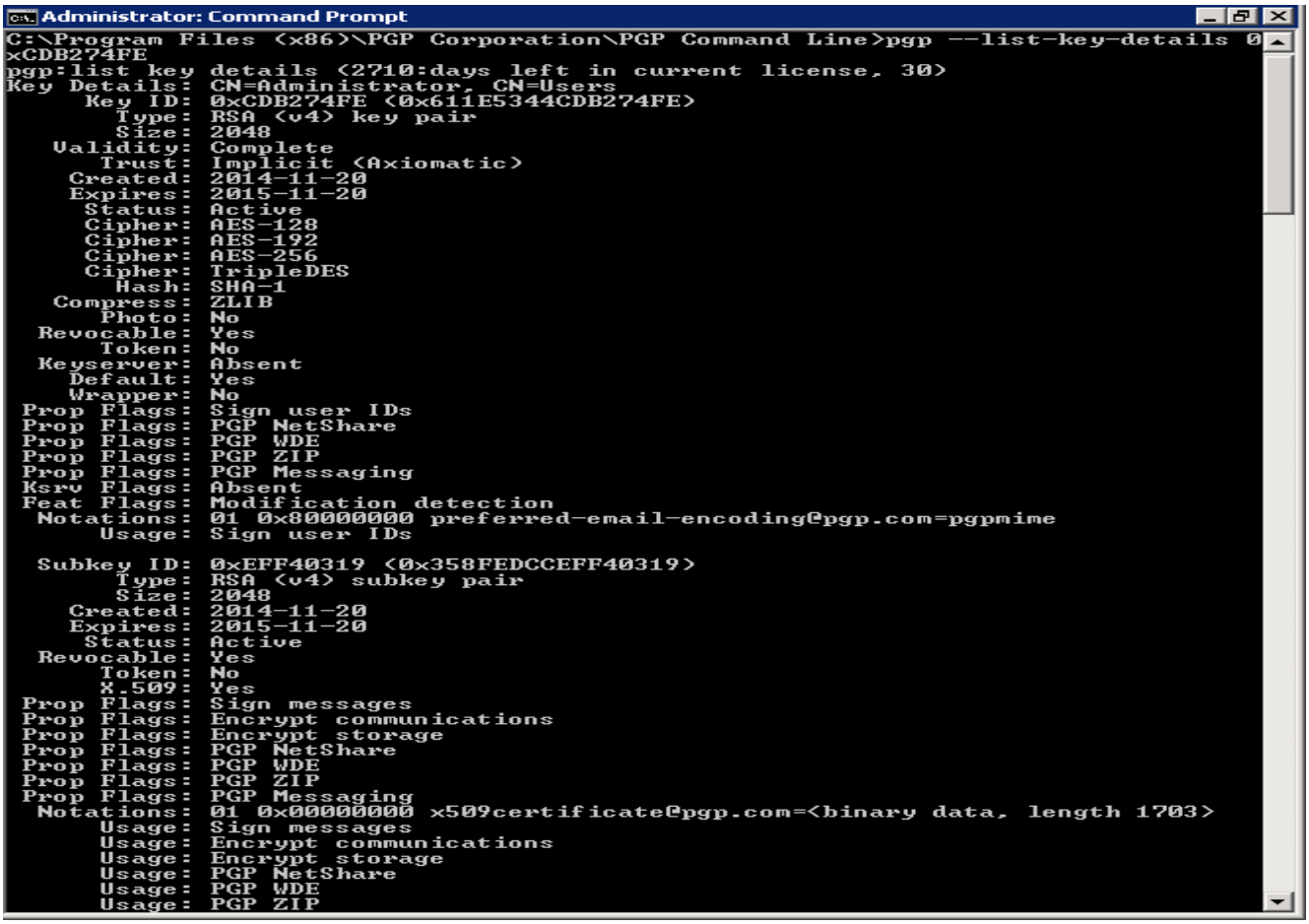
```
pgp --list-keys
```

This will show you all available keys for PGP Command Line

The keys protect by the HSM will show up as key pair since public and private part is available for PGP Command Line.

More details about a single key can be shown when executing:

```
pgp --list-key-details 0xCDB274FE
```

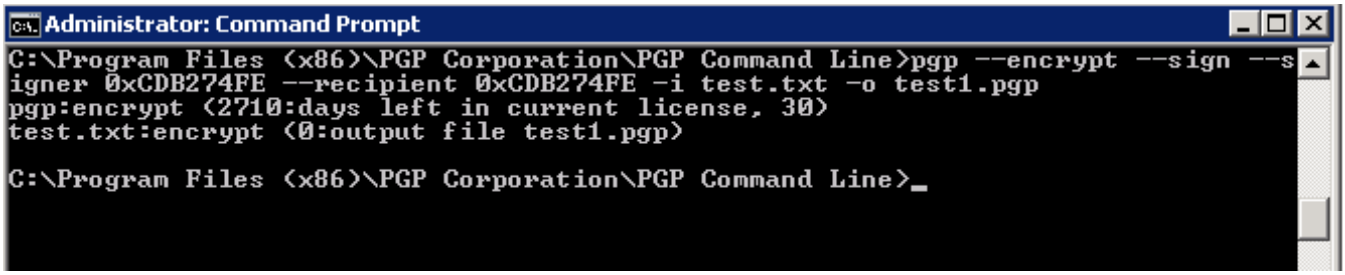


2.3 Using the keys with PGP Command Line

After these steps the keys protected by the HSM can be used in the same way as any other keys available in the PGP key ring.

To sign a file called “test.txt” with the key with ID 0xEB4F76F2 (stored on HSM) and encrypt it to a recipient with the key ID 0xXXXXXXXX execute the following command.

```
pgp --encrypt --sign --signer 0xCDB274FE --recipient 0xCDB274FE -i test.txt -o test1.pgp
```

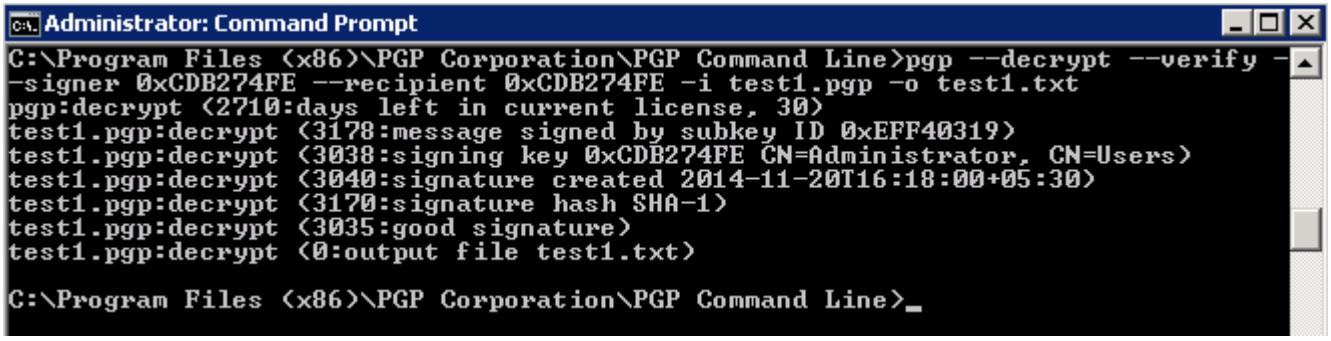


NOTE: We have used here same ID for signer and recipient both, for test purpose.

It will create the encrypted test1.pgp file in the current directory.

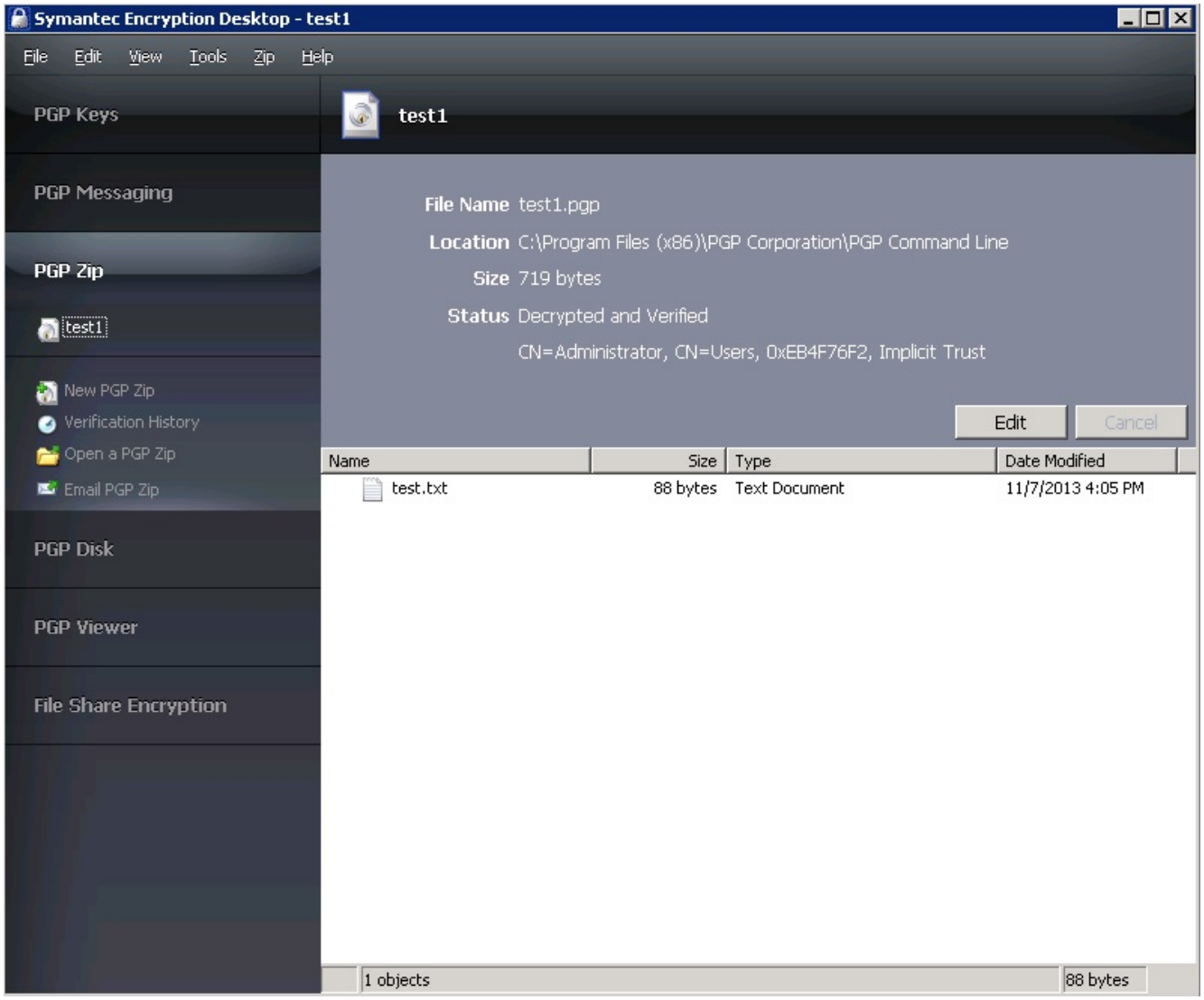
To verify an encrypted file called “test1.pgp” with the key with ID 0xEB4F76F2 (stored on HSM) and encrypt it to a recipient with the key ID 0xXXXXXXXX execute the following command.

```
pgp --decrypt --verify --signer 0xCDB274FE --recipient 0xCDB274FE -i test1.pgp -o test1.txt
```



Verify the test1.txt and test.txt files contents which must be same. You can also use the Symantec Desktop Encryption for verifying the encrypted file using the PGP Zip option.

Open the Symantec Encryption Desktop and click on PGP Zip. Click on Open a PGP Zip. Click on Open a PGP Zip and select the file test1.pgp and click Open. It will verify and decrypt the file using the keys available in key ring.



You can extract the file to verify the decrypted contents. It completes the PGP integration with Luna HSM.