SSL RENEWAL PROCESS

Step1:

Create a certificate request CSR and private key.

Step2:

After sharing CSR file with vendor, we will get .ZIP file containing 3 certificates

- Intermediate certificate: CA_emSign SSL CA - G1.cer
- Domain certificate: EndEntity_wc.piramalswasthya.org.cer
- Root certificate: RootCA_emSign Root CA - G1.cer

Combine three certificates in to single cert file (add each cert in new line and add empty line at the end) using notepad.

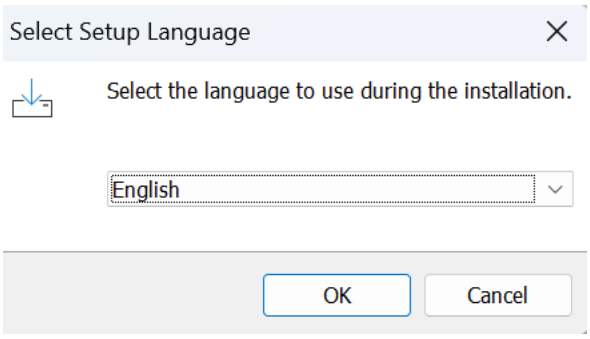
Save the certificate chain as wildcard.crt.

already have private key - wildcard_key.key

Step3:

To Generate *.jks file using two files newcert.crt and wildcard_key.key

Download and install Keystore Explorer here. https://keystore-explorer.org/downloads.html



KeyStore Explorer Setup [5.5.3]

Welcome to the KeyStore Explorer Setup Wizard

This will install KeyStore Explorer version 5.5.3 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Next | Cancel

KeyStore Explorer Setup [5.5.3]

Select Destination Location

Where should KeyStore Explorer be installed?

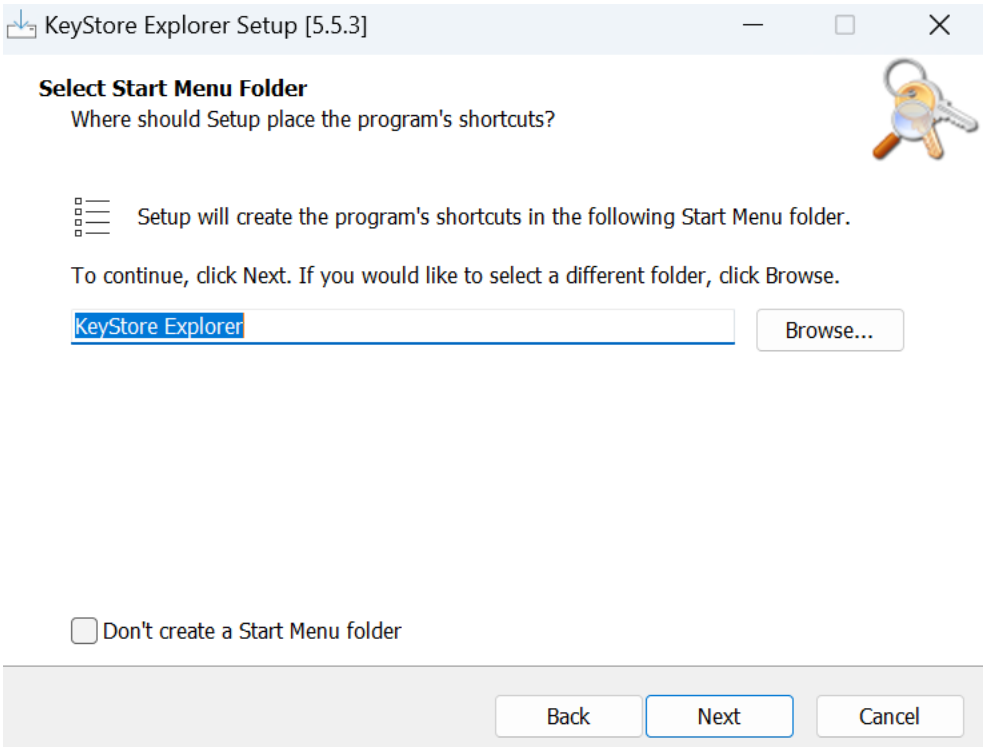
Setup will install KeyStore Explorer into the following folder.

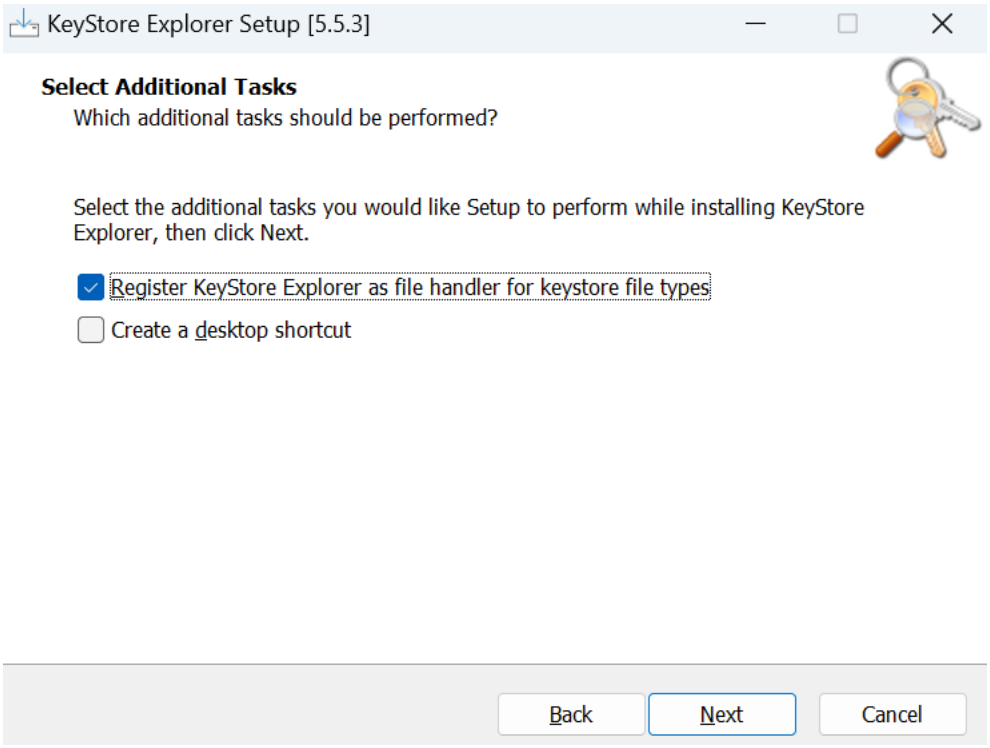
To continue, click Next. If you would like to select a different folder, click Browse.

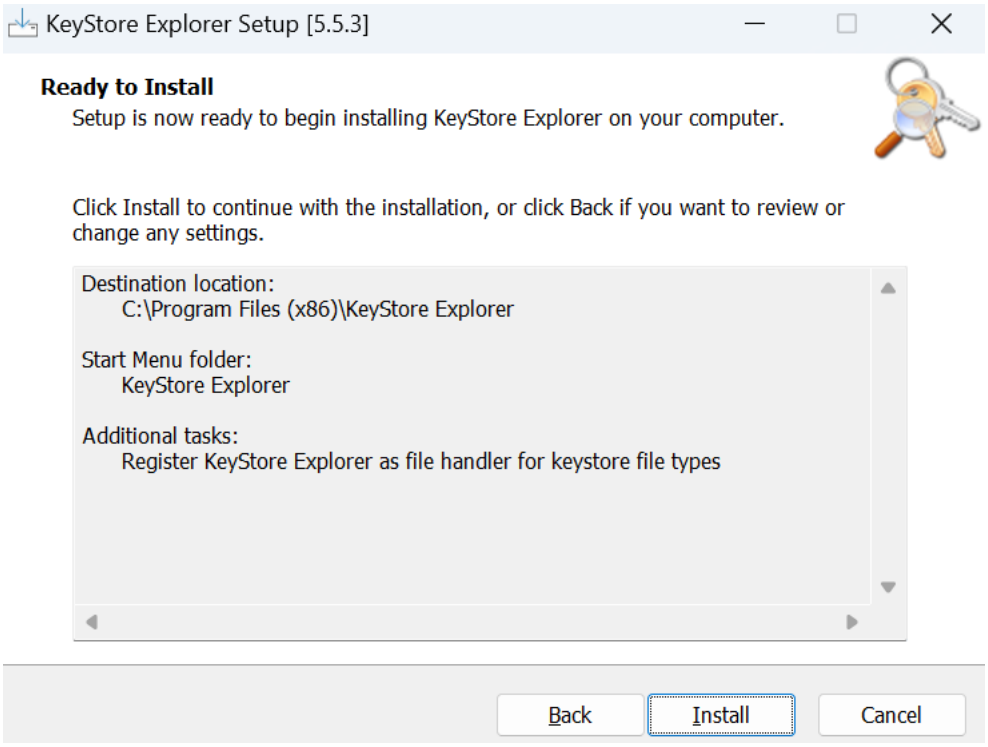
C:\Program Files (x86)\KeyStore Explorer | Browse...

At least 69.8 MB of free disk space is required.

Back | Next | Cancel

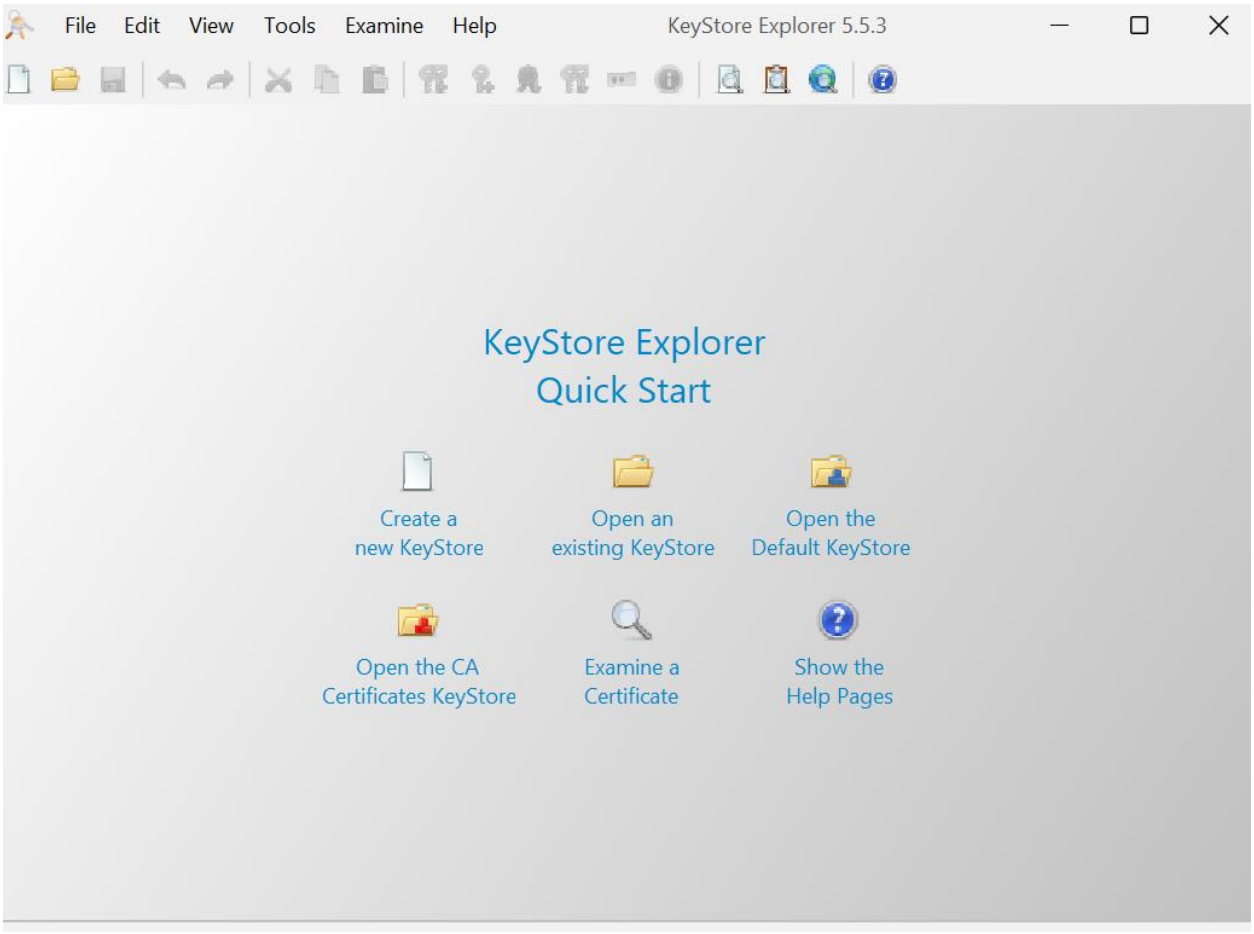

KeyStore Explorer Setup [5.5.3]
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
KeyStore Explorer
Browse...
Don't create a Start Menu folder
Back
Next
Cancel


KeyStore Explorer Setup [5.5.3]
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing KeyStore Explorer, then click Next.
Register KeyStore Explorer as file handler for keystore file types
Create a desktop shortcut
Back
Next
Cancel

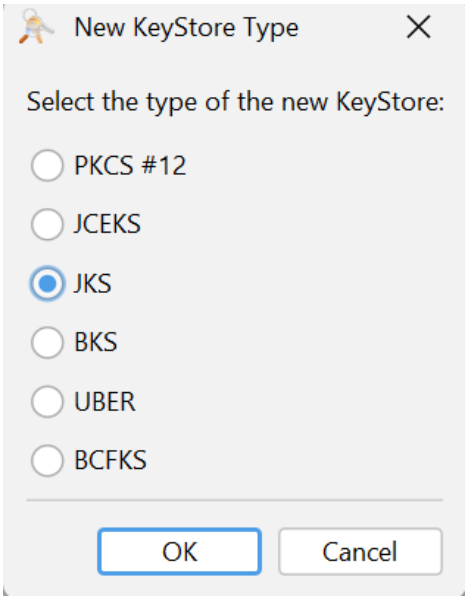

KeyStore Explorer Setup [5.5.3]
Ready to Install
Setup is now ready to begin installing KeyStore Explorer on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files (x86)\KeyStore Explorer
Start Menu folder:
KeyStore Explorer
Additional tasks:
Register KeyStore Explorer as file handler for keystore file types
Back
Install
Cancel

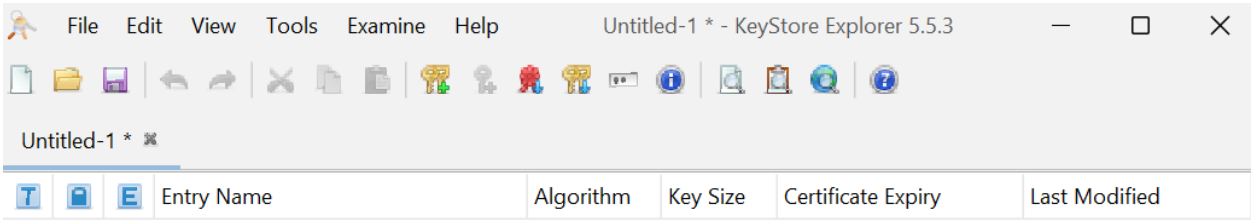

KeyStore Explorer Setup [5.5.3]
Completing the KeyStore Explorer Setup Wizard
Setup has finished installing KeyStore Explorer on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Launch KeyStore Explorer
Finish

Open Keystore Explorer



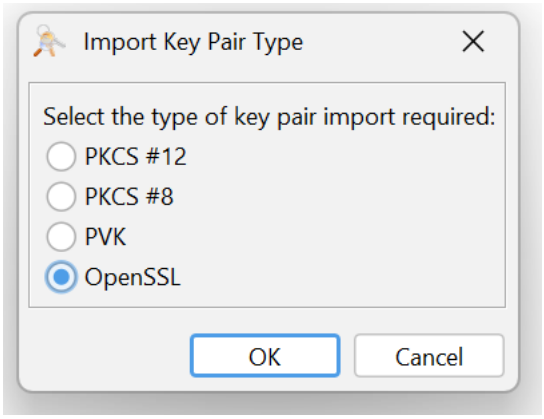
Click on create New key store

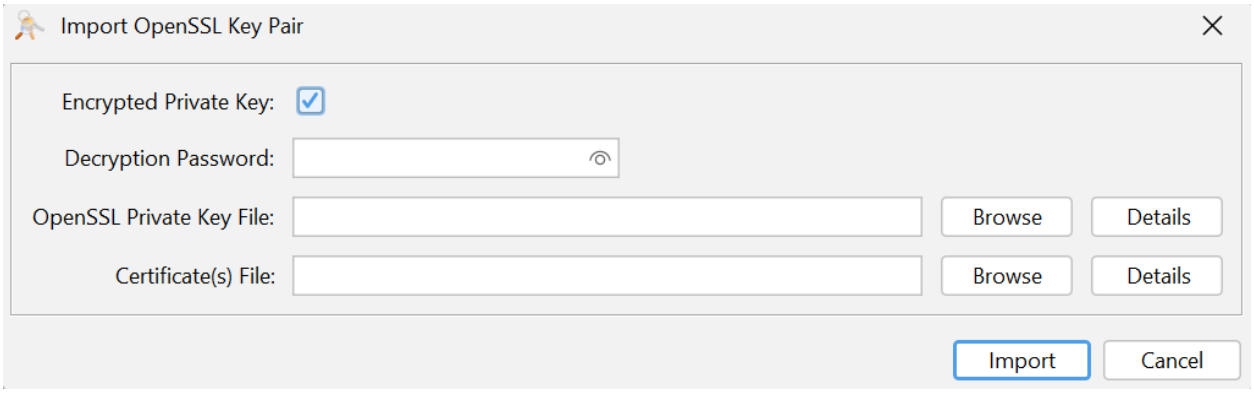


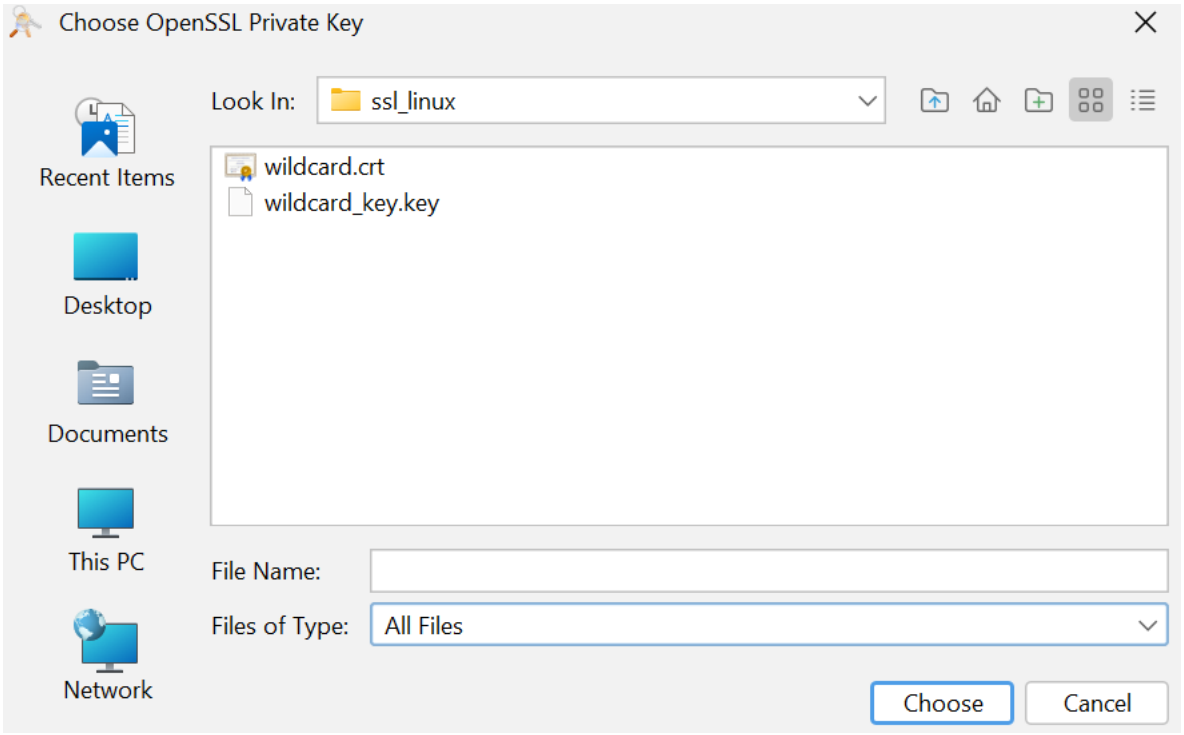


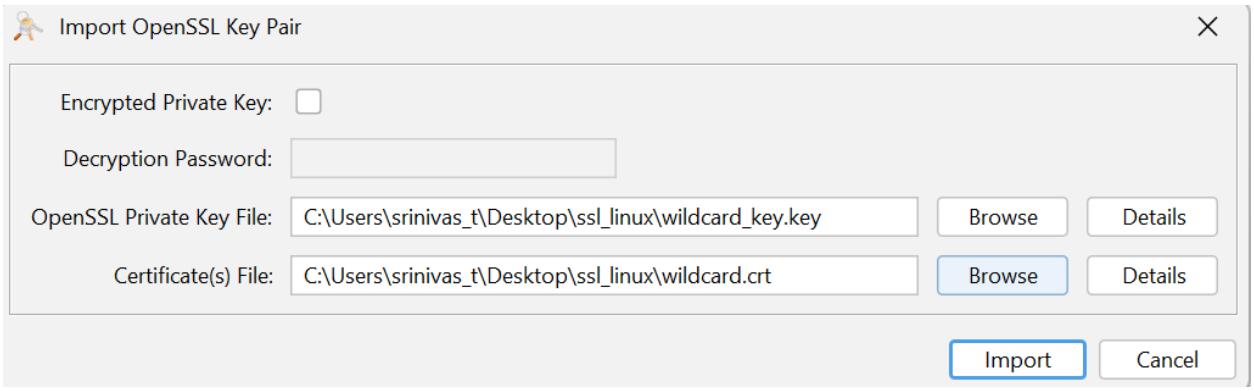
Click on import key pair.

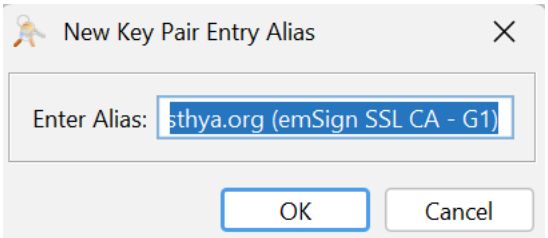
Select OpenSSL



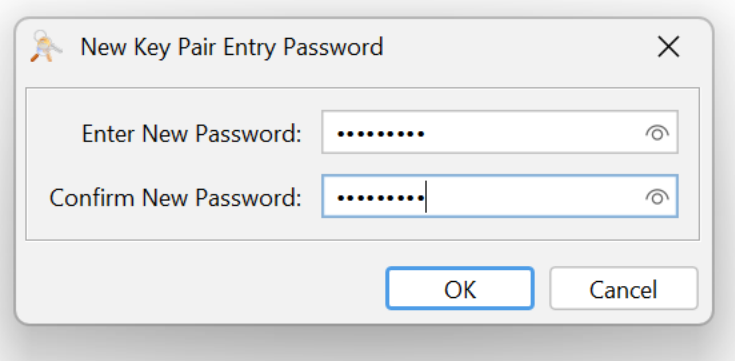

Import OpenSSL Key Pair
Encrypted Private Key:
Decryption Password:
OpenSSL Private Key File:
Browse
Details
Certificate(s) File:
Browse
Details
Import
Cancel

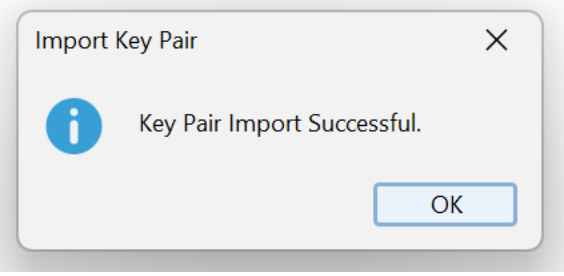

Choose OpenSSL Private Key
Look In:
ssl_linux
Recent Items
Desktop
Documents
This PC
Network
wildcard.crt
wildcard_key.key
File Name:
Files of Type:
All Files
Choose
Cancel

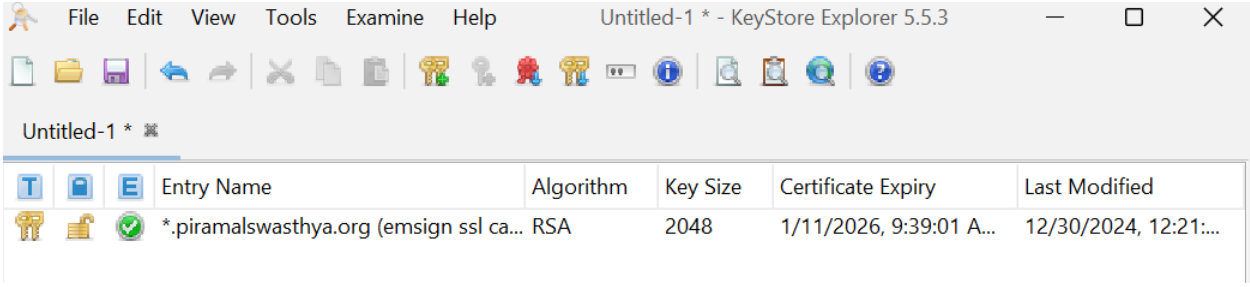

Import OpenSSL Key Pair
Encrypted Private Key:
Decryption Password:
OpenSSL Private Key File:
C:\Users\srinivas_t\Desktop\ssl_linux\wildcard_key.key
Browse
Details
Certificate(s) File:
C:\Users\srinivas_t\Desktop\ssl_linux\wildcard.crt
Browse
Details
Import
Cancel



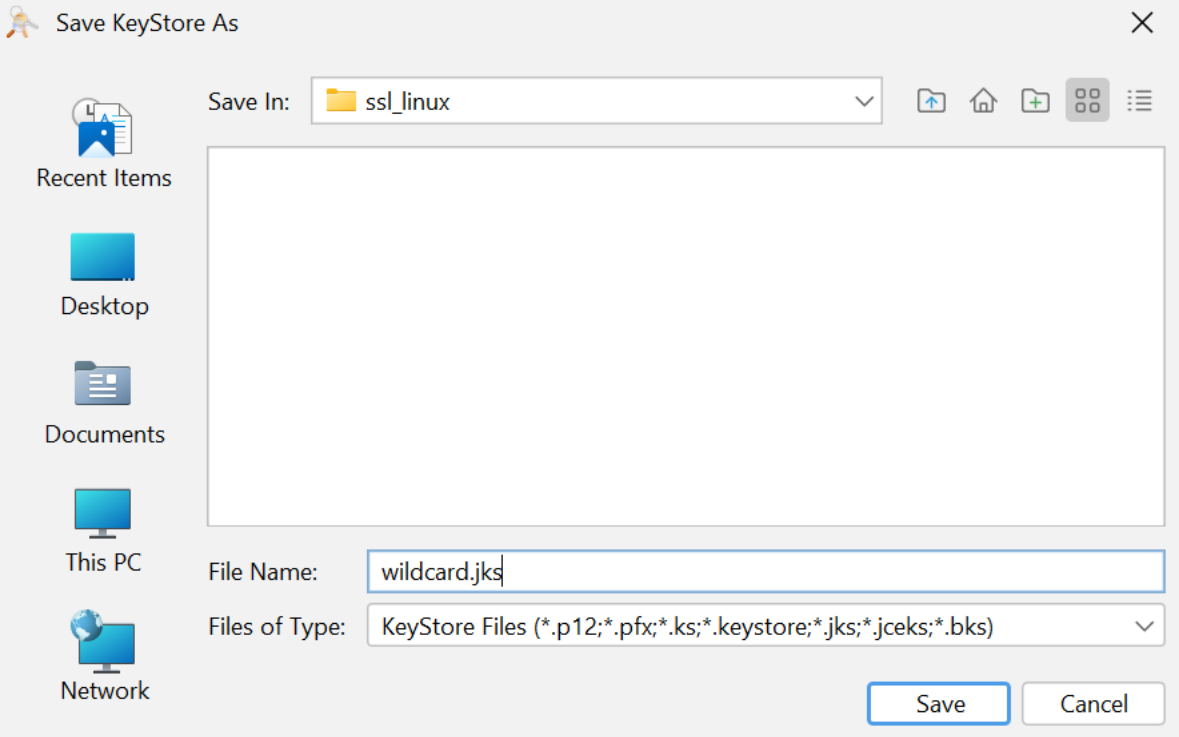
*.piramalswasthya.org (emSign SSL CA - G1)







Click on save



In Windows: only one file is required (*.jks)

In Linux: two files required (*.crt and *.key)

Standalone.xml changes:

For Godaddy:

<key-managers>

<key-manager name="applicationKM" key-store="applicationKS" generate-self-signed-certificate-host="*.piramalswasthya.org (go daddy secure certificate authority - g2)">

<credential-reference clear-text="******"/>

</key-manager>

</key-managers>

For E-mudra:

<key-managers>

<key-manager name="applicationKM" key-store="applicationKS" generate-self-signed-certificate-host="*.piramalswasthya.org (emSign SSL CA - G1)">

<credential-reference clear-text="******"/>

</key-manager>

</key-managers>

Step 5:

Stop wildlfy and then stop redis

Update the jks file under wildlfy configuration folder.

Start redis and then start wildfly.