08. OCID - Renew certificates

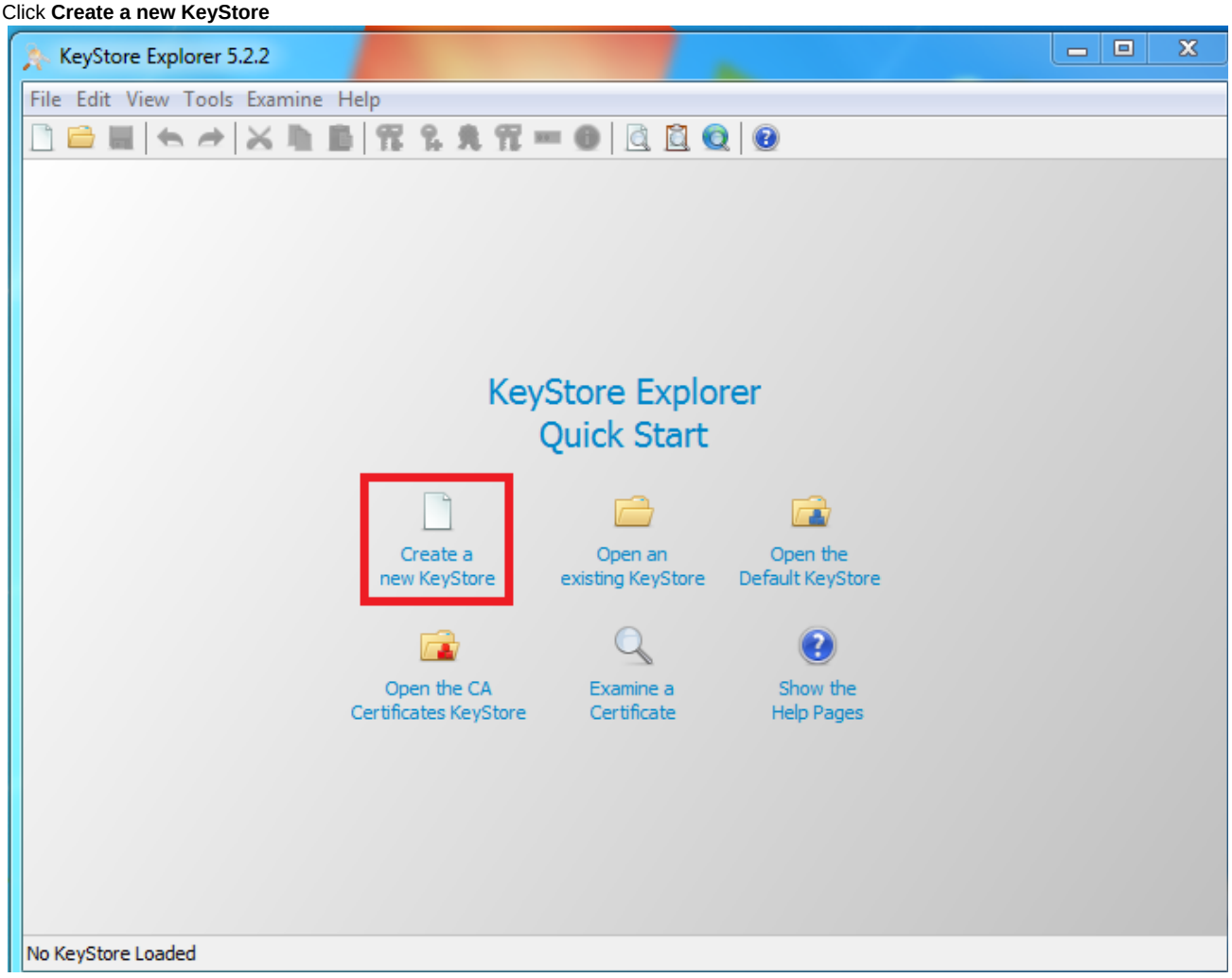
Description

This article describes how to create a new certificate used in project OneCustomerId for contact with PingOne and PingFederate.

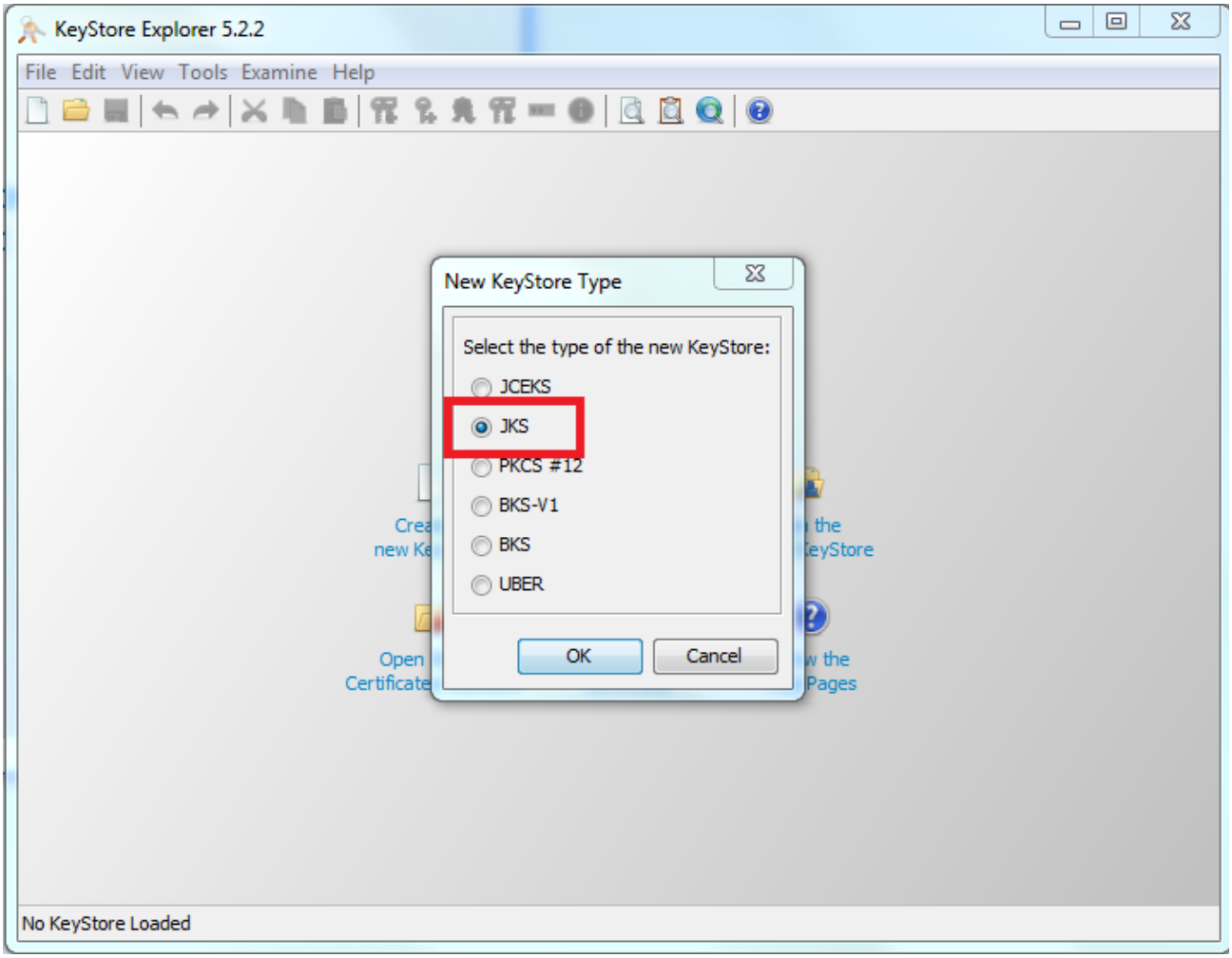
Create certificate steps

To create a certificate, perform the following steps:

1. (Optional) Download and install tool ***KeyStore Explorer***
   You can download this tool using following link: http://keystore-explorer.org/
2. Click **Create a new KeyStore**

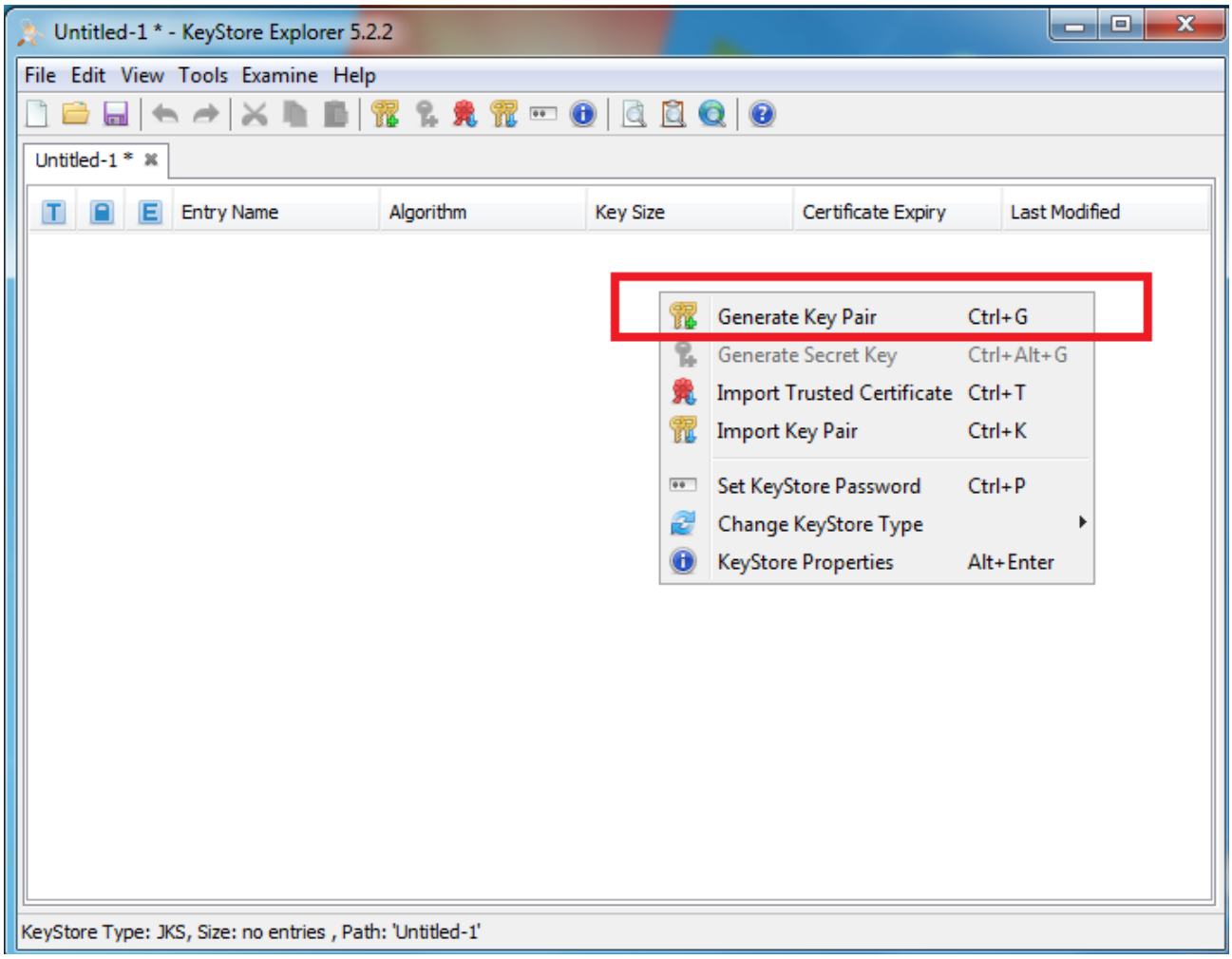


3. In the New KeyStore Type popup, select **JKS**, and click **OK**.

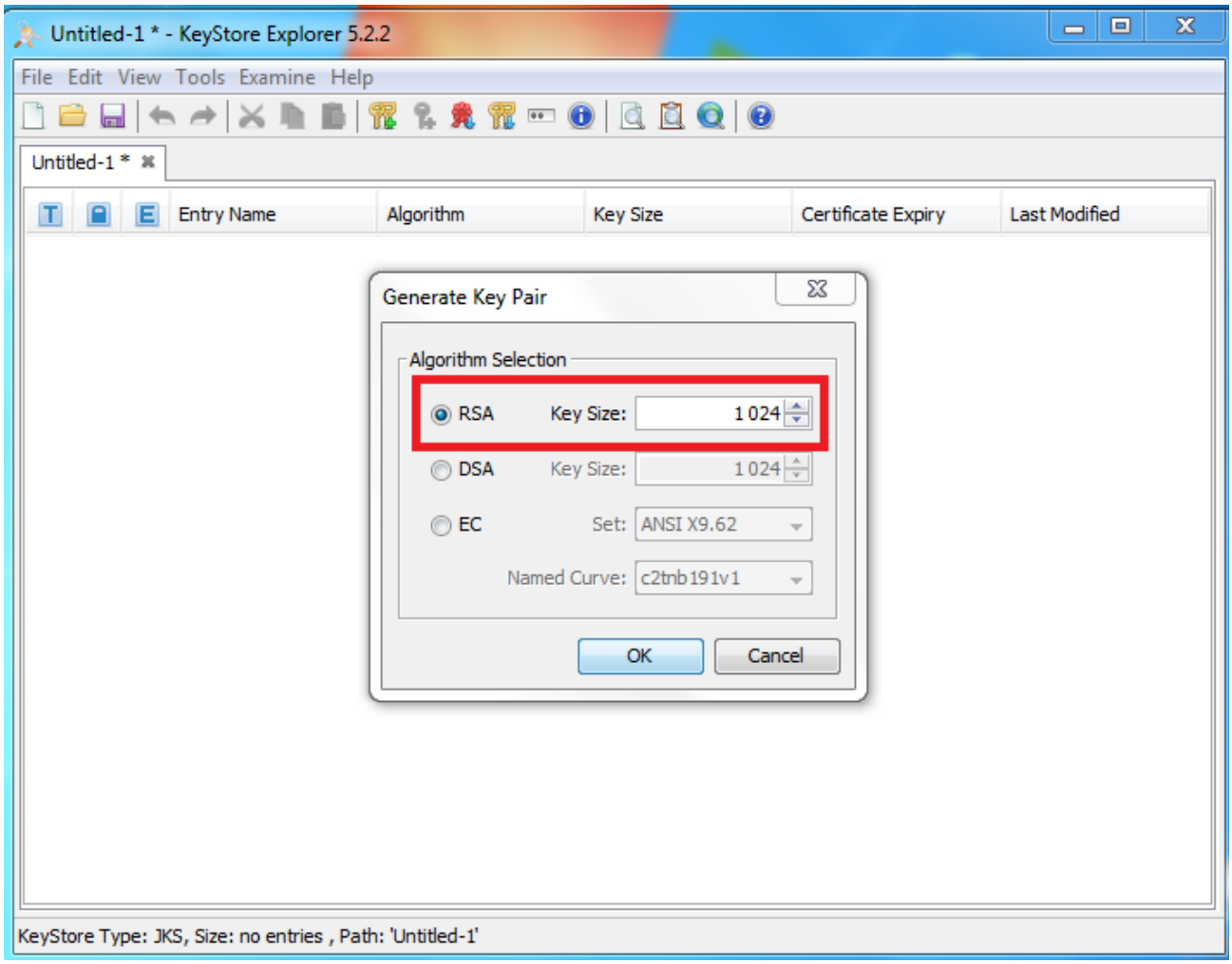


You are taken to the new Keystore window.

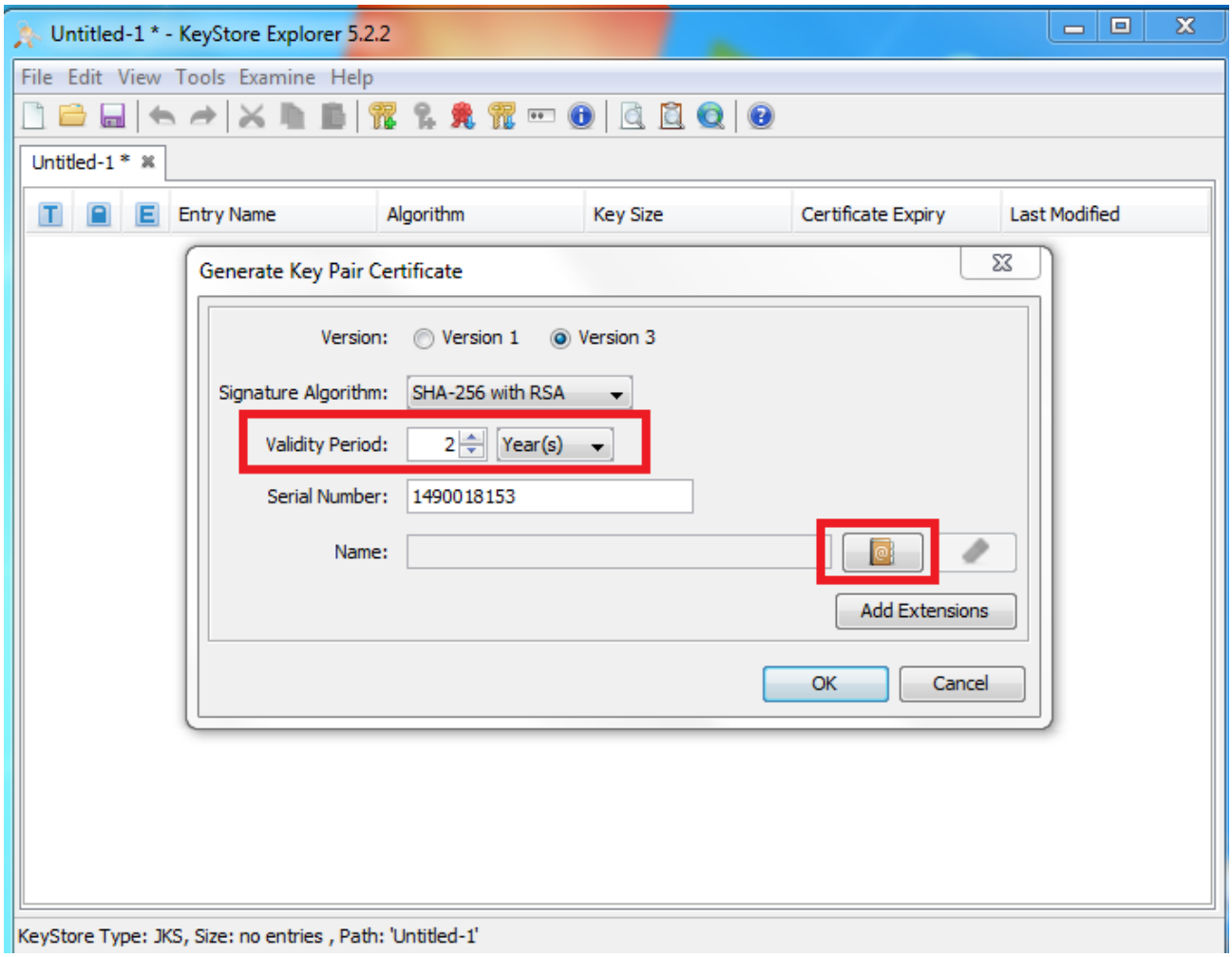
4. Click the right mouse button and choose **Generate Key Pair**.



5. Select algorithm **RSA** and click **OK**.

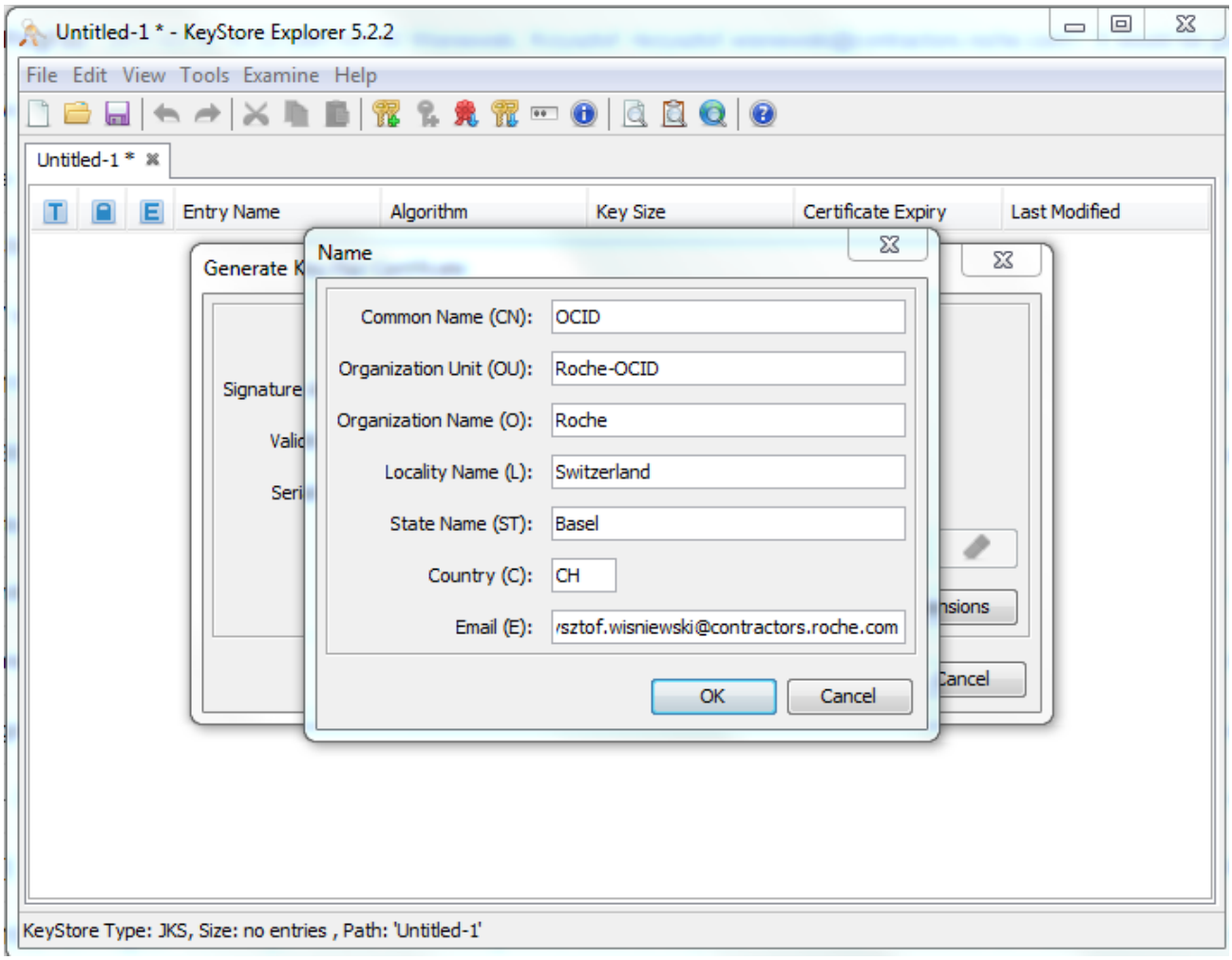


6. Validity Period
   Choose a validity period of **2 Years**. To enter a certificate name in the Name field, press the highlighted button.

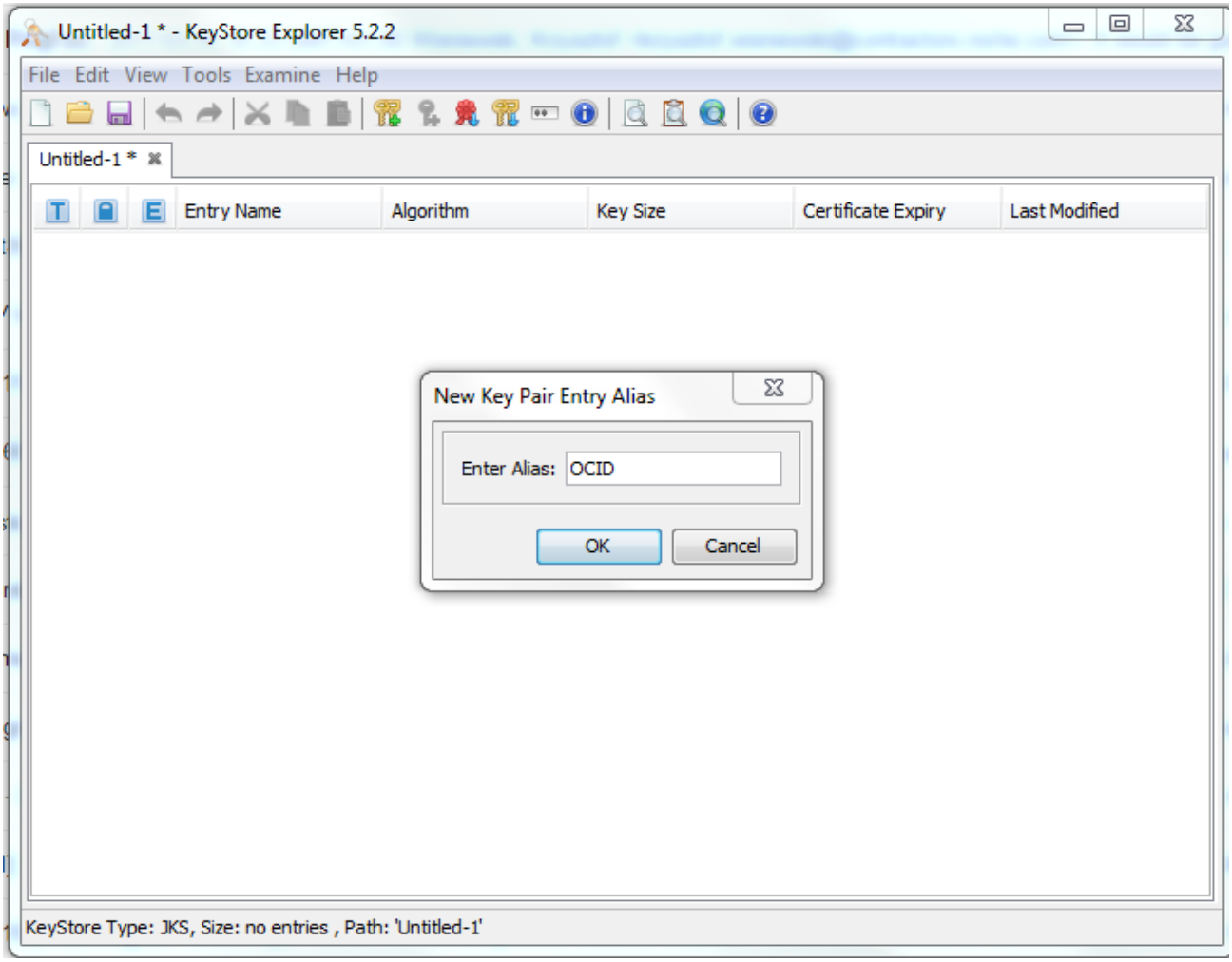


The Name popup window displays.

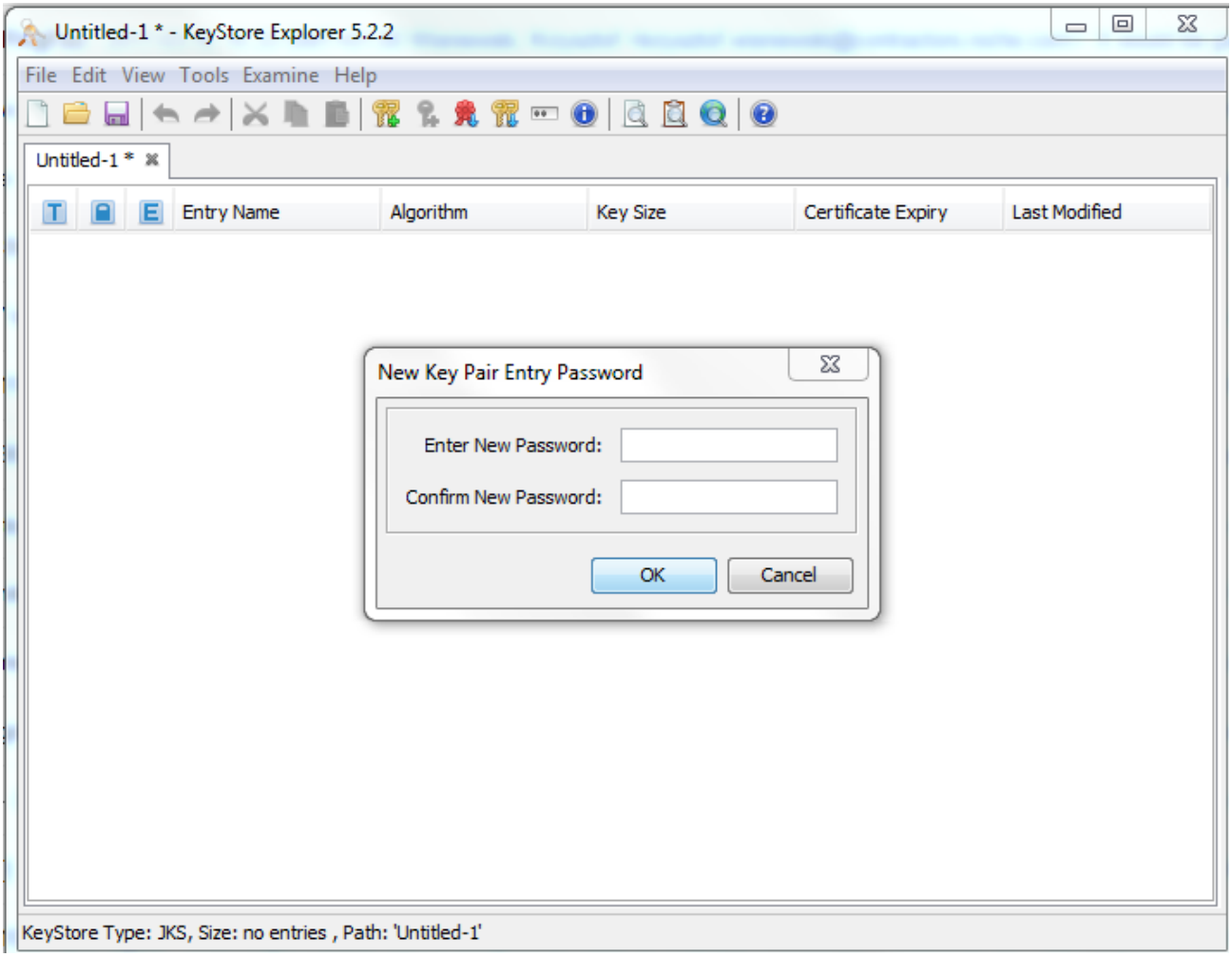
7. Enter the required information in the certificate name fields, then click **OK**.



8. Enter an Alias.

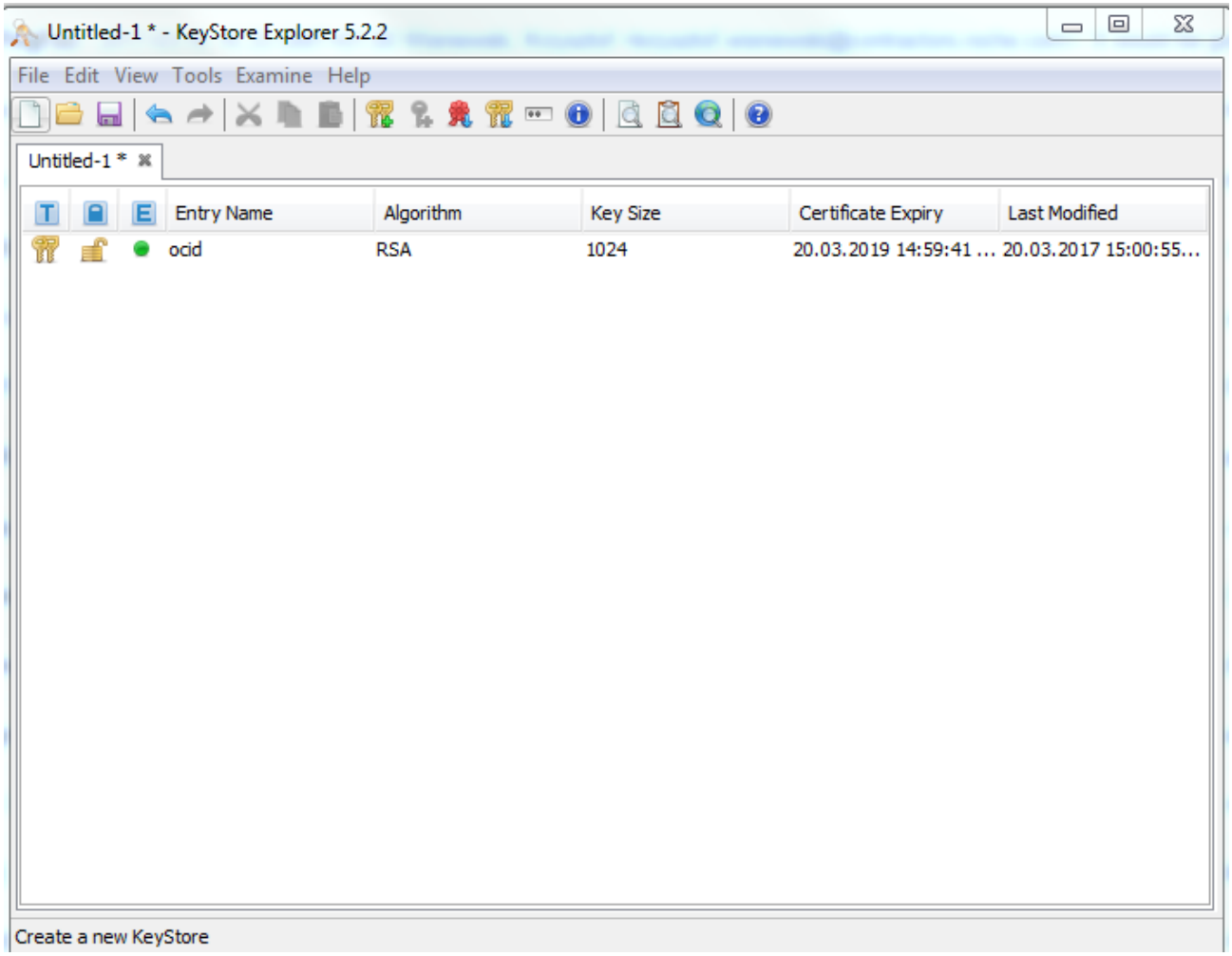


9. Enter a Private Key Password in the provided fields, then click **OK**.

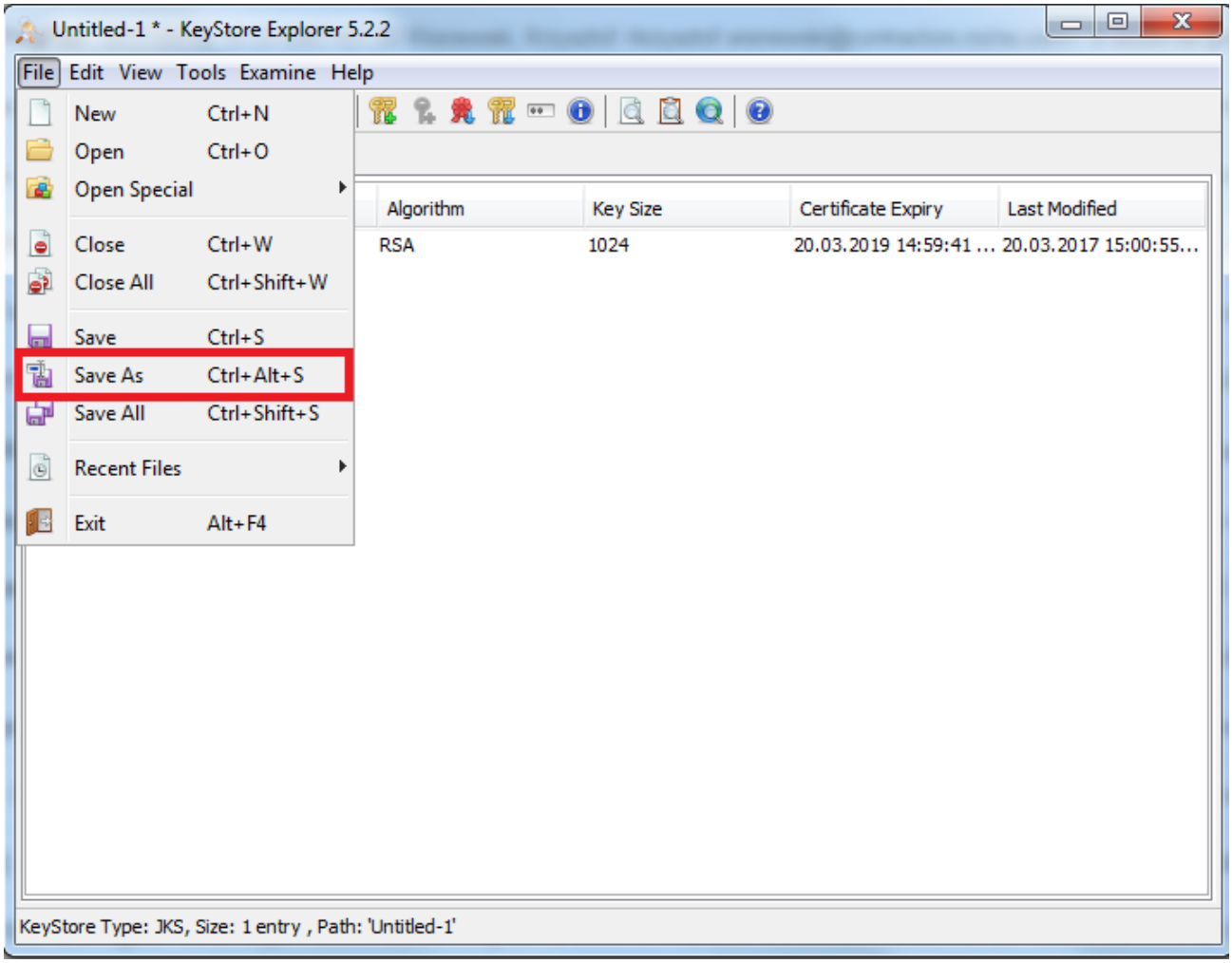


The new Entry is listed in the KeyStore Explorer.

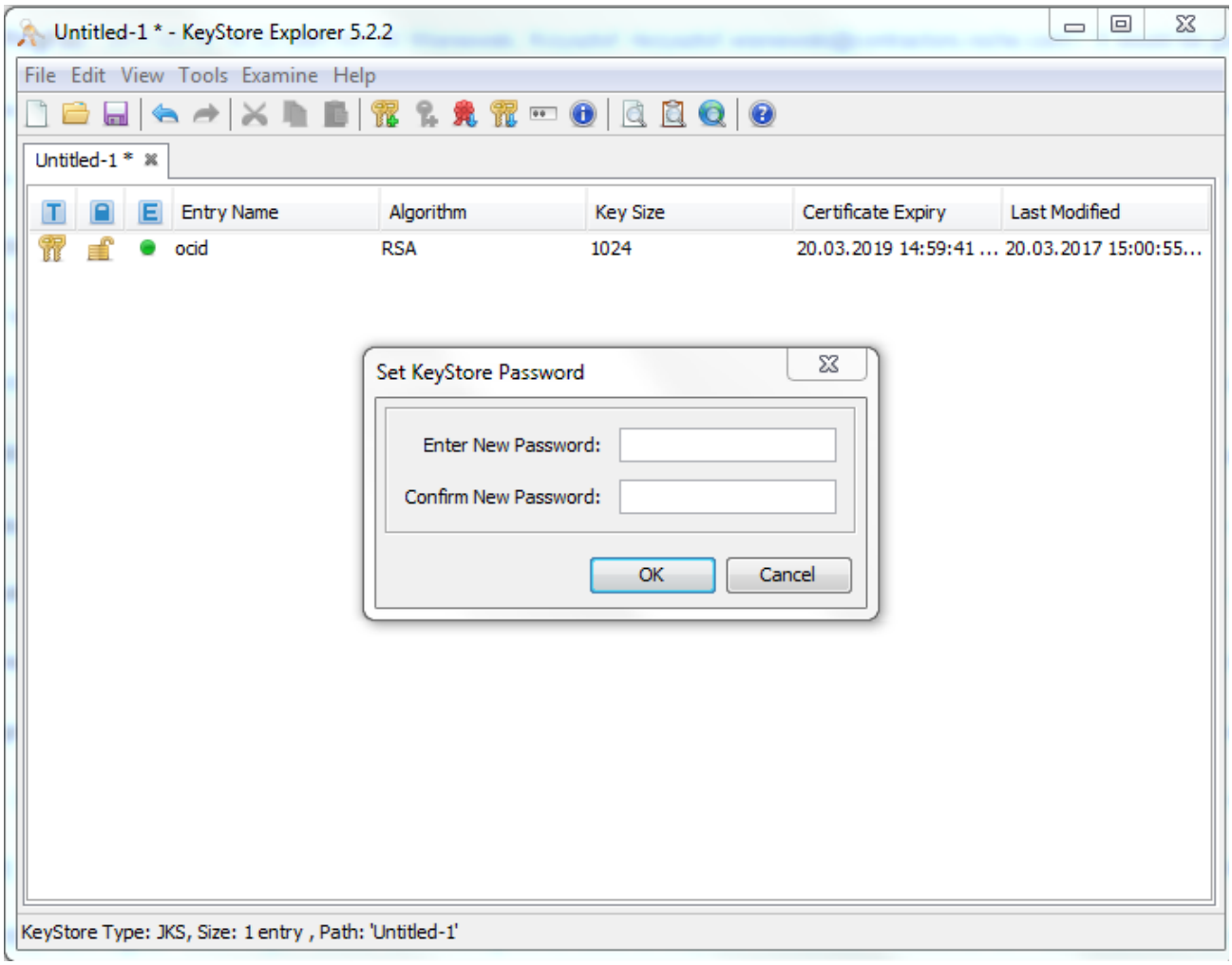
10. Check the displayed result, and make any changes if required.



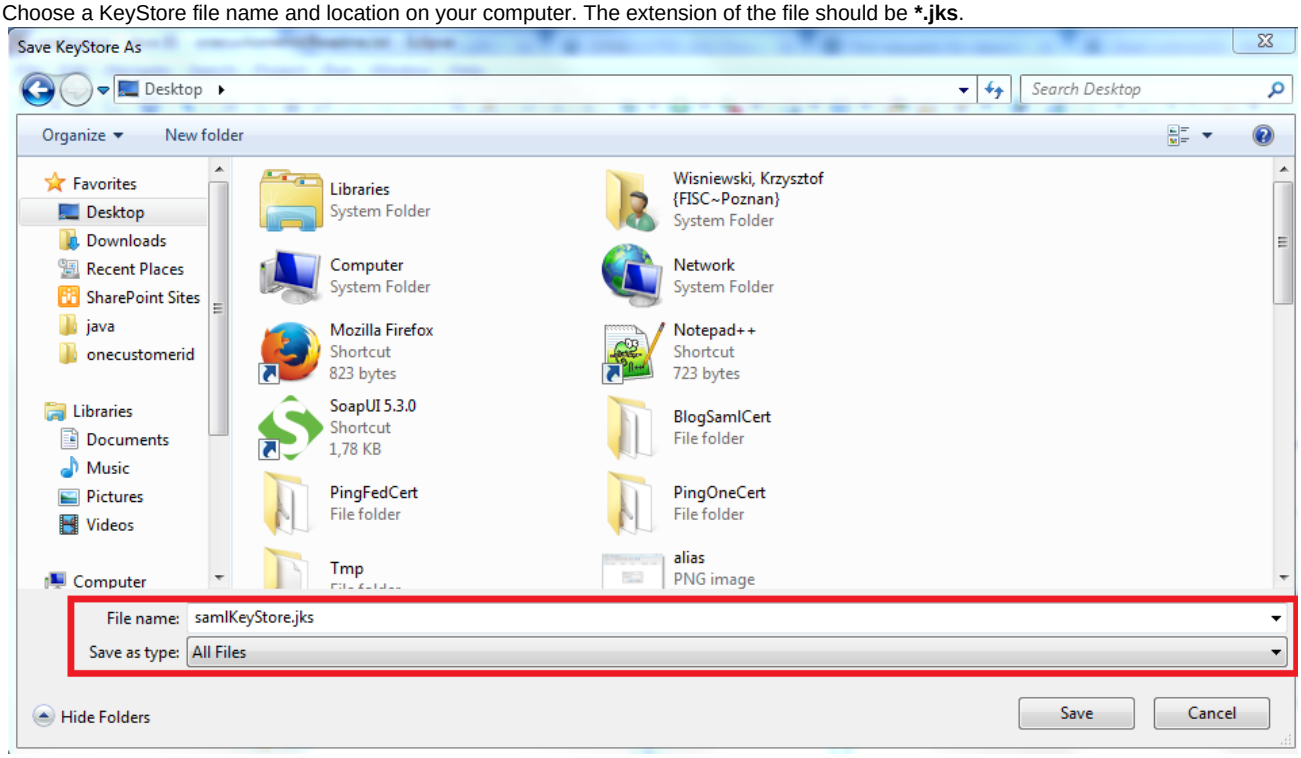
11. Save KeyStore
    To save KeyStore, click **File -> Save As**.



12. Choose KeyStore Password



13. Choose KeyStore file name
Choose a KeyStore file name and location on your computer. The extension of the file should be ***.jks**.



Use certificate in OneCustomerId

To use the generated certificate in a OneCustomerId project, perform the following steps:

1. Add certificate to project code
   Location of the certificate should be in folder "resources\security". For instance: onecustomerid\src\main\resources\security\samlKeyStore.jks
2. Update properties file
   In file "application-<environment>.properties" update all properties connected with signature. For instance:

```
saml.signature.keystore.path=classpath:/security/samlKeyStore.jks
saml.signature.keystore.password=keyStorePassword
saml.singature.privatekey.alias=saml
saml.signature.privatekey.password=privateKeyPassword
```

3. Contact with PingOne and PingFederate administrator to update certificate
   The new generated certificate should be deployed on PingOne and PingFederate servers.