iDEAL Advanced

ING Netherlands

Keystore Explorer manual for iDEAL advanced

Version 3.0 - January 2013

CONTENTS

1. INTRODUCTION

Chapter 8.4 of the iDEAL Merchant Integration Guide (version 3.3.1) discusses the procedure for acquiring XML signing certificates using OpenSSL.

This document describes an alternative solution for obtaining the required free certificates for iDEAL using a free software tool that runs on Windows, Linux and MacOS. This alternative solution offers you the possibility to generate the correct XML signing certificates using a Graphical User Interface.

1.1 Disclaimer

The instruction described in this document is a free service as an alternative for OpenSSL to generate the necessary XML signing certificates for iDEAL.

While ING uses reasonable efforts to include accurate and up-to-date information in this document, errors or omissions sometimes occur. ING and ING companies expressly disclaim any liability, whether in contract, tort, and strict liability or otherwise, for any direct, indirect, incidental, consequential, punitive or special damages arising out of or in any way connected with your access to or use of this document.

All information in this document is provided "as is" and is subject to change without prior notice. Such information is provided, to the fullest extent permissible pursuant to applicable law, without warranty of any kind express or implied, including but not limited to implied warranties of merchantability, fitness for a particular purpose, non-infringement and freedom from computer viruses or similar disabling devices.

ING does not warrant the adequacy, accuracy or completeness of any information in this document and expressly disclaims any liability for errors or omissions therein. Users are responsible for evaluating the accuracy, completeness or usefulness of any information or other content available in the document.

1.2 Version control

This document underwent the following changes:

Version	Date	Change
1.0	25 Sep 2012	Revised version
1.1	16 Oct 2012	Revised version
1.2	6 Nov 2012	Revised version
3.0	23 jan 2013	Revised version

2. SOFTWARE INSTALLATION

2.1 System requirements

Check http://www.lazgosoftware.com/kse/gettingstarted.html for the system requirements for the installation of the software.

This manual is based on the following OS platform and software:

Windows 7

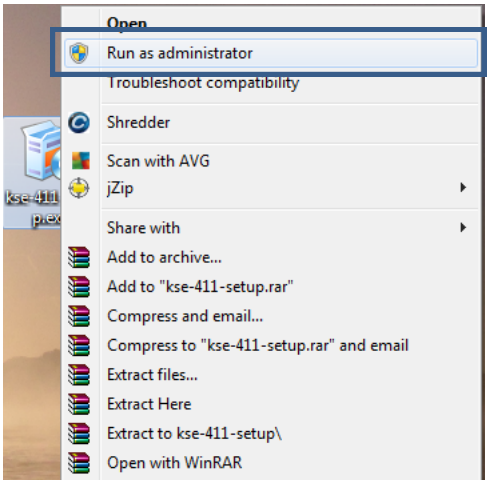
KeyStore Explorer software

2.2 Install KeyStore Explorer software

You can download the required software from: http://www.lazgosoftware.com/kse/downloads.html.

An installation package is available for Windows, MacOS and Linux. An installation manual is also provided on the Downloads page.

Ensure that you run the installation software as an Administrator when you install the software. To do so, click the software installation application, hold down the right mouse button and select the option “Run as administrator” from the pop-up menu:



2.3 System administrators privileges

You need to have the correct access privileges to install the software. In case of questions, please contact your system maintenance department. When installing the Keystore Explorer software, please ensure that you run the installation software as system administrator.

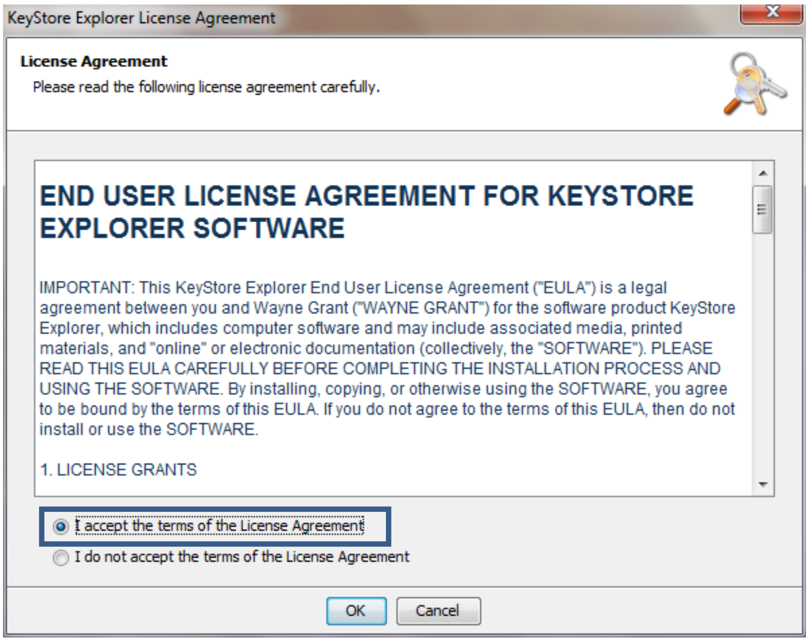
3. PASSWORDS

Throughout the process of generating certificates, you will prompted several times to enter passwords. We recommend using strong passwords and to store the passwords at a save location. You will require the passwords at a later stage with the integration of iDEAL and your web shop.

Visit http://en.wikipedia.org/wiki/Password_policy for more information about strong passwords.

4. CREATING A KEY PAIR

Please launch the KeyStore Explorer via the Windows “Start” menu. The first time you run the application the following screen is shown:



KeyStore Explorer License Agreement

License Agreement

Please read the following license agreement carefully.

END USER LICENSE AGREEMENT FOR KEYSTORE EXPLORER SOFTWARE

IMPORTANT: This KeyStore Explorer End User License Agreement ("EULA") is a legal agreement between you and Wayne Grant ("WAYNE GRANT") for the software product KeyStore Explorer, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation (collectively, the "SOFTWARE"). PLEASE READ THIS EULA CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AND USING THE SOFTWARE. By installing, copying, or otherwise using the SOFTWARE, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, then do not install or use the SOFTWARE.

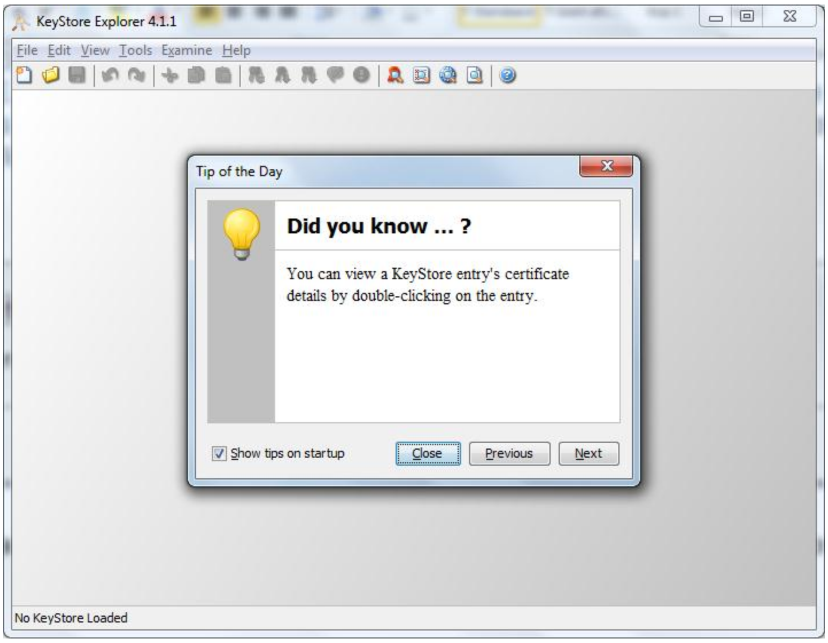
1. LICENSE GRANTS

● I accept the terms of the License Agreement

○ I do not accept the terms of the License Agreement

Select the radio button “I accept the terms of the License Agreement” and click “OK” to continue.

The following screen is shown:

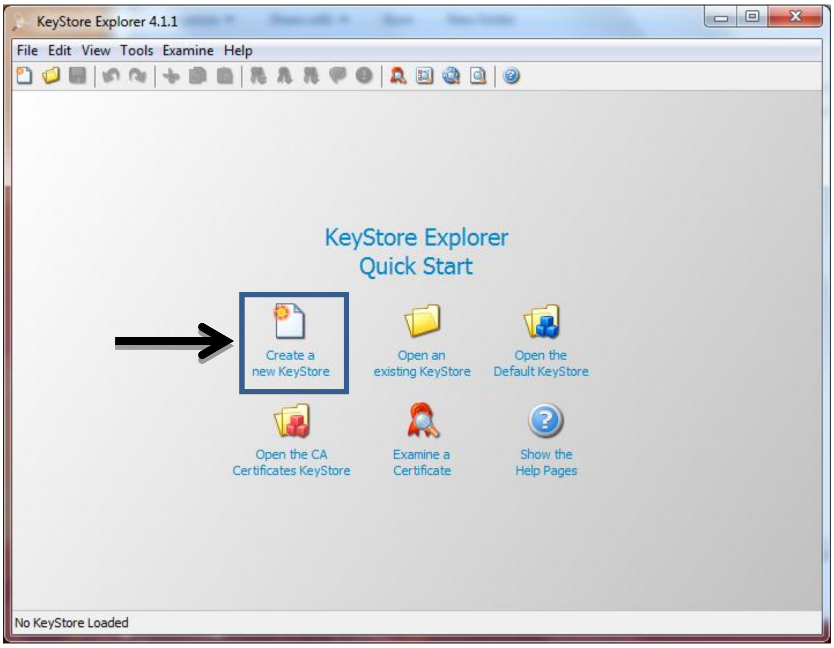


Did you know ... ?

You can view a KeyStore entry's certificate details by double-clicking on the entry.

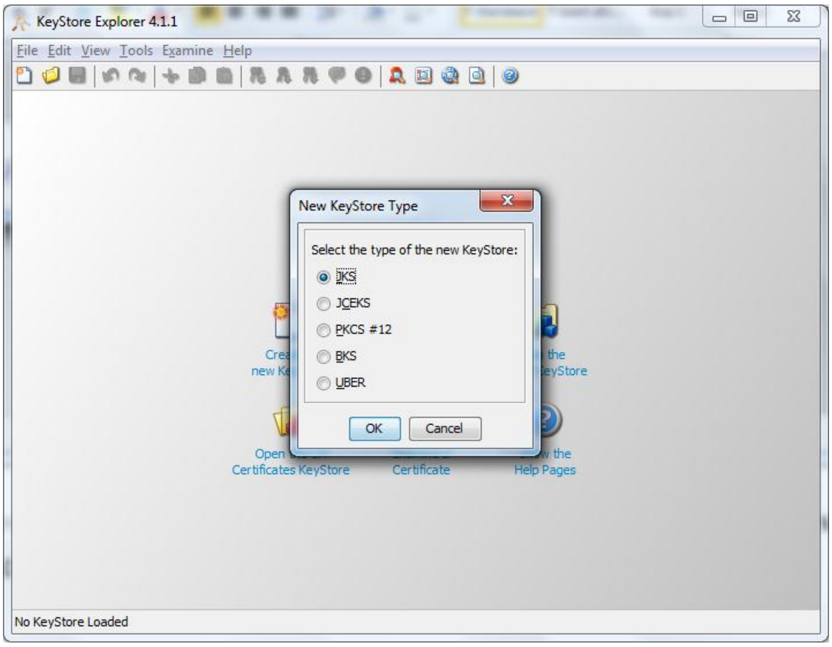
☑ Show tips on startup

Click the “Close” button to continue. The following screen is shown:



To continue, click the “Create a new KeyStore“ button.

The following screen is shown:

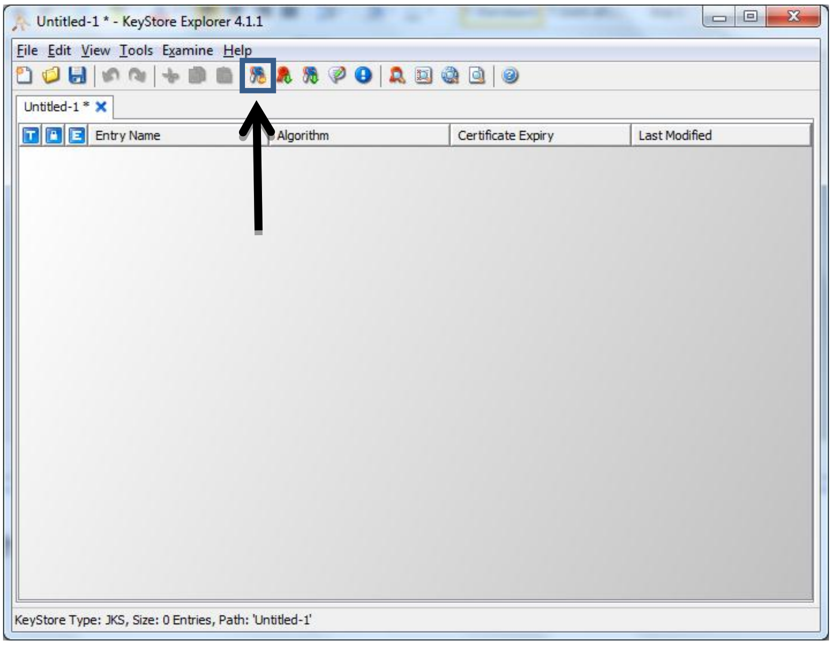


Select the type of the new KeyStore:

● JKS
○ JCEKS
○ PKCS #12
○ BKS
○ UBER

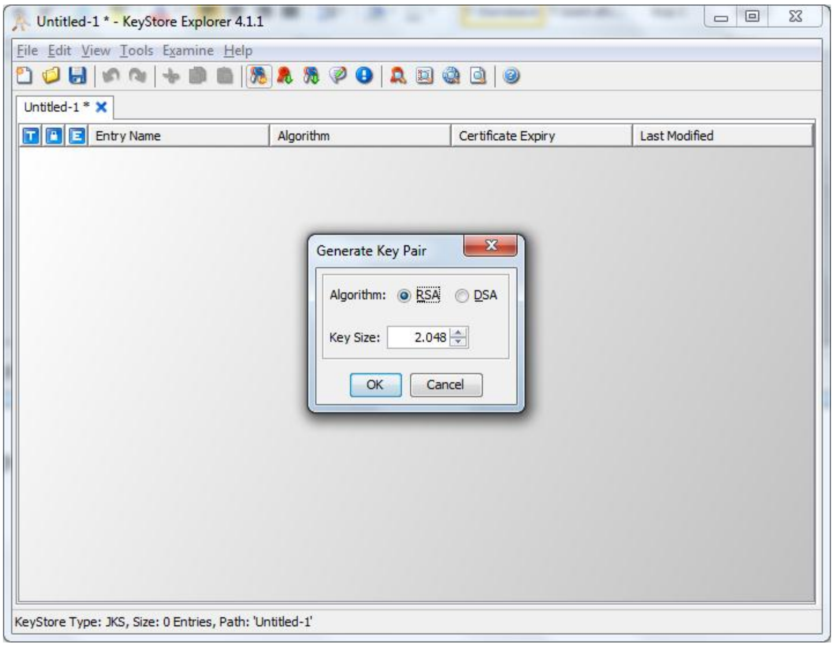
Ensure that the option “JKS” is selected and click the “OK” button.

Now click the first icon with a key symbol in the menu-bar (as indicated by the arrow):


Untitled-1 * - KeyStore Explorer 4.1.1
File Edit View Tools Examine Help
Untitled-1 *
T
E
Entry Name
Algorithm
Certificate Expiry
Last Modified

KeyStore Type: JKS, Size: 0 Entries, Path: 'Untitled-1'

The following screen is shown:



Algorithm: ● RSA ○ DSA

Key Size: 2.048

KeyStore Type: JKS, Size: 0 Entries, Path: 'Untitled-1'

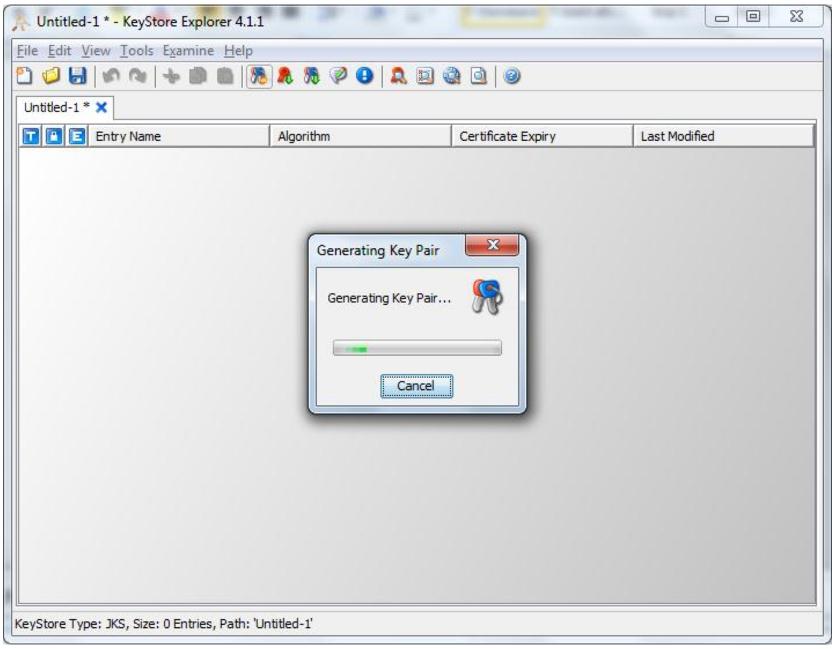
Ensure to select the following:

Algorithm:	“RSA”
Key Size:	“2048”

To continue, click the “OK” button.

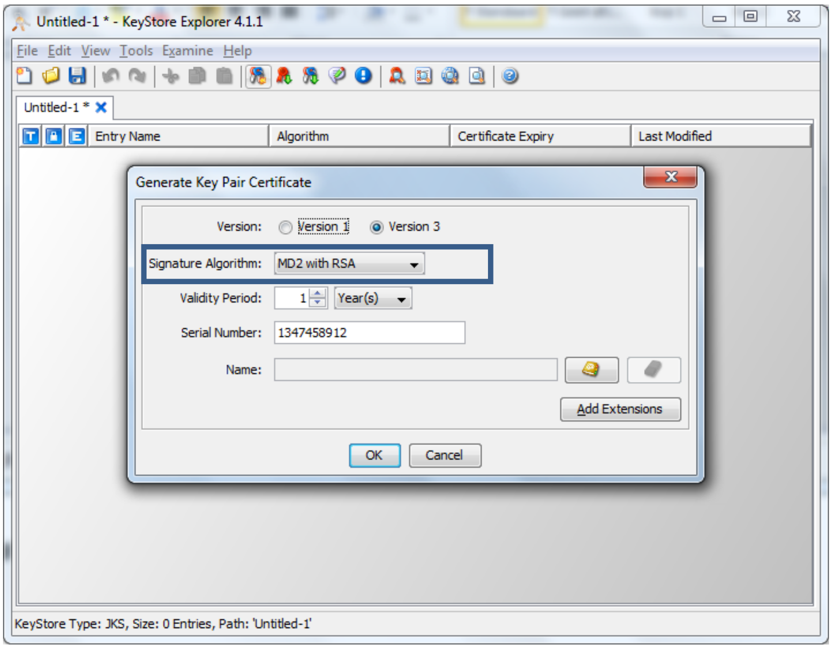
Your key pair will now be generated.

The following screen is shown:



KeyStore Type: JKS, Size: 0 Entries, Path: 'Untitled-1'

After the key pair has been generated, the following screen is shown:



Untitled-1 * - KeyStore Explorer 4.1.1
File Edit View Tools Examine Help
Untitled-1 *
Entry Name
Algorithm
Certificate Expiry
Last Modified
Generate Key Pair Certificate
Add Extensions
OK
Cancel

Version: ○ Version 1 ● Version 3

Signature Algorithm: MD2 with RSA

Validity Period: 1 Year(s)

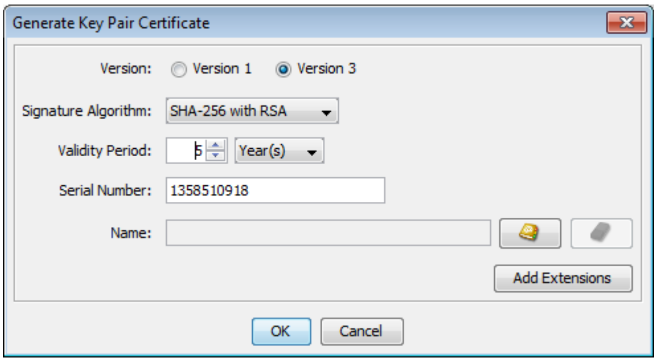
Serial Number: 1347458912

Name:

KeyStore Type: JKS, Size: 0 Entries, Path: 'Untitled-1'

From the drop down menu “Signature Algorithm”, select “SHA-256 with RSA”.

Set the validity period to 5 years, as shown below:



Generate Key Pair Certificate

Version: ○ Version 1 ● Version 3

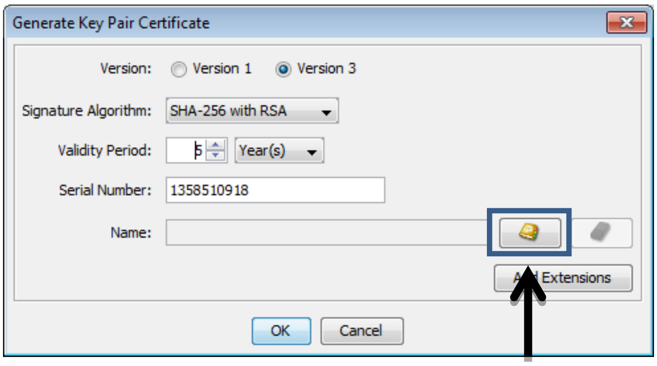
Signature Algorithm: SHA-256 with RSA

Validity Period: 5 Year(s)

Serial Number: 1358510918

Name:

The serial number is automatically generated but can be overruled by the user. Now click the button designated by the arrow below:



Generate Key Pair Certificate

Version: ○ Version 1 ● Version 3

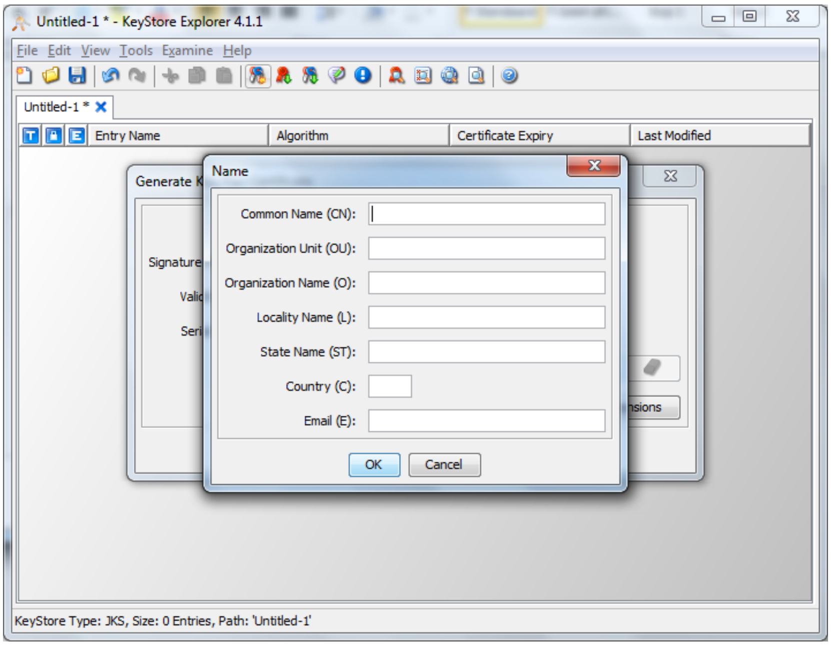
Signature Algorithm: SHA-256 with RSA

Validity Period: 5 Year(s)

Serial Number: 1358510918

Name:

The following screen is shown:



Name

Common Name (CN):

Organization Unit (OU):

Organization Name (O):

Locality Name (L):

State Name (ST):

Country (C):

Email (E):

KeyStore Type: JKS, Size: 0 Entries, Path: 'Untitled-1'

In the field “Common name” the common name is entered. Typically the name of the web shop.

In the field “Organizational unit” the department name is entered.

In the field “Organizational name” the name of the organisation is entered. Duplicate values are allowed.

In the field “Locality name” the city of residence is entered.

In the field “State Name” the name of the state is entered.

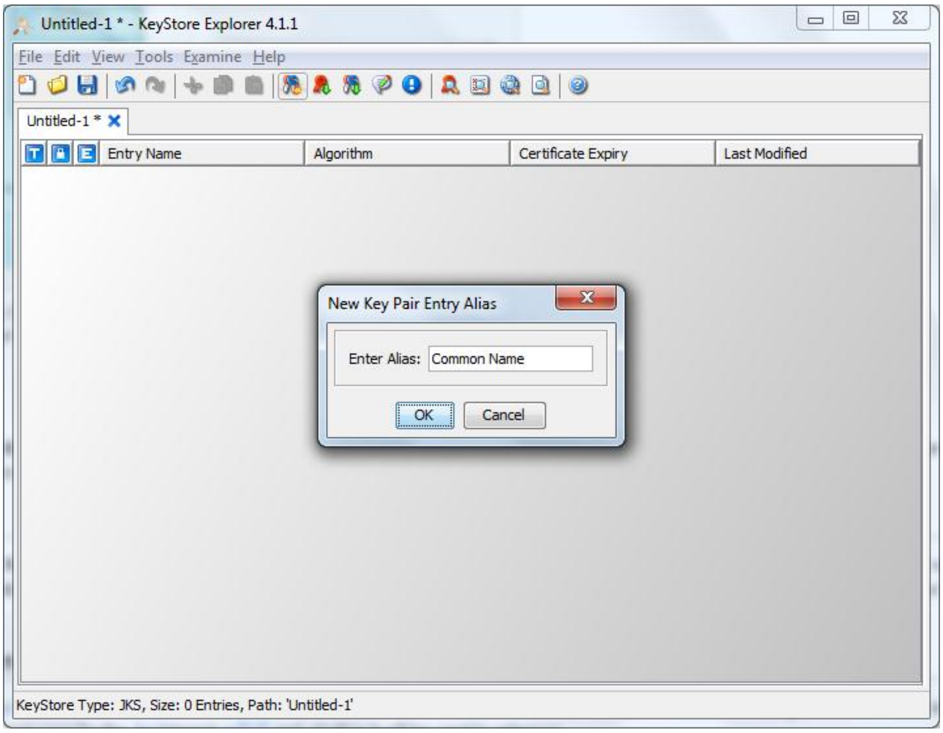
In the field “Country” the 2 letter country code is entered, i.e. “NL” for The Netherlands, “UK” for Great Britain, “US” for United States of America, etc.

In the field “E-Mail” the e-mail address of the administrative contact is entered. We recommend entering a common mailbox name, such as the mailbox of the system maintenance department.

Click the “OK” button after the fields are entered.

Click again on the “OK” button in the following screen.

The following screen is shown:

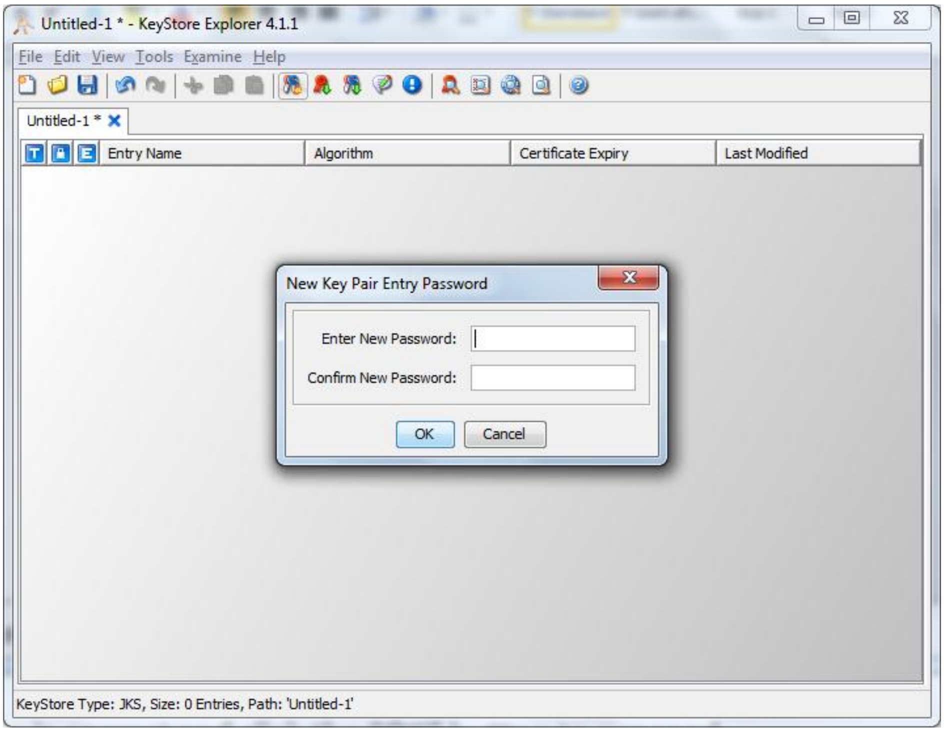


Enter Alias: Common Name

KeyStore Type: JKS, Size: 0 Entries, Path: 'Untitled-1'

Enter the Alias Name of the Key Pair and click OK”.

The following screen is shown:



Untitled-1 * - KeyStore Explorer 4.1.1
File Edit View Tools Examine Help
Untitled-1 *
Entry Name
Algorithm
Certificate Expiry
Last Modified
New Key Pair Entry Password
OK
Cancel

Enter New Password:

Confirm New Password:

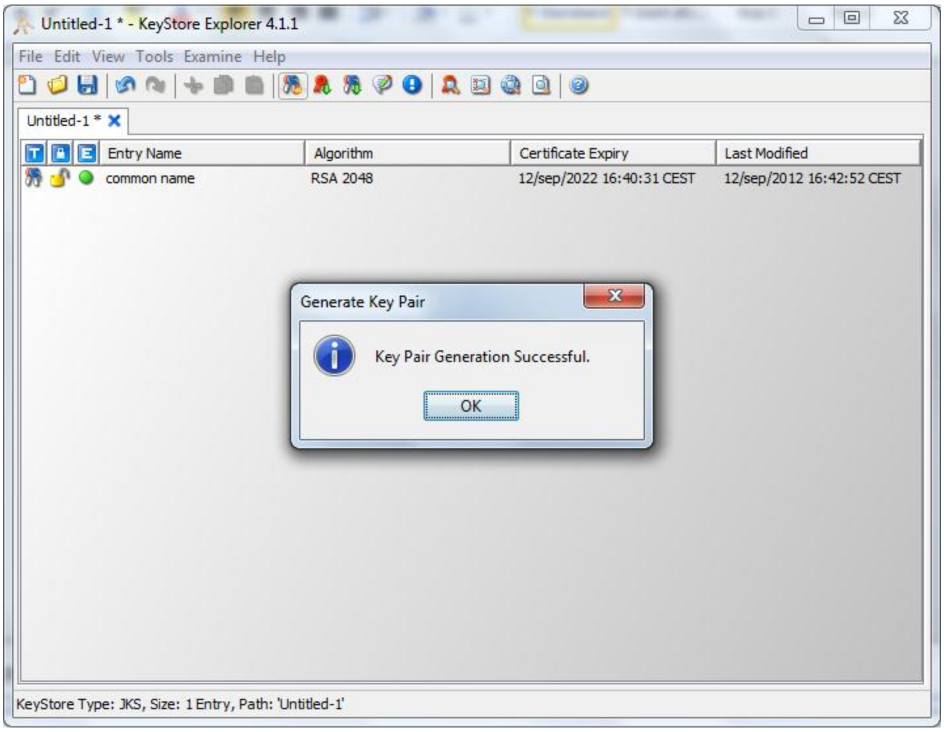
KeyStore Type: JKS, Size: 0 Entries, Path: 'Untitled-1'

Enter the password for the key pair twice and click the “OK” button.

IMPORTANT:

Save the password that you assigned to your key pair at a save location as you will require it at a later stage.

The following screen is shown:



Untitled-1 * - KeyStore Explorer 4.1.1

T	E	Entry Name	Algorithm	Certificate Expiry	Last Modified
		common name	RSA 2048	12/sep/2022 16:40:31 CEST	12/sep/2012 16:42:52 CEST

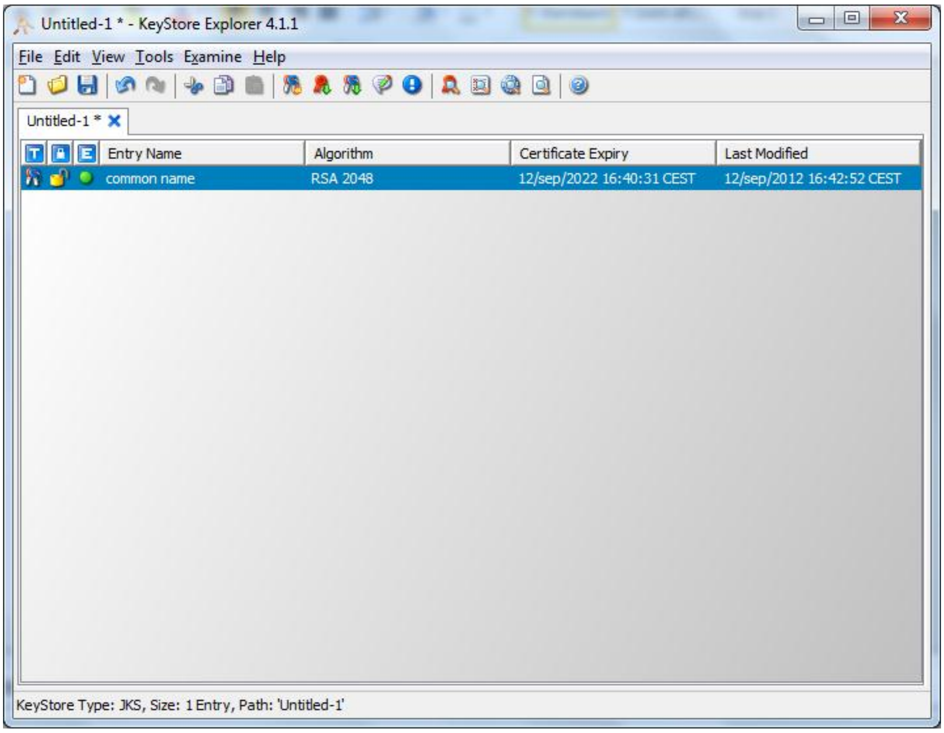
Generate Key Pair

Key Pair Generation Successful.

KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

Your key pair has now been generated.

The following screen is shown:



Untitled-1 * - KeyStore Explorer 4.1.1

T	E	Entry Name	Algorithm	Certificate Expiry	Last Modified
		common name	RSA 2048	12/sep/2022 16:40:31 CEST	12/sep/2012 16:42:52 CEST

KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

5. EXPORTING YOUR CERTIFICATES

In this chapter, the procedure for exporting your certificates, private and public keys is explained.

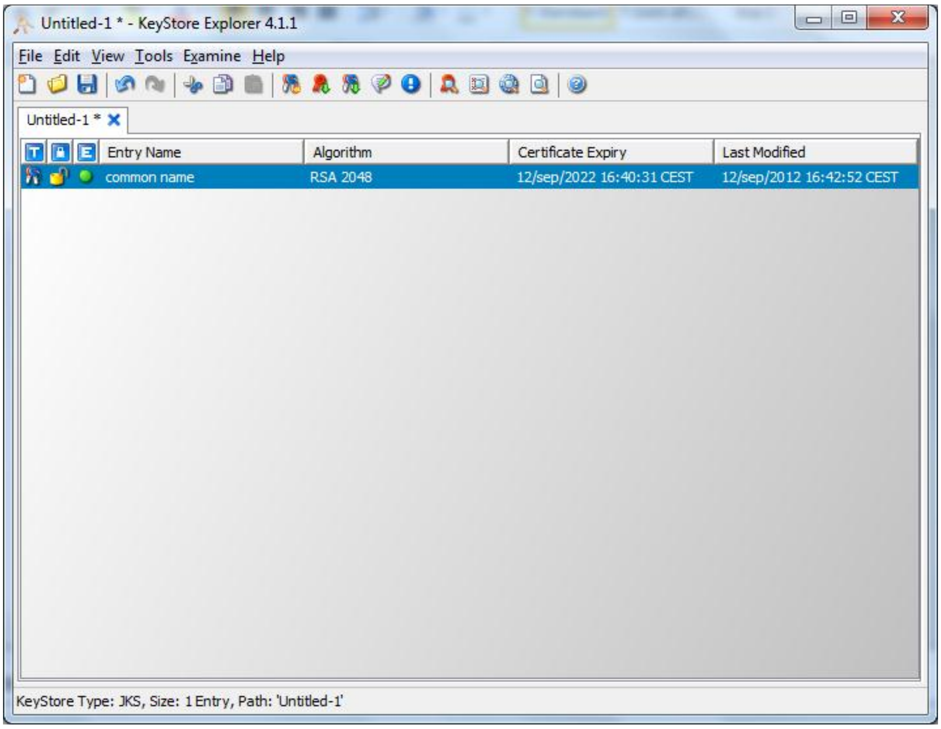
IMPORTANT:

We strongly recomment to use the following naming conventions when exporting the certificates:

Key Pair	pair.p12
Certificate Chain	cert.cer
Private Key	priv.pem

5.1 Exporting the Key Pair

To export the key pair, select the newly generated certificate by clicking its name. The file is highlighted in the Keystore Explorer window:



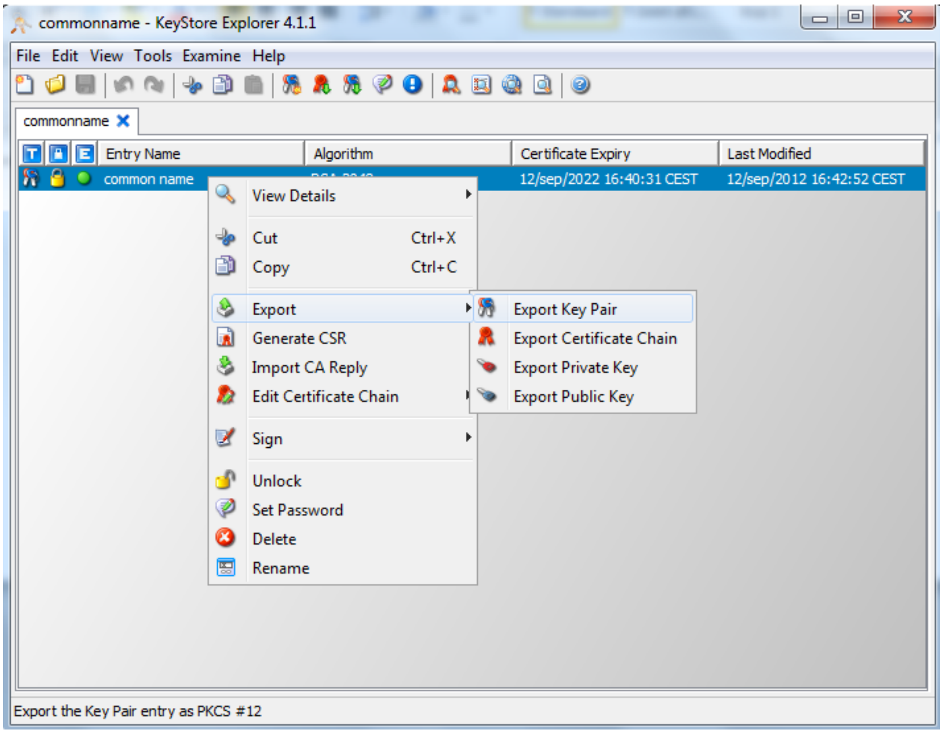
Untitled-1 * - KeyStore Explorer 4.1.1
File Edit View Tools Examine Help
Untitled-1 *

T	E	Entry Name	Algorithm	Certificate Expiry	Last Modified
	●	common name	RSA 2048	12/sep/2022 16:40:31 CEST	12/sep/2012 16:42:52 CEST

KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

Click the right mouse button on the selected key pair..

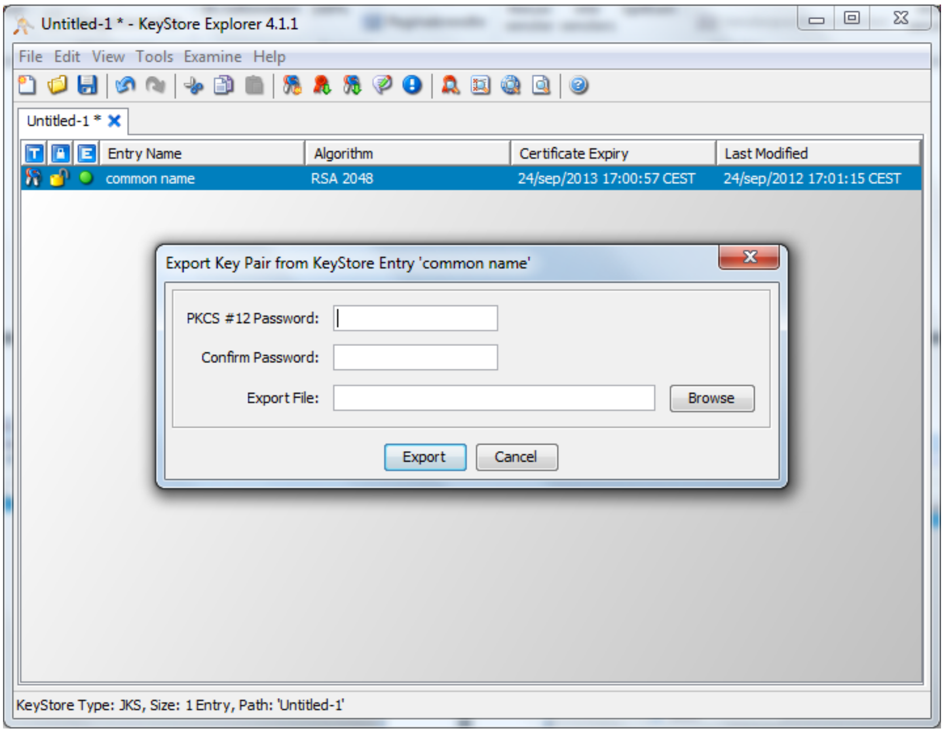
The following menu is shown:



Entry Name	Algorithm	Certificate Expiry	Last Modified
common name	RSA 2048	12/sep/2022 16:40:31 CEST	12/sep/2012 16:42:52 CEST

Export the Key Pair entry as PKCS #12

Select the menu option “Export Key Pair”. The following screen is shown:



Untitled-1 * - KeyStore Explorer 4.1.1
File Edit View Tools Examine Help
Untitled-1 *
Export Key Pair from KeyStore Entry 'common name'
Browse
Export
Cancel

Entry Name	Algorithm	Certificate Expiry	Last Modified
common name	RSA 2048	24/sep/2013 17:00:57 CEST	24/sep/2012 17:01:15 CEST

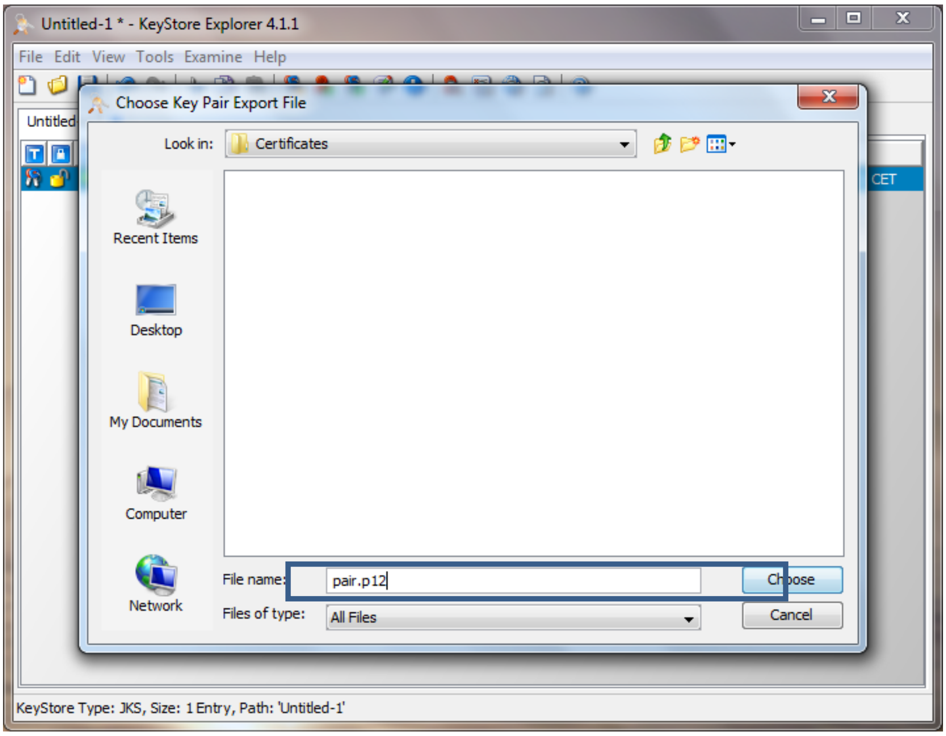
PKCS #12 Password:

Confirm Password:

Export File:

KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

Enter the password for the key pair twice and click the “Browse” button to determine the location where the key pair is to be stored. We recommend storing all iDEAL certificates in a common directory.


Untitled-1 * - KeyStore Explorer 4.1.1
File Edit View Tools Examine Help
Choose Key Pair Export File
Recent Items
Desktop
My Documents
Computer
Network
Choose
Cancel

Look in: Certificates

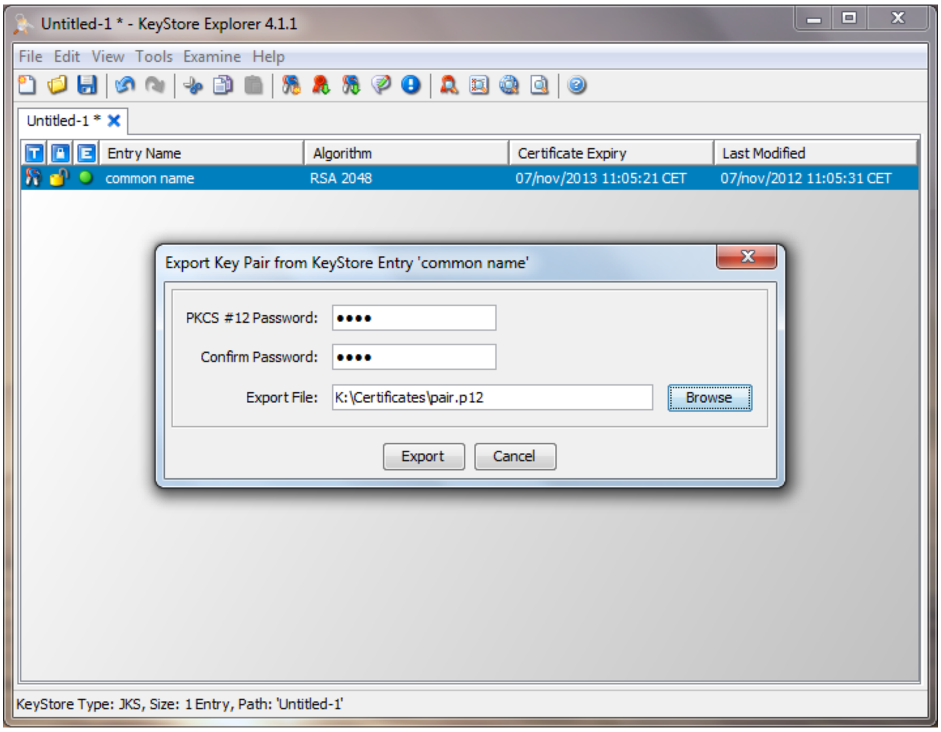
File name: pair.p12

Files of type: All Files

KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

Click the “Choose” button after the file location has been selected you have entered a name.

The screen looks as following:


Untitled-1 * - KeyStore Explorer 4.1.1
File Edit View Tools Examine Help
Untitled-1 *
Browse
Export
Cancel

Entry Name	Algorithm	Certificate Expiry	Last Modified
common name	RSA 2048	07/nov/2013 11:05:21 CET	07/nov/2012 11:05:31 CET

Export Key Pair from KeyStore Entry 'common name'

PKCS #12 Password: ••••

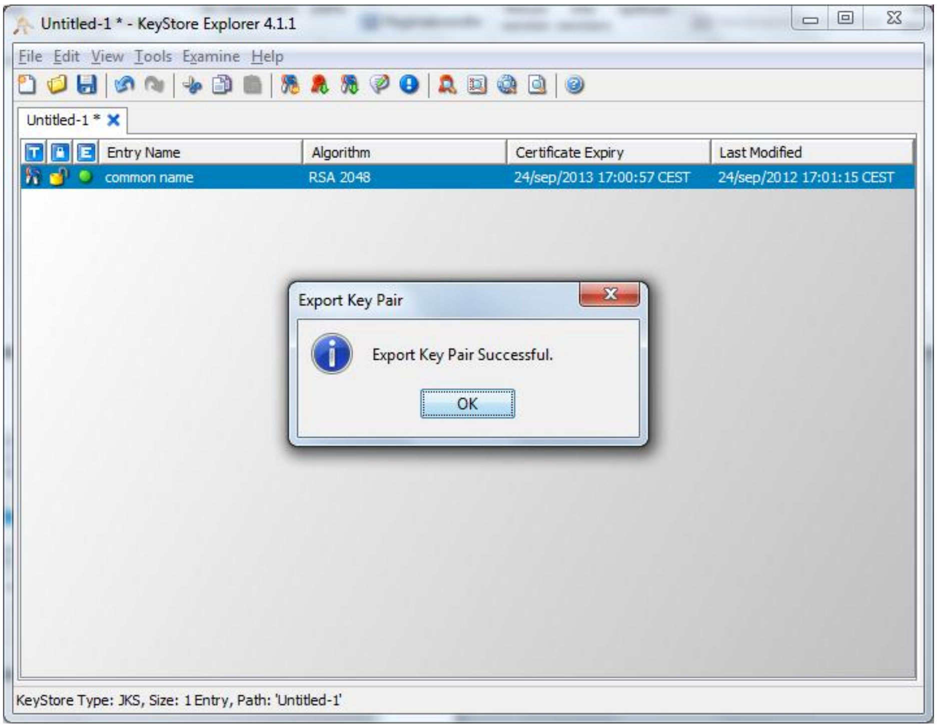
Confirm Password: ••••

Export File: K:\Certificates\pair.p12

KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

Click the “Export” button to continue.

The key pair has now been exported to the selected directory:


Untitled-1 * - KeyStore Explorer 4.1.1
File Edit View Tools Examine Help
Untitled-1 *
OK

Entry Name	Algorithm	Certificate Expiry	Last Modified
common name	RSA 2048	24/sep/2013 17:00:57 CEST	24/sep/2012 17:01:15 CEST

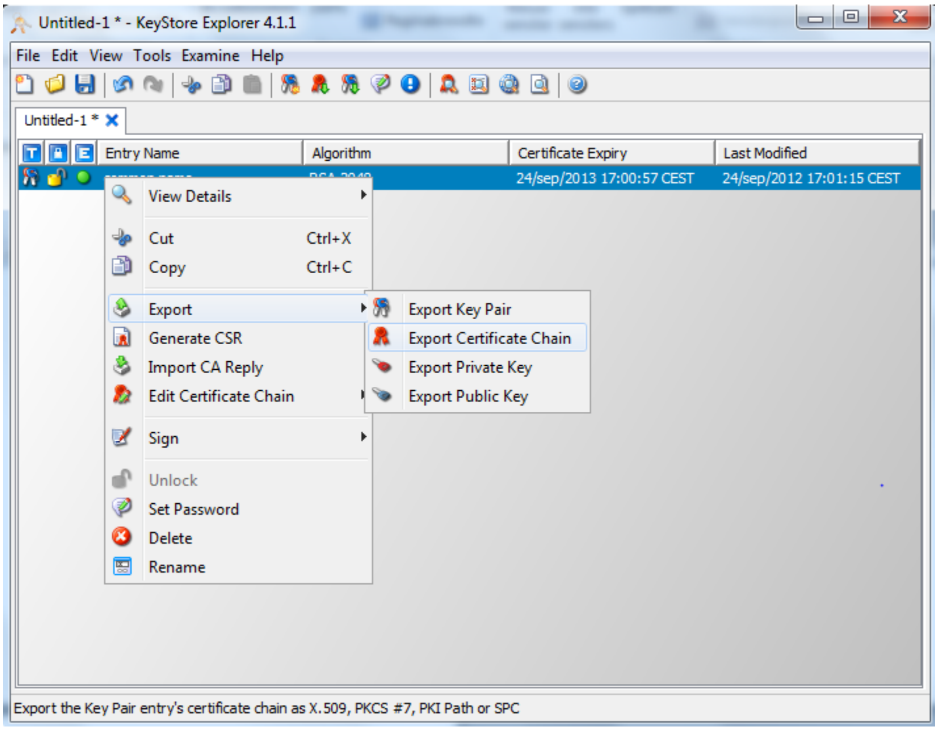
Export Key Pair

Export Key Pair Successful.

KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

5.2 Exporting the Certificate Chain

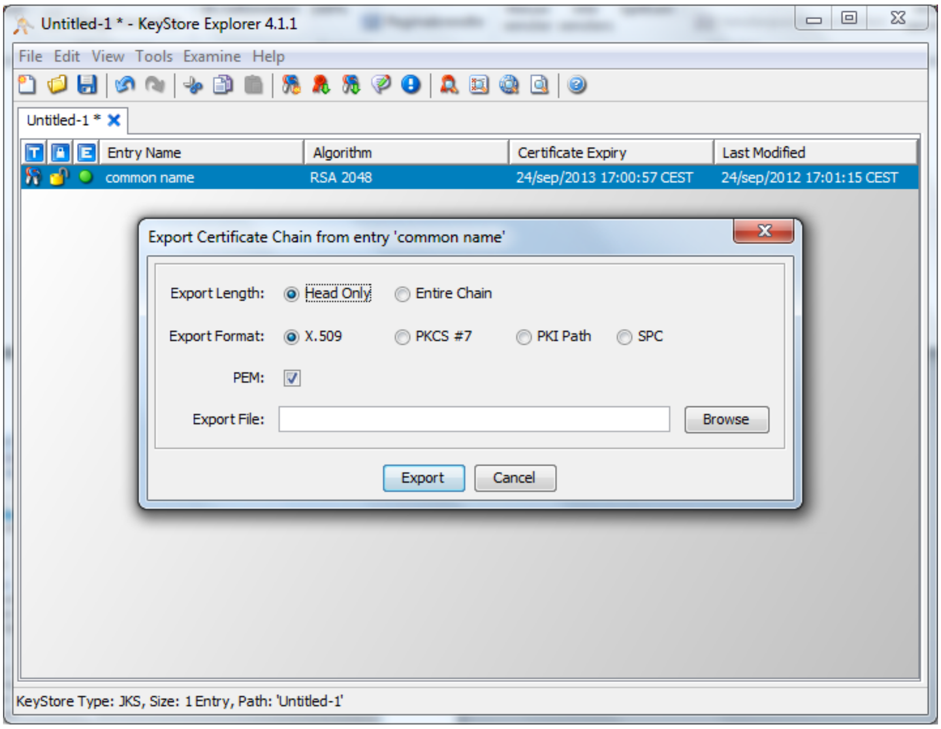
Please undertake the following actions to export the entire certificate chain. In the Keystore Explorer application, select the appropriate certificate file and click the right mouse button. Select the “Export Certificate Chain” menu option.



Entry Name	Algorithm	Certificate Expiry	Last Modified
		24/sep/2013 17:00:57 CEST	24/sep/2012 17:01:15 CEST

Export the Key Pair entry's certificate chain as X.509, PKCS #7, PKI Path or SPC

The following screen is shown:



Untitled-1 * - KeyStore Explorer 4.1.1

Entry Name	Algorithm	Certificate Expiry	Last Modified
common name	RSA 2048	24/sep/2013 17:00:57 CEST	24/sep/2012 17:01:15 CEST

Export Certificate Chain from entry 'common name'

Export Length: ● Head Only ○ Entire Chain

Export Format: ● X.509 ○ PKCS #7 ○ PKI Path ○ SPC

PEM: ☑

Export File:

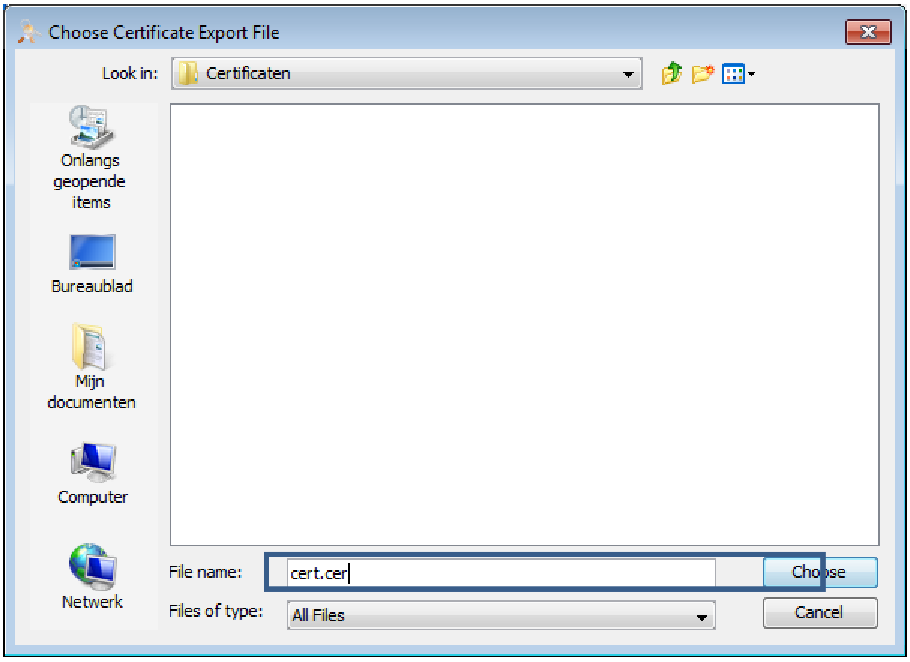
KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

Ensure that the following parameters are set:

Export Length:	“Head Only”
Export format:	“X.509”
PEM:	Ensure that this check box is ticked

To select the directory where to store certificate chain, click the “Browse” button.

The following screen is shown:



Choose Certificate Export File

Look in: Certificaten

File name: cert.cer

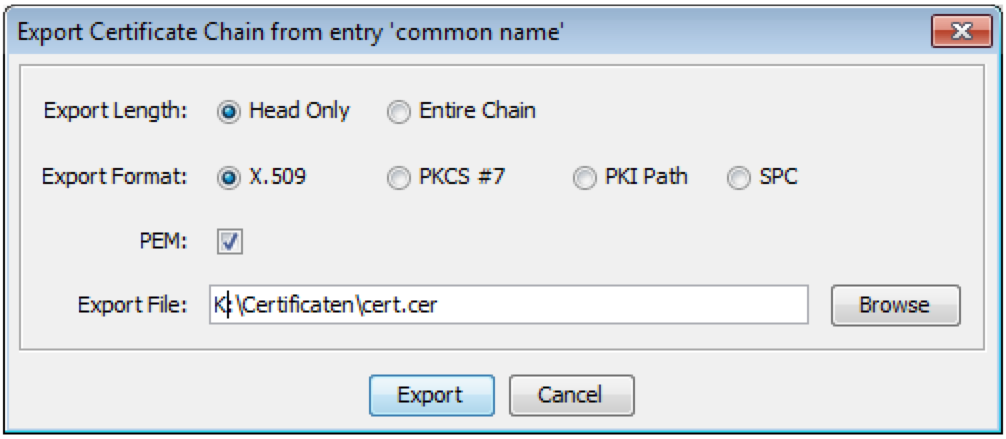
Files of type: All Files

Enter the name of the certificate chain.

IMPORTANT:

Ensure you have the extension .CER after the file name of the certificate chain (as indicated above). To continue, click the “Choose” button.

The following screen is shown:



Export Certificate Chain from entry 'common name'

Export Length: ● Head Only ○ Entire Chain

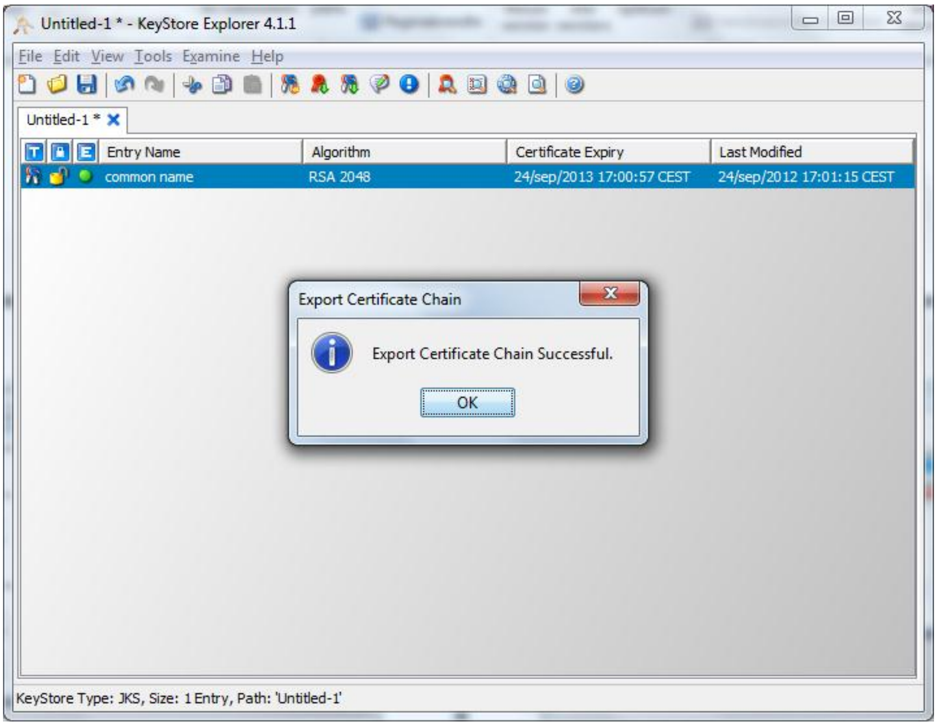
Export Format: ● X.509 ○ PKCS #7 ○ PKI Path ○ SPC

PEM: ☑

Export File: K:\Certificaten\cert.cer

Click the “Export” button to complete the export of the certificate chain.

Once completed, the following screen is shown:



Untitled-1 * - KeyStore Explorer 4.1.1

Entry Name	Algorithm	Certificate Expiry	Last Modified
common name	RSA 2048	24/sep/2013 17:00:57 CEST	24/sep/2012 17:01:15 CEST

Export Certificate Chain

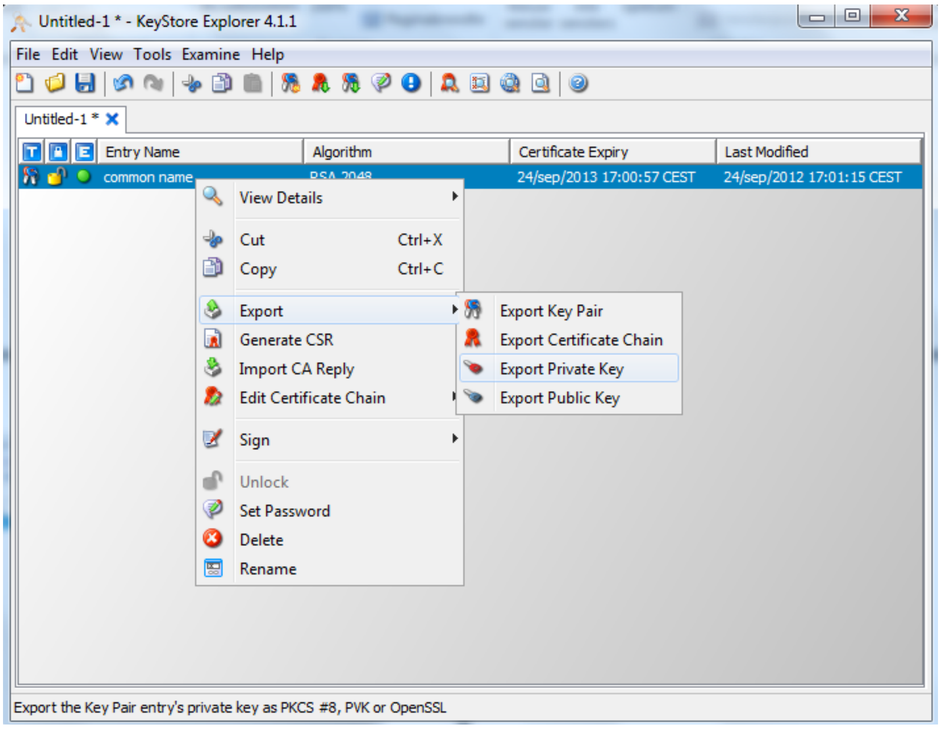
Export Certificate Chain Successful.

OK

KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

5.3 Exporting the Private Key

To export the Private Key of the certificate, select the certificate name in the Keystore Explorer application and click the right mouse button:

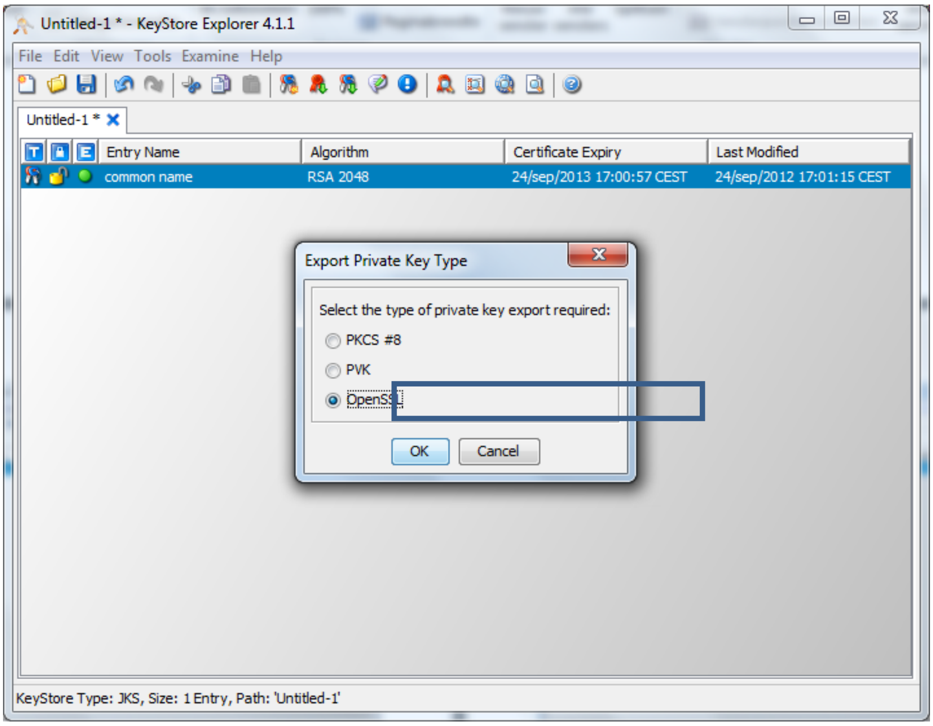


Untitled-1 * - KeyStore Explorer 4.1.1

Entry Name	Algorithm	Certificate Expiry	Last Modified
common name	RSA 2048	24/sep/2013 17:00:57 CEST	24/sep/2012 17:01:15 CEST

Export the Key Pair entry's private key as PKCS #8, PVK or OpenSSL

From the pop-up menu, select “Export Private Key”. The following screen is shown:



Untitled-1 * - KeyStore Explorer 4.1.1

Entry Name	Algorithm	Certificate Expiry	Last Modified
common name	RSA 2048	24/sep/2013 17:00:57 CEST	24/sep/2012 17:01:15 CEST

Export Private Key Type

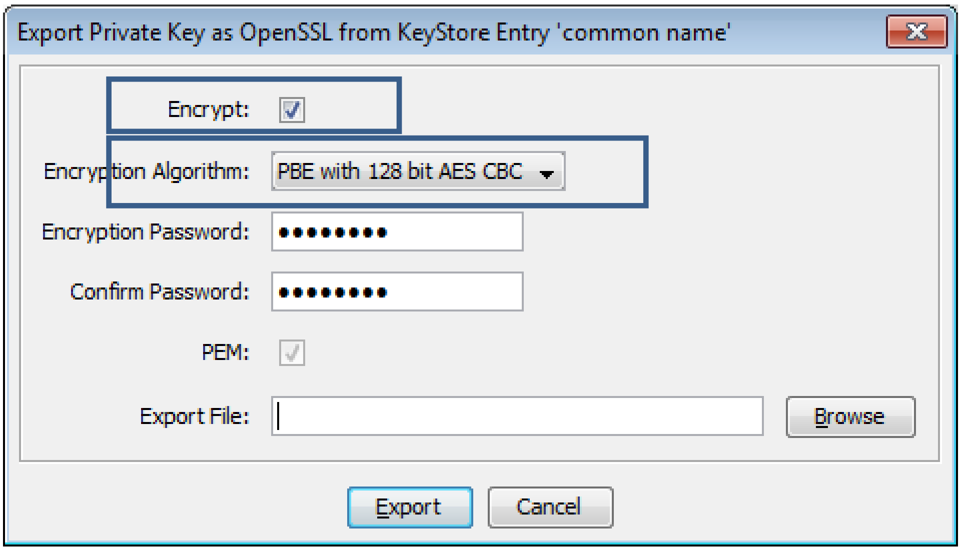
Select the type of private key export required:

○ PKCS #8
○ PVK
● OpenSSL

OK | Cancel

KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

Ensure to select “OpenSSL”. Click “OK” to continue. The following screen is shown:

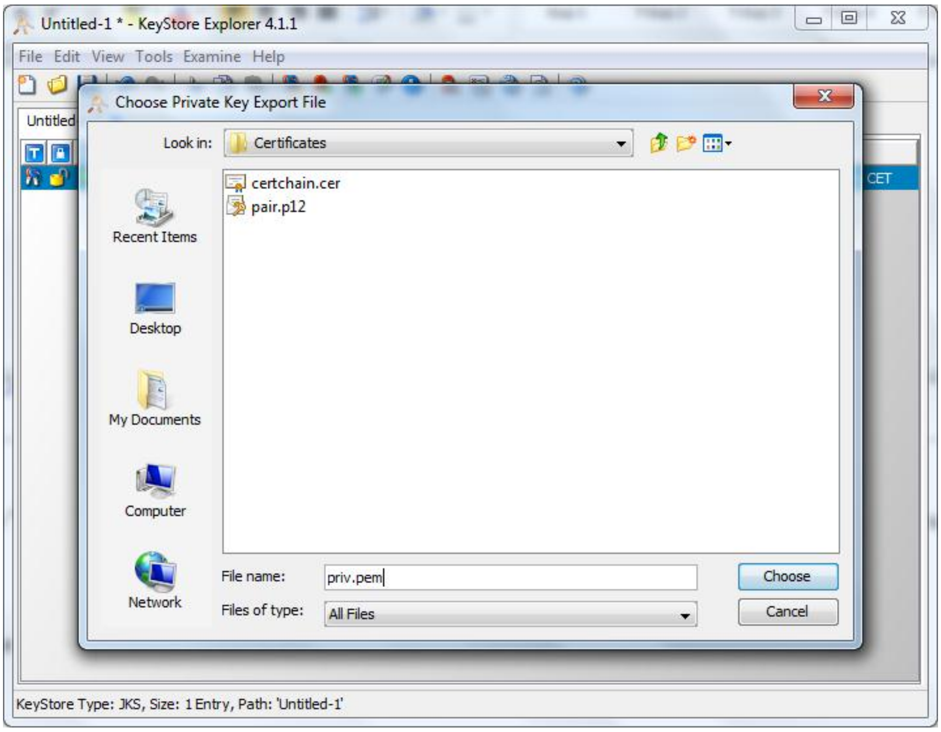


Export Private Key as OpenSSL from KeyStore Entry 'common name'

Encrypt: ☑
Encryption Algorithm: PBE with 128 bit AES CBC
Encryption Password: ••••••••
Confirm Password: ••••••••
PEM: ☑
Export File:

Ensure to tick the radio button “Encrypt” and to set the “Encryption Algorithm” to “PBE with 128 bit AES CBC”.

Click the “Browse” button to select the directory where to store the file and to enter the file name:


Untitled-1 * - KeyStore Explorer 4.1.1
File Edit View Tools Examine Help
Untitled
CET
Choose Private Key Export File
Recent Items
Desktop
My Documents
Computer
Network
Choose
Cancel

Look in: Certificates

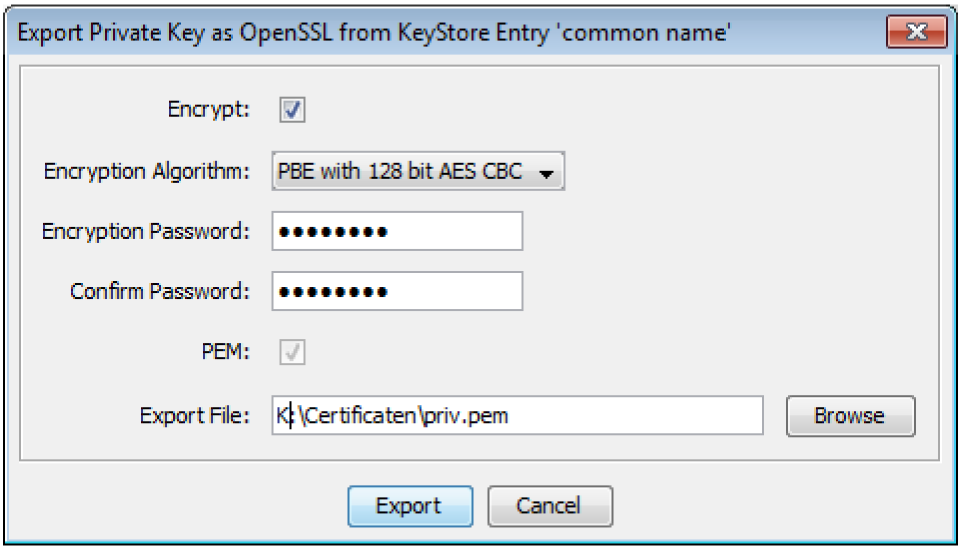
certchain.cer
pair.p12

File name: priv.pem

Files of type: All Files

KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

Enter the name of the file and click the “Choose” button. The following screen is shown:


Export Private Key as OpenSSL from KeyStore Entry 'common name'
Browse
Export
Cancel

Encrypt: ☑

Encryption Algorithm: PBE with 128 bit AES CBC

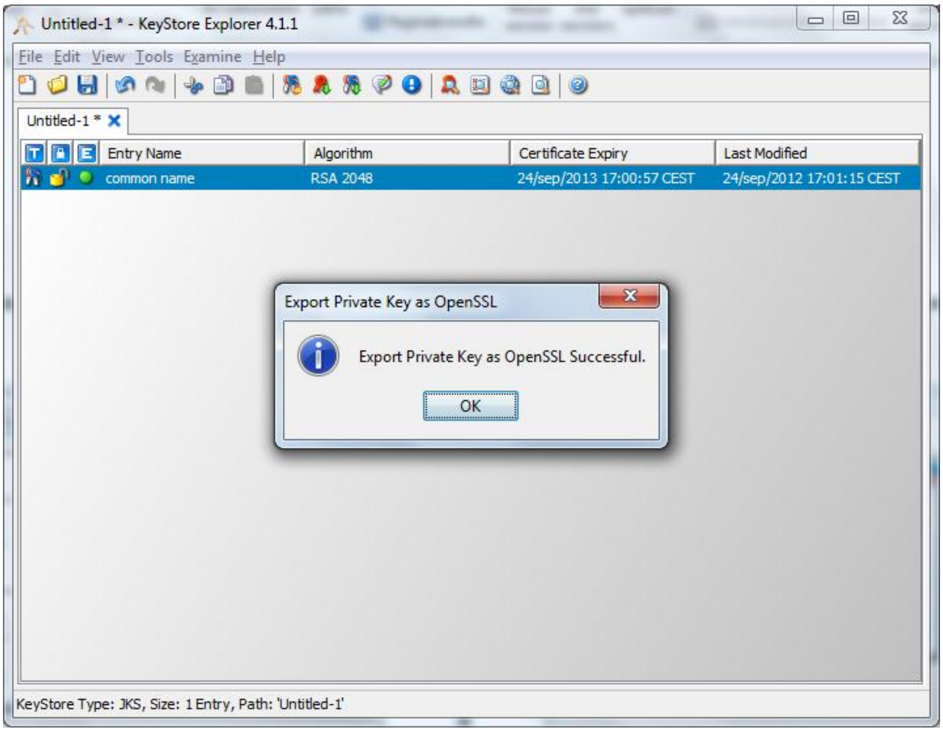
Encryption Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

PEM: ☑

Export File: K:\Certificaten\priv.pem

Click the “Export” button to continue. The following screen is shown:



Untitled-1 * - KeyStore Explorer 4.1.1
File Edit View Tools Examine Help
Untitled-1 *

T	🔒	E	Entry Name	Algorithm	Certificate Expiry	Last Modified
		●	common name	RSA 2048	24/sep/2013 17:00:57 CEST	24/sep/2012 17:01:15 CEST

Export Private Key as OpenSSL

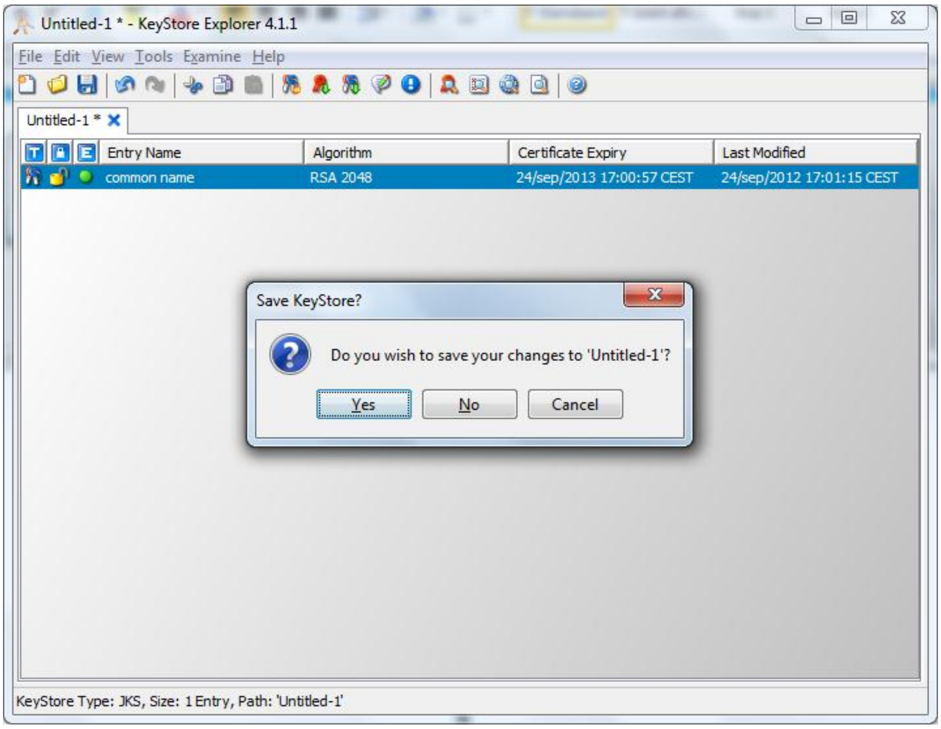
Export Private Key as OpenSSL Successful.

KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

Your private key has now been generated.

6. QUITTING KEYSTORE EXPLORER AND SAVING THE CERTIFICATE

To close the Keystore Explorer application, select “Exit” from the “File” menu or click the red cross button on the right of the screen. If you haven”t saved the certificate yet, you will be prompted to do so:

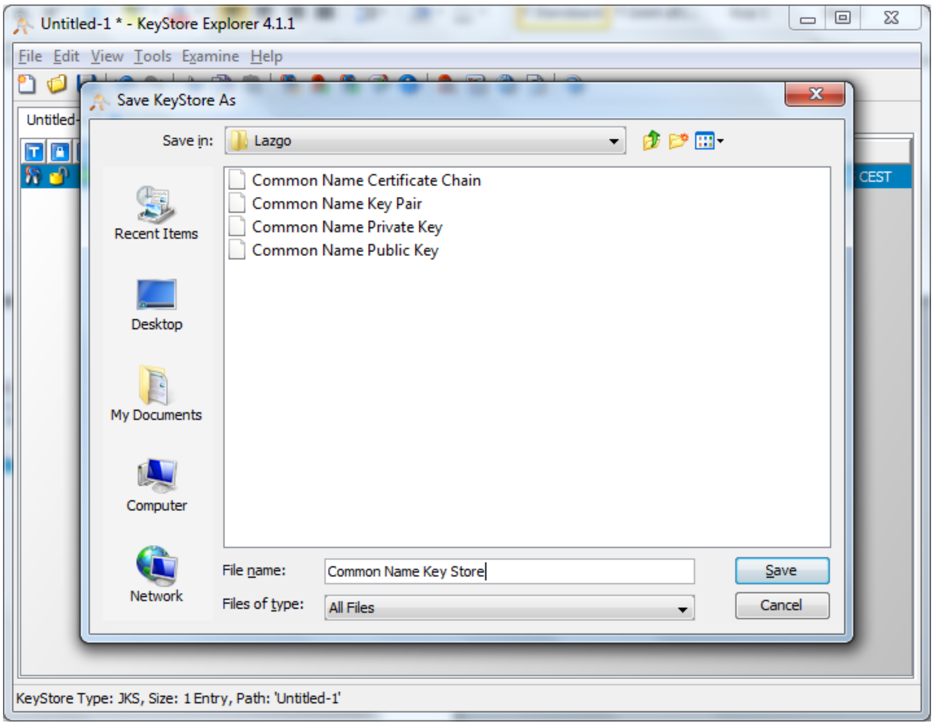

Untitled-1 * - KeyStore Explorer 4.1.1
File Edit View Tools Examine Help
Untitled-1 *
Save KeyStore?
Yes
No
Cancel

Entry Name	Algorithm	Certificate Expiry	Last Modified
common name	RSA 2048	24/sep/2013 17:00:57 CEST	24/sep/2012 17:01:15 CEST

Do you wish to save your changes to 'Untitled-1'?

KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

Click “Yes” to save the certificate. The following screen is shown:



Untitled-1 * - KeyStore Explorer 4.1.1

Save KeyStore As

Save in: Lazgo

Common Name Certificate Chain
Common Name Key Pair
Common Name Private Key
Common Name Public Key

File name: Common Name Key Store

Files of type: All Files

KeyStore Type: JKS, Size: 1 Entry, Path: 'Untitled-1'

Enter the name of the file and click the “Save” button to proceed. The application is automatically terminated.

7. USING CERTIFICATES WITH IDEAL

Please check the instructions in the iDEAL integration guides how to manage your certificates. You will need to install the certificate chain on your webserver. The public key of your certificate needs to be uploaded to the iDEAL Merchant Dashboard.