



En el siguiente documento se detalla los pasos a seguir para poder generar transacciones con interbanking.

Los requisitos para poder realizarlas transacciones son, generar un certificado digital, generar claves pública y privada y cargarlas en los respectivos servidores.

Debe contar con los datos operativos de interbanking para acceder a la aplicación.

Contenido del documento

Configuración del servidor:

[cURL](#)

[openssl](#)

Instalación del KeyStore

Generación de Certificado y clave pública y privada:

[Keystore](#)

[Key Pair](#)

[Export Certificado](#)

[Export Keys](#)

[Export Private Key](#)

Carga de Archivos:

[XX.cer](#)

[Private Key](#)

Configuración del servidor:

cURL

Permite enviar HTTP-Headers desde PHP.

Para habilitarla en el server solo haga en el php.ini lo siguiente:

- Buscar la línea "extension=php_curl.dll"
- Quitar el ;(punto y coma) de comienzo de línea
- Reiniciar el servicio

openssl

Esta librería es para mantener sesiones seguras SSL mediante certificados de seguridad.

Para instalar debe seguir estos pasos:

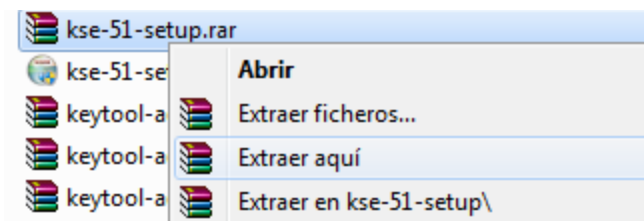
- Descargar OpenSSL
- Si se usa en Windows Server seguramente hay que instalar la libreria del C++
- Seguir los pasos de instalación desde la descarga
- Buscar en el php.ini "extension=php_openssl.dll"
- Quitar el ;(punto y coma) de comienzo de línea
- Reiniciar el servicio

Instalación del KeyStore

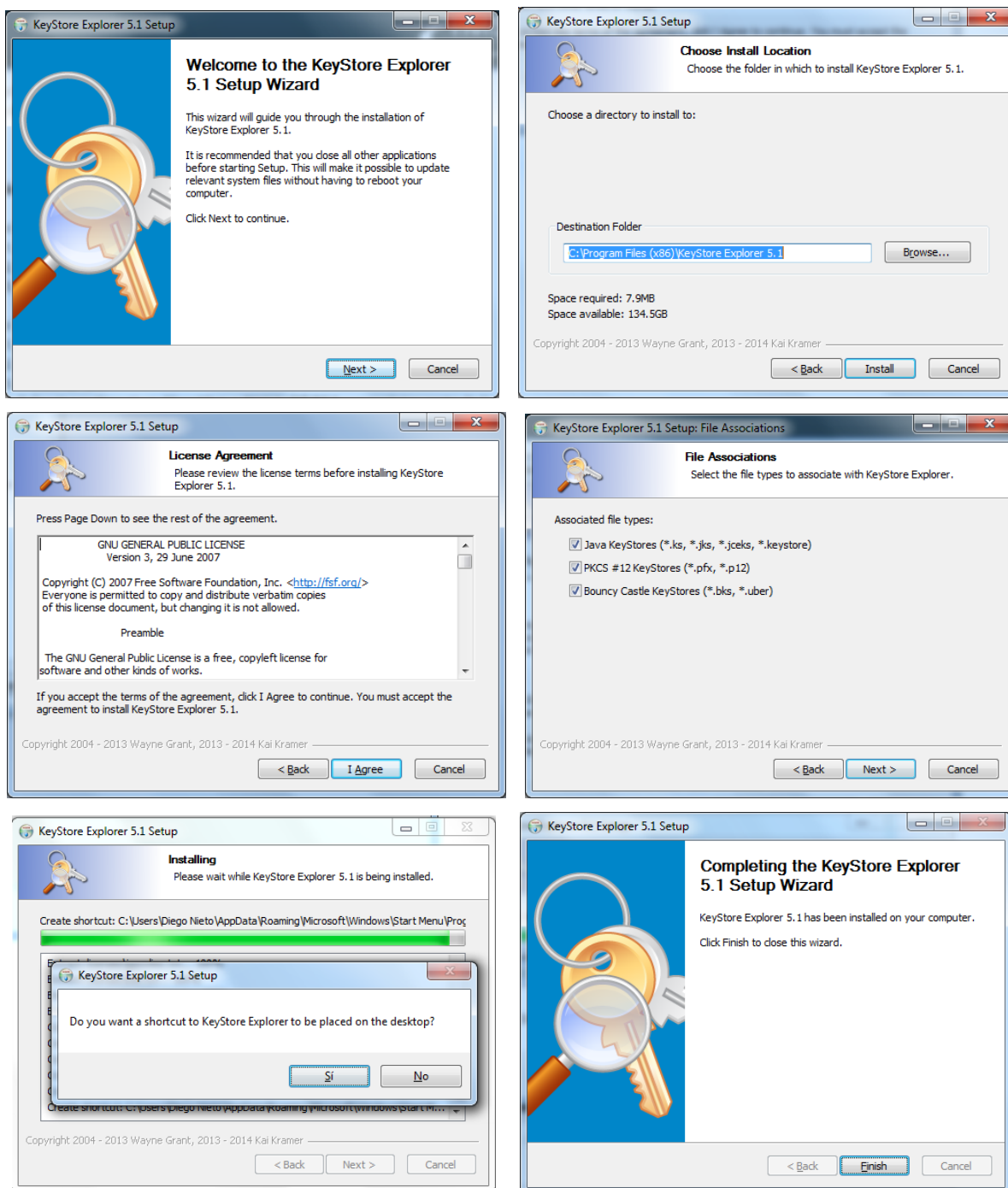
Ingresa a la aplicación, en el menú principal **Config->Config**. En el apartado **Certificado** descargar **kse-51-setup.rar**



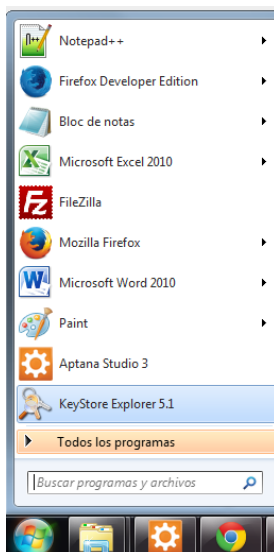
y descomprimirlo.



Acceder a **kse-51-setup.exe** y seguir los siguientes pasos para la instalación del KeyStore.



La instalación no debería generar complicaciones. Una vez instalada la aplicación accedemos a la misma.



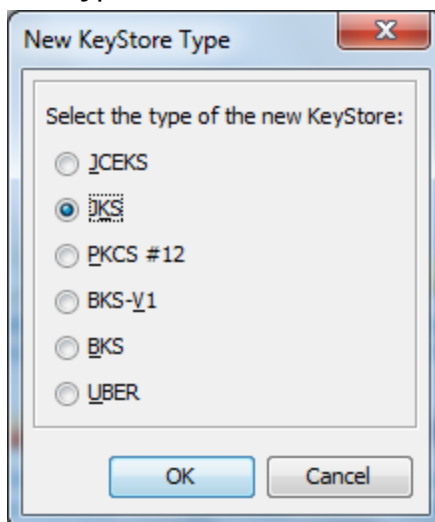
Generación de Certificado y clave pública y privada:

Keystore

1. Click en File

1.1. New Key

1.2. Seleccionar New KeyStore type = **JKS**



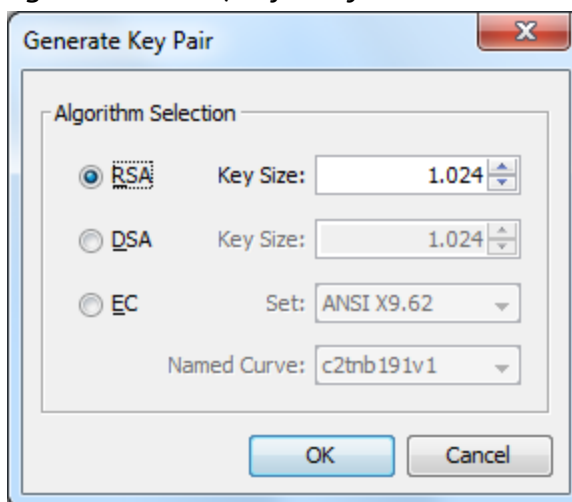
1.3. Presionar OK

Key Pair

2. Click en Tools

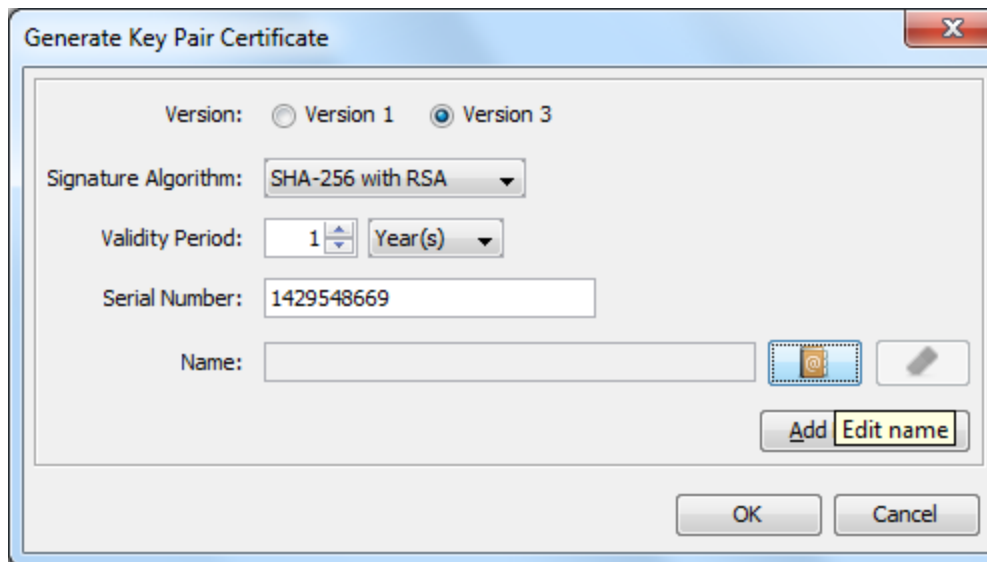
2.1. Generate Key Pair

2.2. Seleccionar Key Algorithm = **RSA**, dejar key size = **1024**



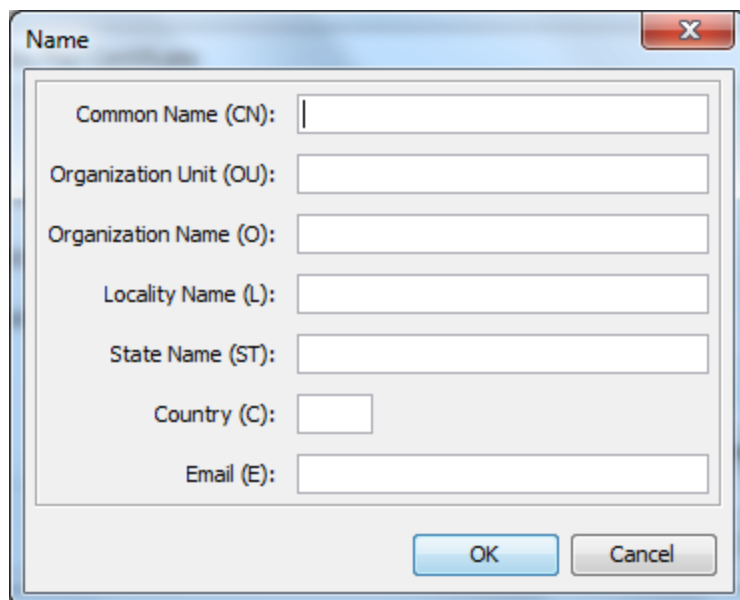
2.3. Presionar OK

2.4. Seleccionar Signatura Algorithm = **SHA1withRSA** y completar resto de los campos



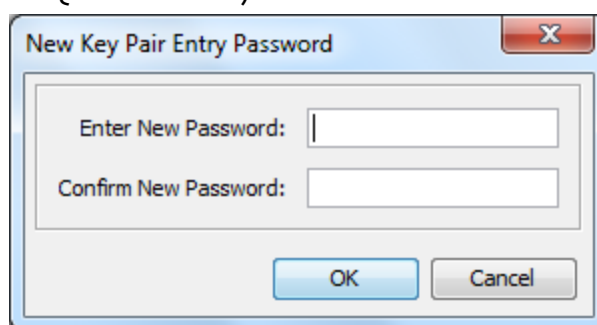
2.5. Presionar OK

2.6. Ingresar alias del certificado

A dialog box titled "Name" with a close button (X) in the top right corner. It contains several text input fields: "Common Name (CN):", "Organization Unit (OU):", "Organization Name (O):", "Locality Name (L):", "State Name (ST):", "Country (C):", and "Email (E):". At the bottom, there are "OK" and "Cancel" buttons.

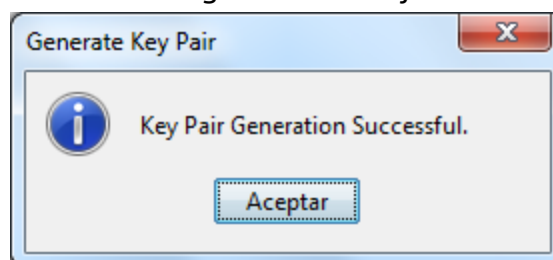
2.7. Presionar OK

2.8. Ingresar password y confirmación (SE ACONSEJA INGRESAR **MISMA** PASSWORD EN TODOS LOS CASOS QUE SOLICITE)

A dialog box titled "New Key Pair Entry Password" with a close button (X) in the top right corner. It contains two text input fields: "Enter New Password:" and "Confirm New Password:". At the bottom, there are "OK" and "Cancel" buttons.

2.9. Presionar OK

2.10 Si todo ok, esta se muestra el siguiente mensaje

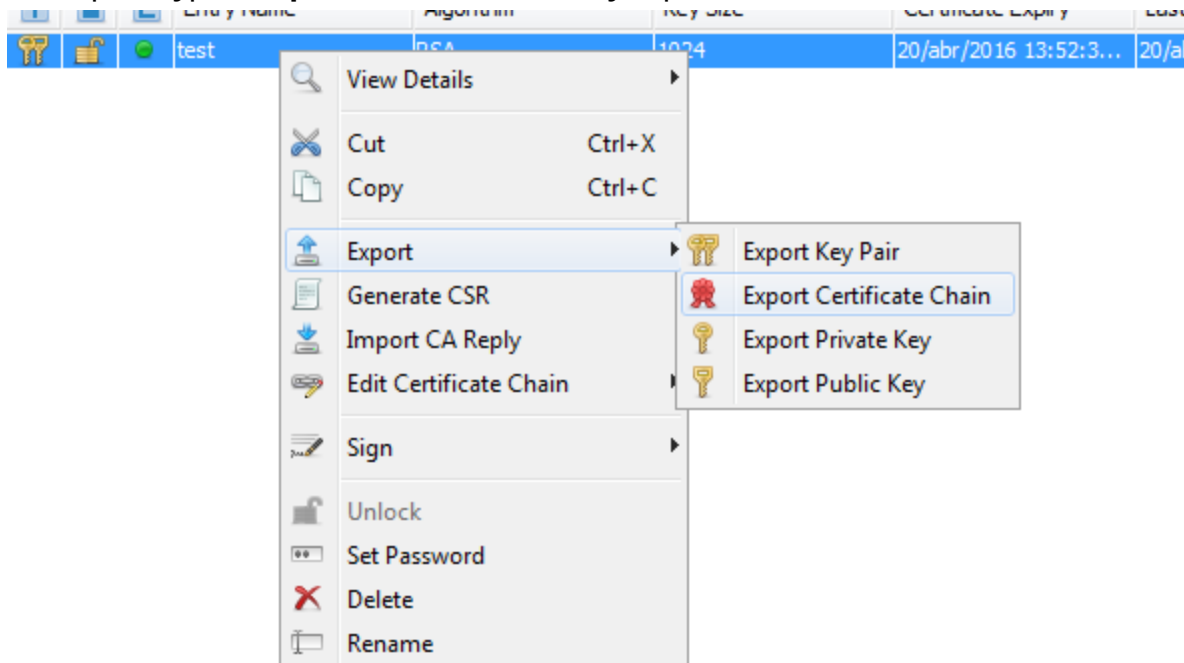
A dialog box titled "Generate Key Pair" with a close button (X) in the top right corner. It contains an information icon (i) and the text "Key Pair Generation Successful.". At the bottom, there is an "Aceptar" button.

Export Certificado

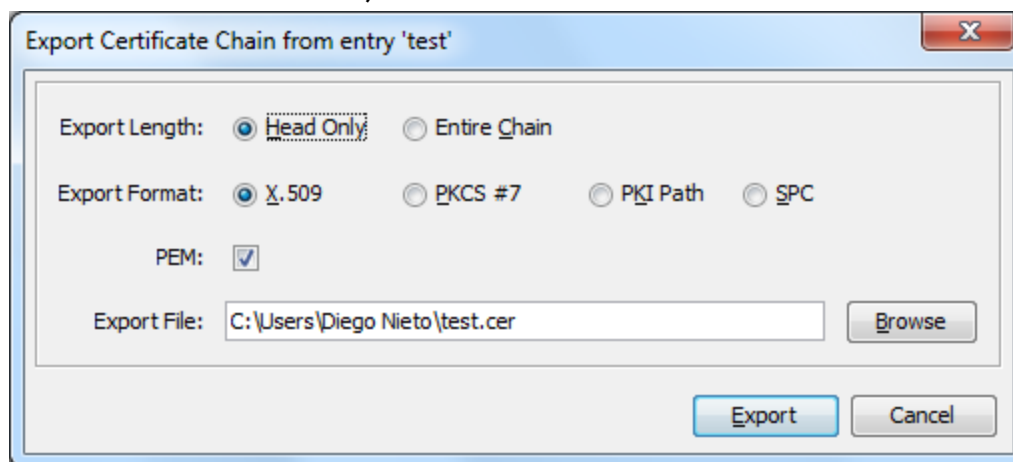
3. Click con el botón secundario del mouse sobre el keystore generado.

3.1. Export

3.2. Export Type = **Export Certificate Chain** y Export Format = **PEM encoded**



3.3. Alojarse el certificado en la carpeta que se desee, con nombre "[xxx].cer" (NO OLVIDARSE DE LA EXTENSIÓN)



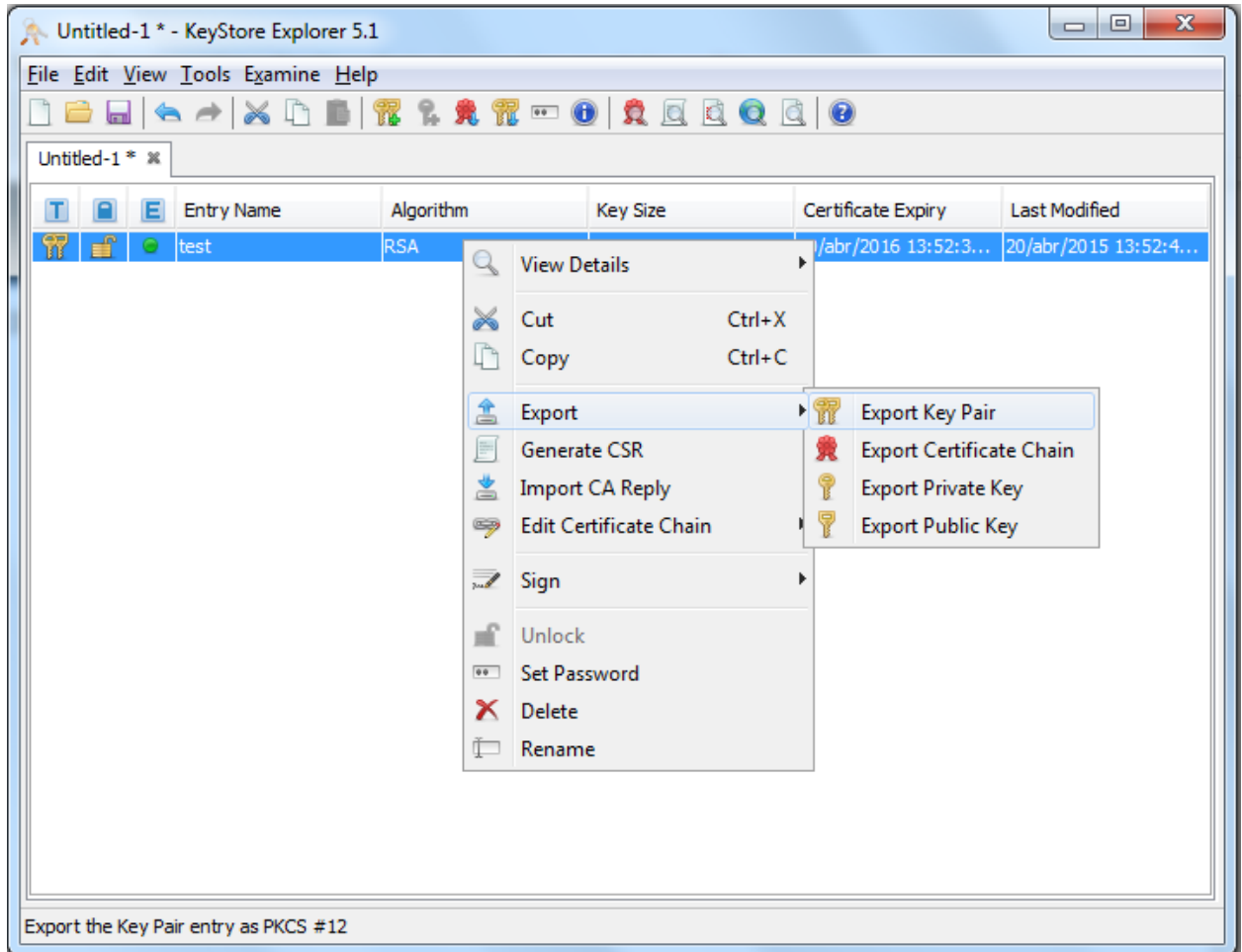
3.4. Presionar Export

Export Keys

4. Click con el botón secundario del mouse sobre el keystore generado.

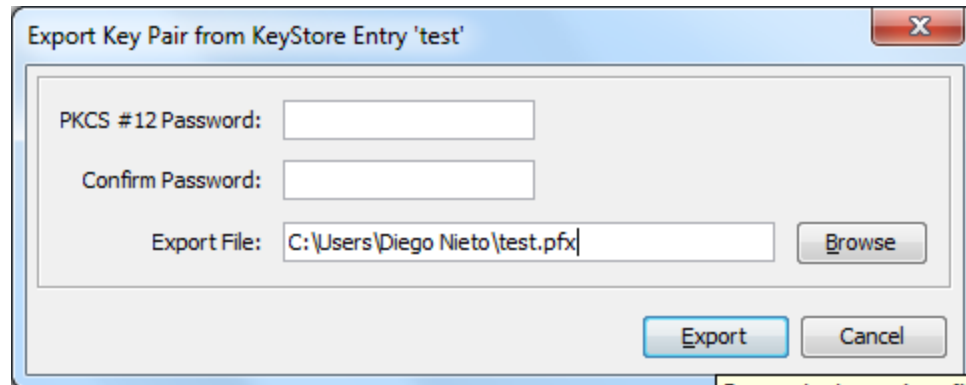
4.1. Export

4.2. Export Type = **Export Key Pair**

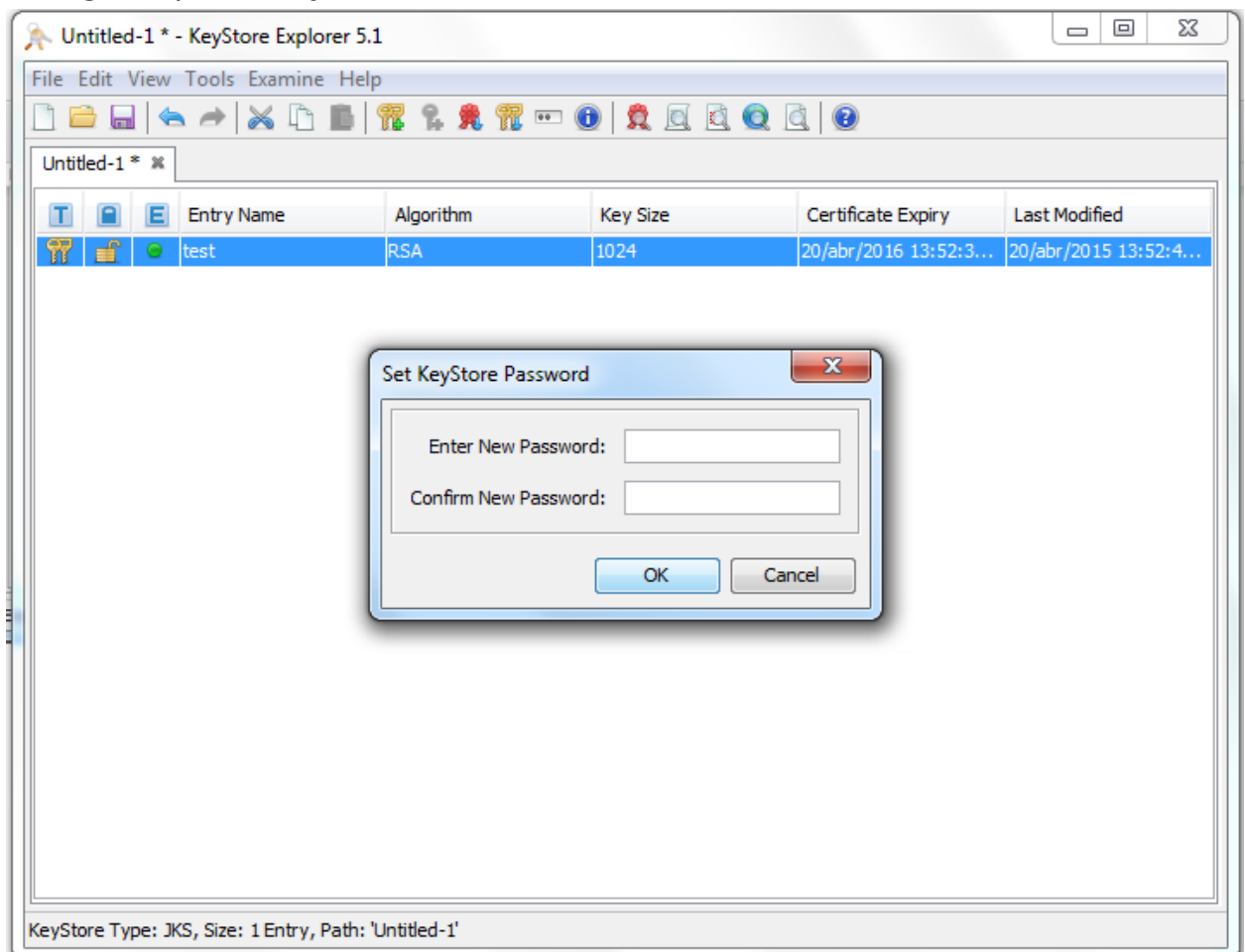


4.3. Ingresar password y confirmación de la misma (esta sería la clave privada).

4.4. Alojar el certificado en la misma carpeta que se utilizó previamente con nombre "[xxx].pfx"



- 4.6. Presionar Export
- 5. Click en File
 - 5.1. Save Keystore As...
 - 5.2. Ingresar password y confirmación de la misma.



5.3. Presionar OK

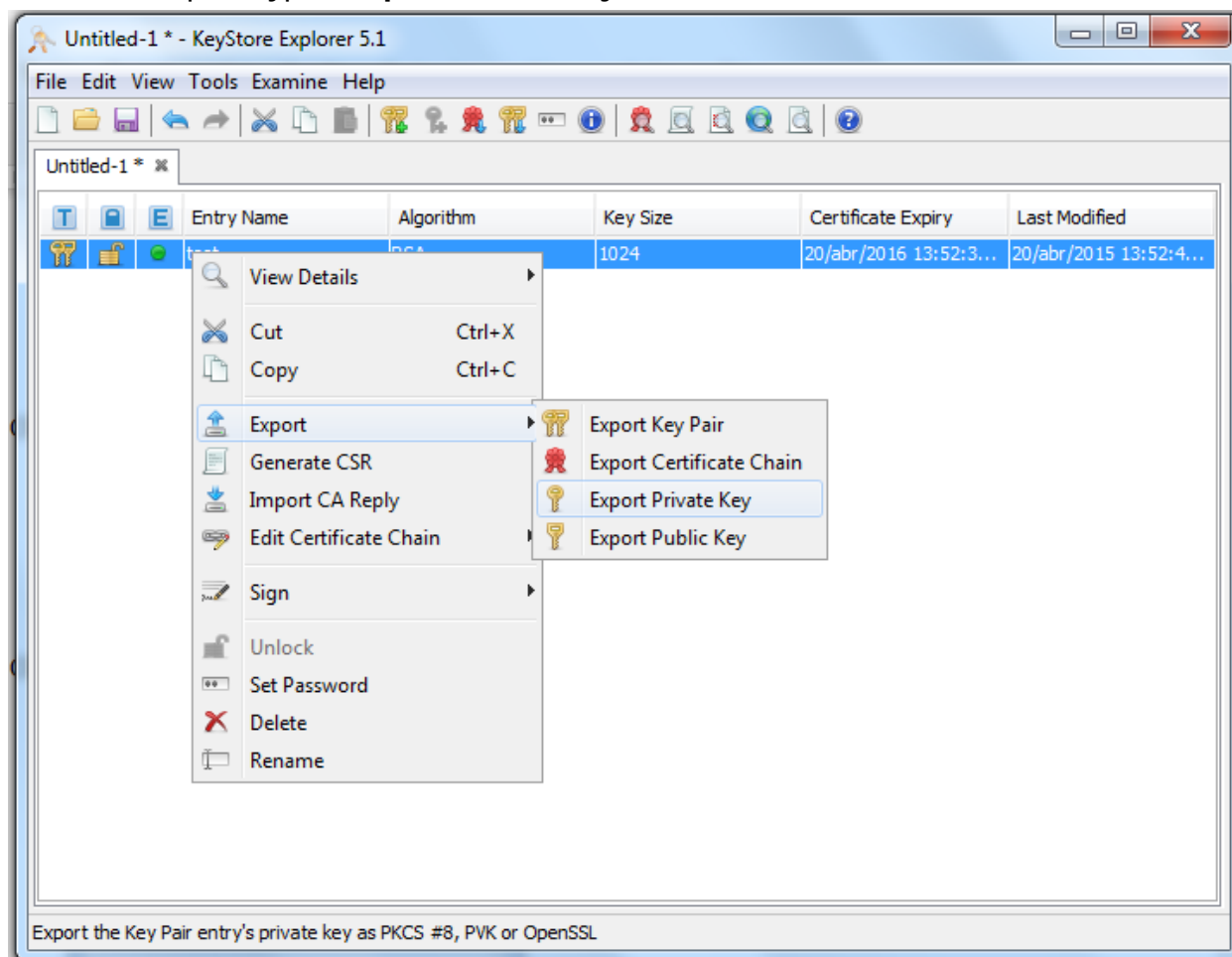
5.4. Alojar el keystore en la misma carpeta que se utilizó previamente, con nombre "[xxx].ks"

Export Private Key

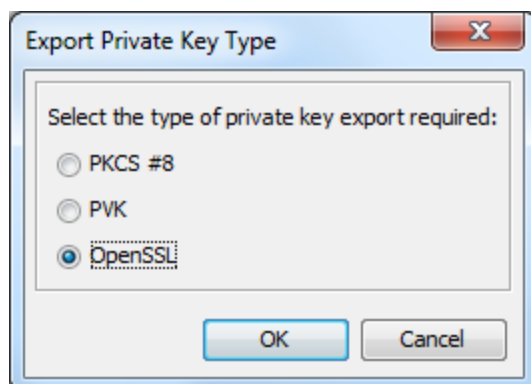
6. Click con el botón secundario del mouse sobre el keystore generado.

6.1. Export

6.2. Export Type = **Export Private Key**

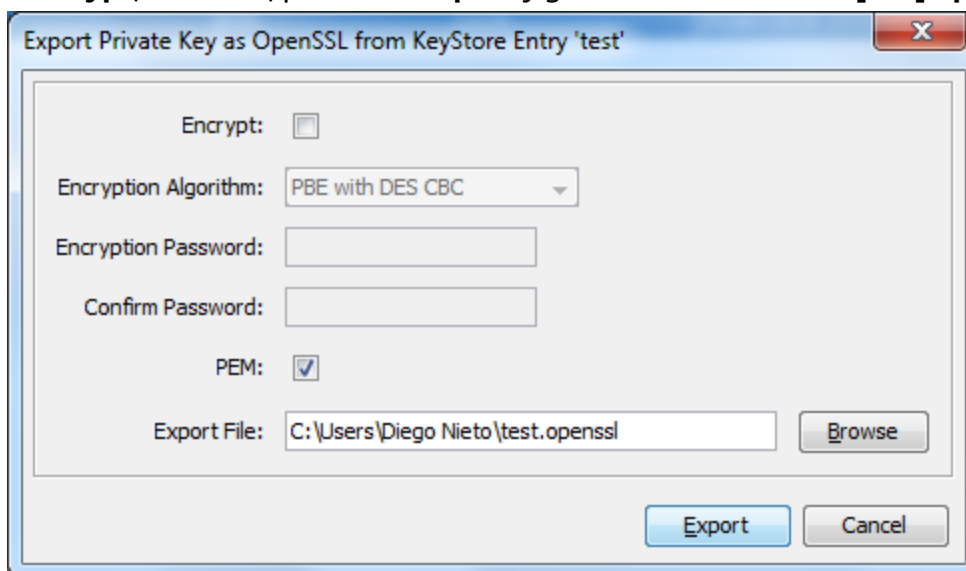


5.1. Seleccionar OpenSSL



5.3. Presionar OK

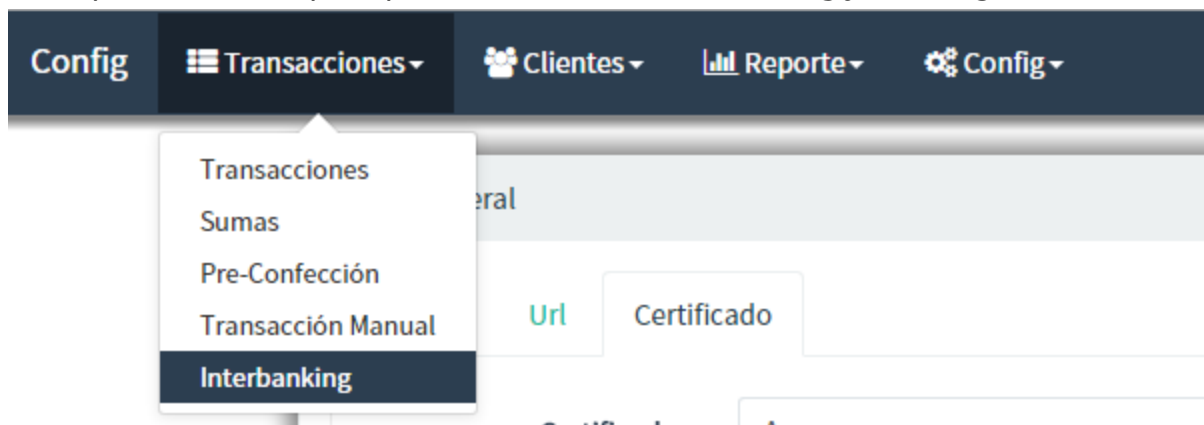
5.4. Sin **Encrypt**, con **PEM**, presionar **Export** y guardamos el archivo "[xxx].openssl"



Carga de Archivos:

[xxx].cer

En la aplicación, menú principal **Transacciones>Interbanking** y hacer login



Dentro de interbanking **Administración->ABM|Configuración Datos**, seleccionamos la opción **Comunidad**.



En el apartado **Certificado Digital** cargamos el archivo “[xxx].cer”

Certificado Digital		Modificar
Estado:	Habilitado	
Fecha de vencimiento:	17/04/2016	
Certificado de interBANKING:	Descargar certificado de interBANKING	

Debe quedar así.

Certificado Digital

Datos del Certificado

Modificar

Denominación:	E=amena@amena.org.ar,C=ES,ST=Mendoza,L=Mendoza,O=A.M.E.N.A.,OU=Amena,CN=Amena E=amena@amena.org.ar,C=ES,ST=Mendoza,L=Mendoza,O=A.M.E.N.A.,OU=Amena,CN=Amena
Fecha de vencimiento:	17/04/2016
Estado:	Habilitado

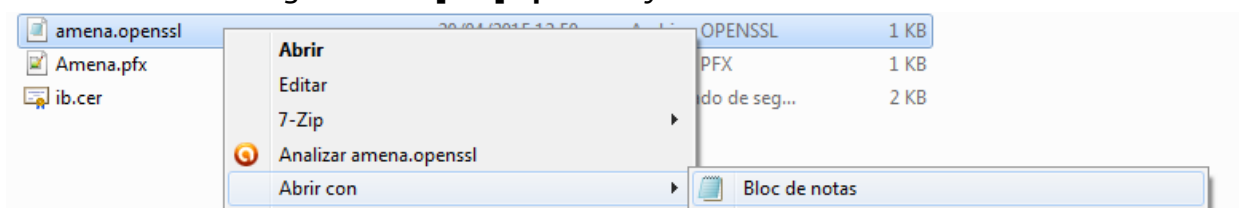
Detalle

CANCELAR

ELIMINAR

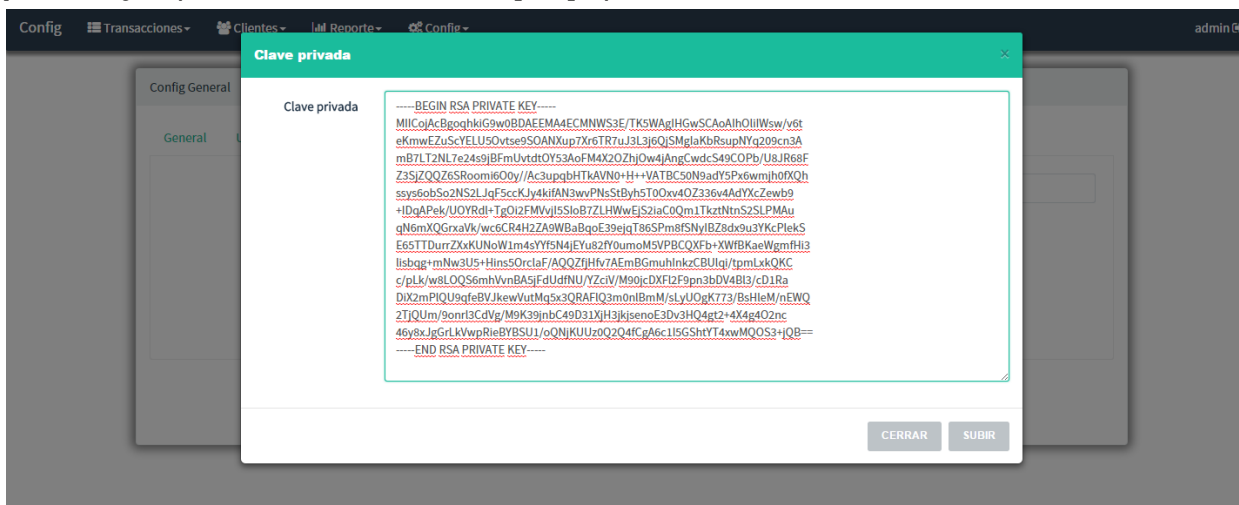
Private Key

Buscamos el archivo generado "[xxx].openssl" y lo abrimos con el bloc de notas.



Copiamos el todo el contenido del mismo.

En la aplicación, menú principal **config->Config->Certificado**, seleccionamos 'clave privada' y copiamos el contenido de "[xxx].openssl"



Si quiere puede guardar un backup de los archivos generados, en config general, certificados. Haciendo click en el subir archivo podrá guardar en el servidor, los archivos "[xxx].cer", "[xxx].ks", "[xxx].pfx", el archivo "[xxx].openssl" no debe subirlo al servidor.