



Banco de la República
Bogotá D. C., Colombia

Dirección General de Tecnología
Departamento de Seguridad Informática

**DSI-GI-97 Manual para la generación y transformación de credenciales emitidas por
la CA BANREP**

Agosto de 2014

Versión 1

CONTENIDO

1. INTRODUCCIÓN	3
1.1 AUDIENCIA	3
1.2 ALCANCE	3
2. CONSIDERACIONES ESPECIALES	4
3. GENERACIÓN DE CREDENCIALES PARA EL SUSCRIPTOR	5
3.1 PROCEDIMIENTO PARA INICIALIZAR EL TOKEN	5
3.1.2 CREACIÓN CERTIFICADO DIGITAL DEL SUSCRIPTOR.....	9
3.1.3 RECUPERACIÓN DE CERTIFICADO DIGITAL PARA SUSCRIPTORES	17
4. GENERACIÓN DE CREDENCIALES PARA PROCESOS AUTOMÁTICOS Y B2B (BUSINESS TO BUSINESS) 24	
CERTIFICADOS BUSINESS TO BUSINESS (B2B):.....	27
CERTIFICADOS PARA AUTOMATIZACIÓN DE OPERACIONES CRIPTOGRÁFICAS	28
5. TRANSFORMACIÓN DE CREDENCIALES	31

1. INTRODUCCIÓN

El propósito de este documento es dar a conocer los pasos necesarios para realizar la creación y recuperación de los certificados digitales emitidos por la Entidad de Certificación Digital CA BANREP definidos en su Declaración de Políticas de Certificación- DPC (<http://www.banrep.gov.co/es/contenidos/page/declaracion-prcticas-certificacion-ca-banrep>).

1.1 Audiencia

Este documento está dirigido a todas las entidades financieras que requieren usar un certificado digital emitido por la CA BANREP para intercambiar información con los servicios electrónicos que ofrece el Banco de la Republica.

1.2 Alcance

En este documento se describen los requerimientos necesarios para realizar procesos de creación y recuperación de certificados digitales para suscriptores, procesos automáticos y comunicación B2B.

2. CONSIDERACIONES ESPECIALES

A continuación se presentan los requerimientos y consideraciones necesarias que se deben tener en cuenta para la generación, recuperación y transformación de Credenciales.

Se debe solicitar la creación y/o recuperación del profile PKI siguiendo el procedimiento establecido en la DPC (<http://www.banrep.gov.co/es/contenidos/page/declaracion-prcticas-certificacion-ca-banrep>), el Banco de la República enviará la información de activación (“Reference Number” y “Authorization Code”) necesarios para realizar la operación requerida.

La Entidad debe tener conexión con WSEBRA por medio de los canales dedicados que las entidades tienen contra el Banco de la República. La conexión se realiza mediante el agente WSAM que se activa al momento de ingresar al portal WSEBRA.

En el equipo en donde se desee hacer la creación o recuperación del certificado digital, se deben tener instalado los componentes de software descritos a continuación, estos componentes son los necesarios para el manejo de las credenciales y son suministrados por el Banco de la República.

- Entrust Security Provider (ESP).
- Safenet Authentication Client (SAC)

*El manual de instalación “**4. SUCED-ENTR-43 Manual de Instalación y Uso SUCEDGUI.pdf**” se encuentran en <https://caribe.banrep.gov.co/emisor>,

Para realizar la transformación de Credenciales se hace necesario utilizar el software público “Portecle”. Este software es de carácter público y su descarga es gratuita.

3. GENERACIÓN DE CREDENCIALES PARA EL SUSCRIPTOR

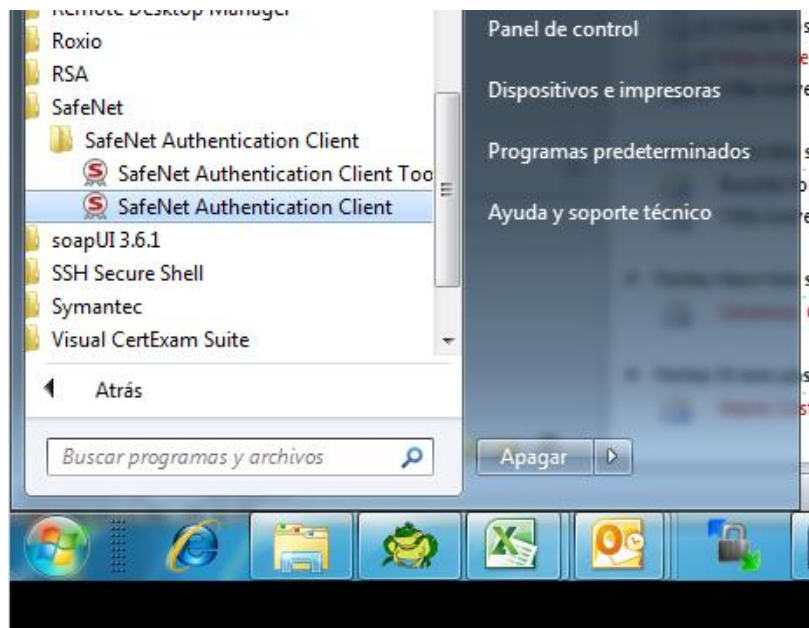
La generación de certificados digitales para el suscriptor contempla dos escenarios, creación (Enroll) y Recuperación (Recovery) del profile, en ambos casos se debe realizar el proceso de inicialización del Token, el cual se describe a continuación:

3.1 Procedimiento para Inicializar el Token

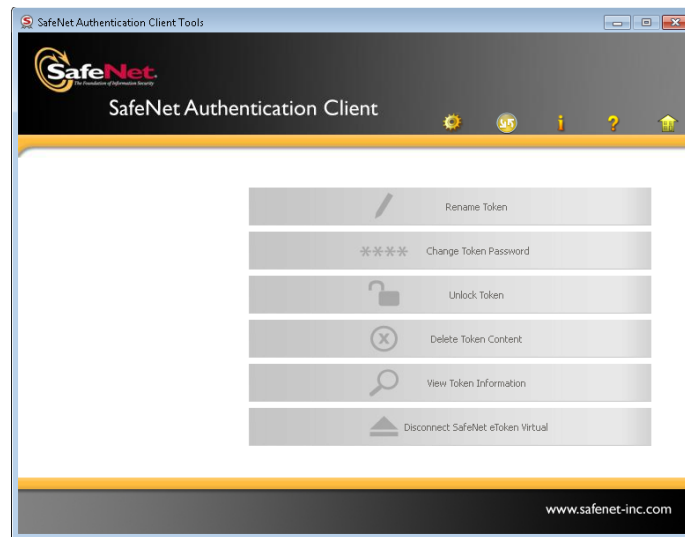
Para empezar con el proceso de creación o recuperación del certificado digital para un suscriptor, es indispensable realizar la operación **Inicializar Token**, que se describe a continuación:

1. Ingresar al Software SafeNet Authentication Client, en la cual se podrá observar una pantalla de inicio de la siguiente manera:

Se debe ejecutar el cliente “SafeNet Authentication Client” en Inicio → Todos los Programas → Safenet



2. Cuando ingresa, se observa la siguiente pantalla:



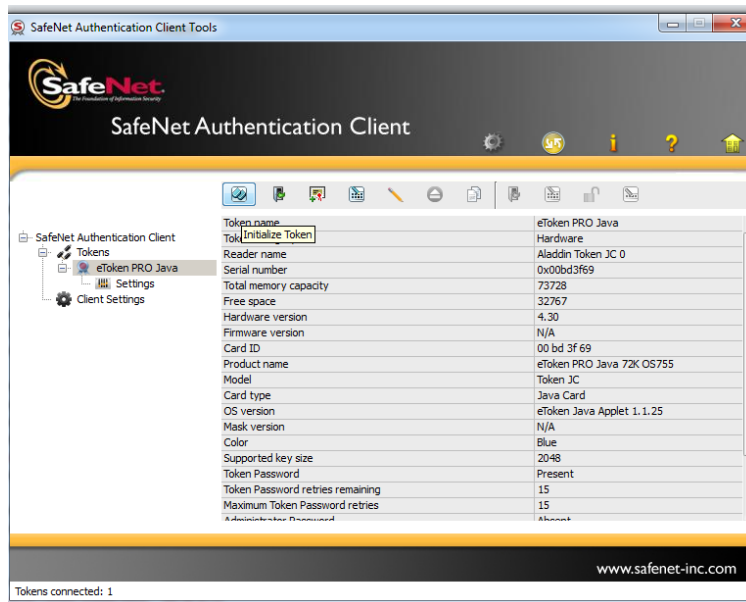
Se debe hacer clic en el icono de “*configuración*”



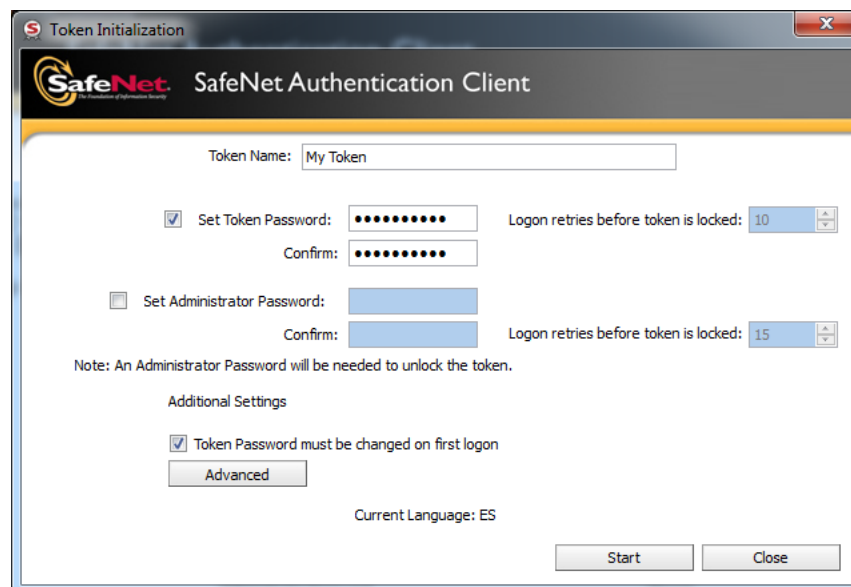
3. En la sección Tokens, debemos seleccionar el Token Correspondiente,

Token name	eToken PRO Java
Token category	Hardware
Reader name	Aladdin Token JC 0
Serial number	0x00bd3f69
Total memory capacity	73728
Free space	32767
Hardware version	4.30
Firmware version	N/A
Card ID	00 bd 3f 69
Product name	eToken PRO Java 72K OS755
Model	Token JC
Card type	Java Card
OS version	eToken Java Applet 1.1.25
Mask version	N/A
Color	Blue
Supported key size	2048
Token Password	Present

Haga clic en el icono “*Inicializar Token*”



4. En la siguiente ventana de inicialización del token,



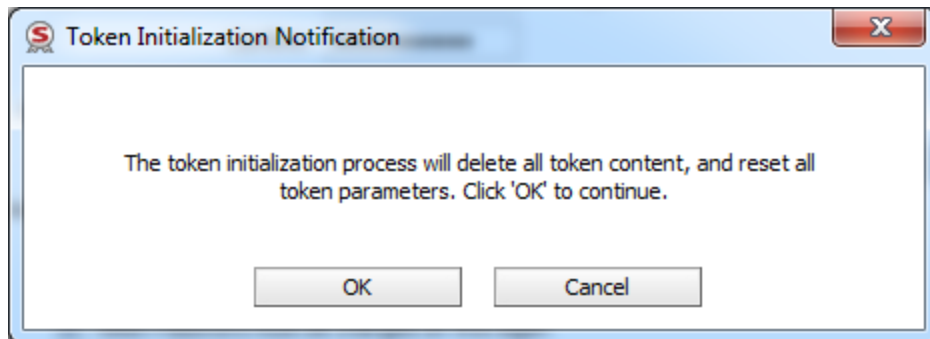
En este paso debemos indicar el Nombre del Token, el cual debe seguir la siguiente estructura: **“Cedula de ciudadanía –Login– tipo de sector -codigoEntidad – código de ciudad”**.

Ejemplo: 1070945805-cramirra-00-01000-01

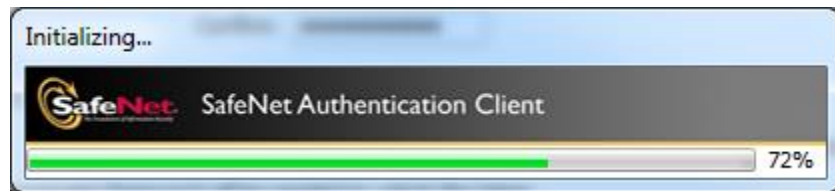
Se debe establecer el password en la Opción **“Establecer Contraseña”** o **“Set Token Password”** y confirmarlo.

Luego se debe seleccionar la opción de **“Iniciar”** o **“Start”**.

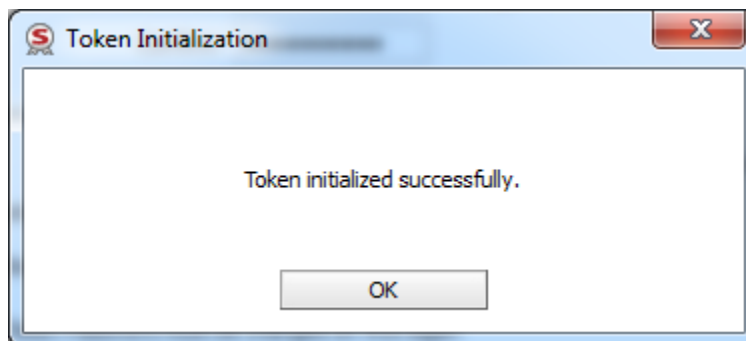
En la siguiente ventana, solicita confirmación de la operación de inicialización, se debe dar clic en el botón **“OK”** para proceder.



Se inicia la “inicialización del Token”.




Al terminar debe presentar un mensaje de inicialización exitosa.

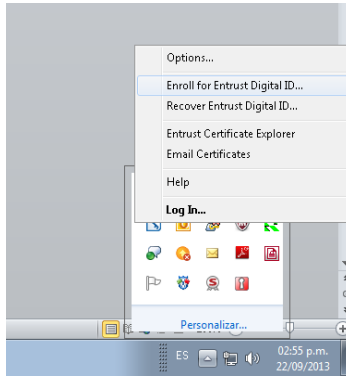


3.1.2 Creación Certificado Digital del Suscriptor

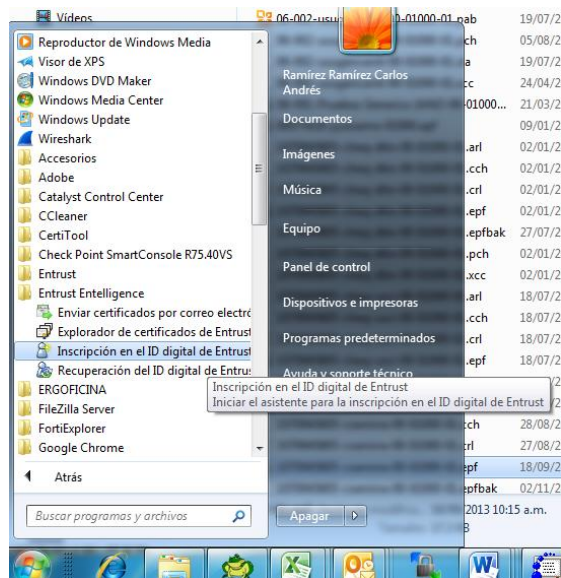
Para realizar este proceso se debe contar con la información de activación (el código de autorización y número de referencia suministrados por el Banco de la República) y con acceso a WSEBRA, y verificar la sección 2 (*Consideraciones Especiales*). El procedimiento de solicitud de certificado se define en la Declaración de Practicas de Certificación DPC para la CA – BANREP. (<http://www.banrep.gov.co/es/contenidos/page/declaraci-n-pr-cticas-certificaci-n-ca-banrep>)

Existen dos opciones de iniciar el proceso de Enroll o creación del Profile, las cuales se describen a continuación:

Opción 1: En la parte inferior izquierda del escritorio de Windows hacer clic derecho sobre el icono de ESP , procedemos a seleccionar la opción *Enroll for Entrust Digital ID*.



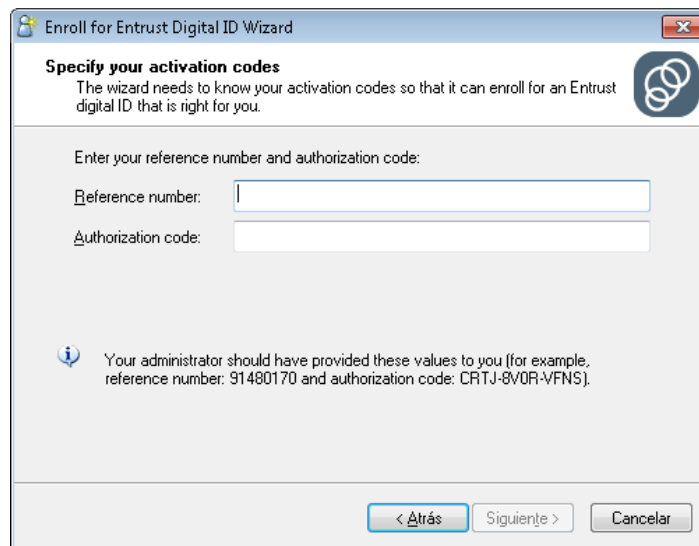
Opción 2: Nos dirigimos Inicio → Todos los programas → Entrust Entelligence → *“Inscripción en el ID Digital de Entrust”*.



Una vez seleccionada esta opción, se abrirá la siguiente ventana. Haga clic en “siguiente”.

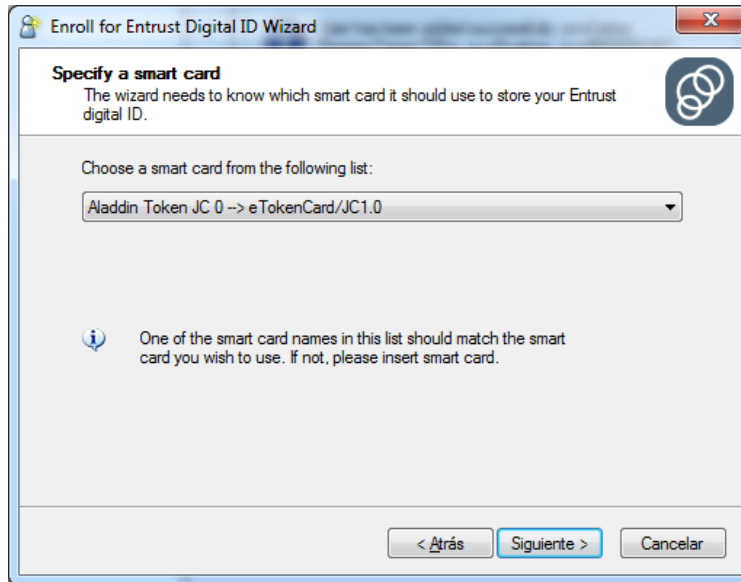


Aparece la siguiente ventana, ingresar el código de autorización y numero de referencia provistos por el Banco de la República y dar clic en “Siguiente”

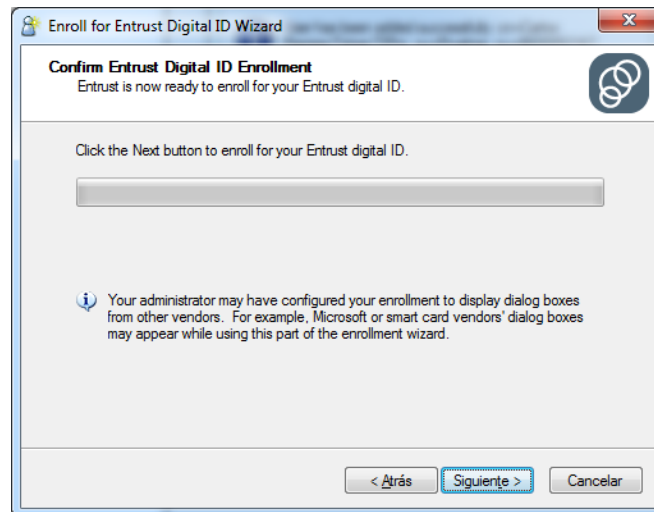


El sistema detectará que el Token está conectado en el PC.

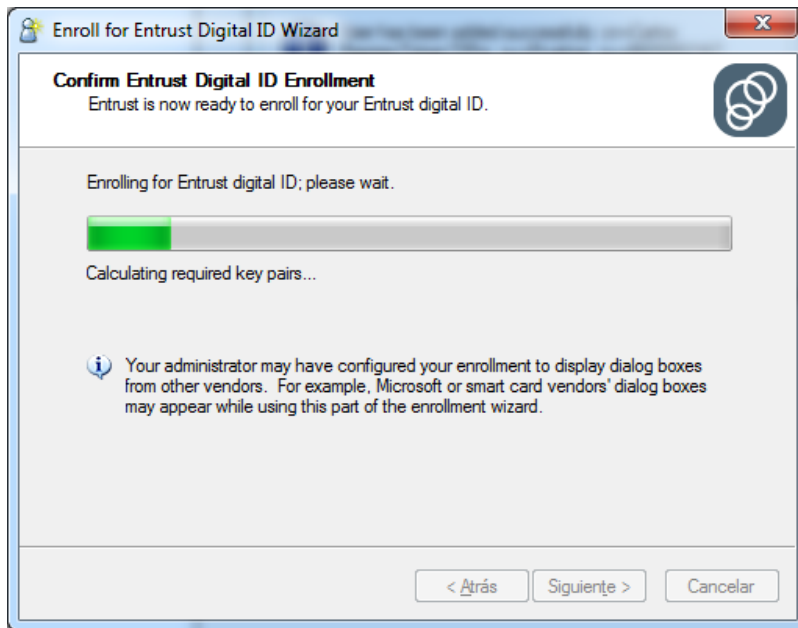
Hacer clic en “Siguiente”.



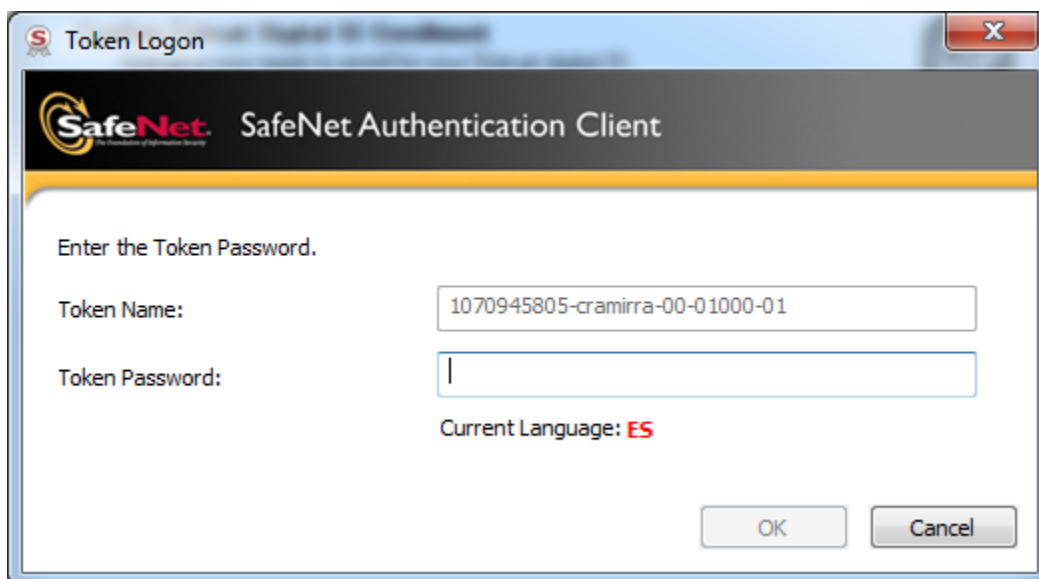
Se inicia el proceso de creación, para realizar esta actividad se comunicación con la infraestructura tecnológica del Banco por lo que debe tener abierta la sesión de WSEBRA, dar clic en “Siguiente”



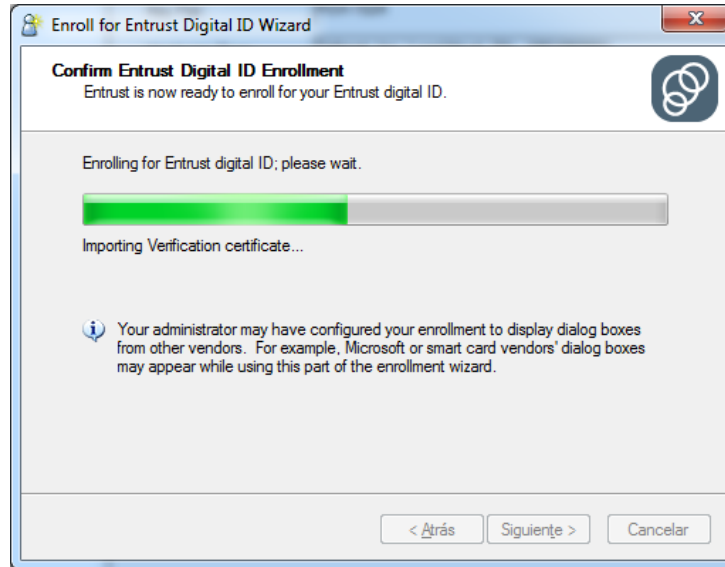
Se iniciará el proceso de Enroll del certificado.



Para poder almacenar el Profile en el token, el cliente SafeNet Authentication Client solicitará la clave del Dispositivo (Ver sección **3.1 Inicializar Token**), por favor ingresar la clave y dar clic en “OK”.



Si la contraseña ingresada corresponde al token, el sistema continuará con el proceso de creación.

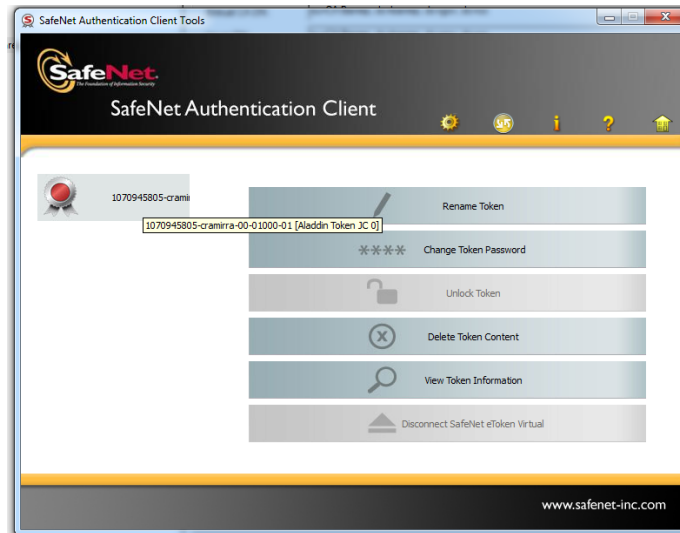



Una vez finalice, se indica que el proceso ha terminado “*The Enroll for Entrust Digital ID Wizard has completed*”, de clic en “Finalizar”

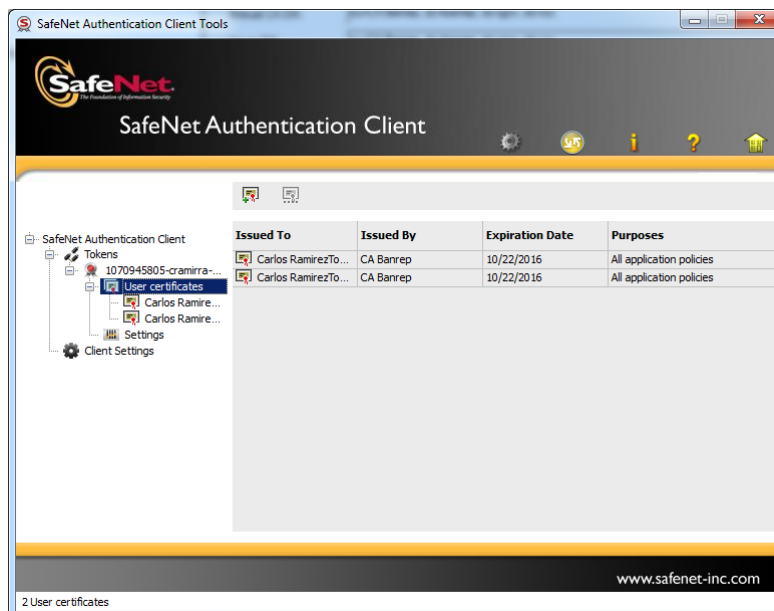


Nota: Si la creación del certificado no termino correctamente, debe verificar que se encuentra en línea a través de WSEBRA, si el problema continúa debe contactar a Soporte Informático del Banco de la República.

A continuación, debe verificar la creación del Profile abriendo el cliente "Safenet Authentication Client", en la ventana principal (Parte Izquierda) se ve la información del nombre de nuestro Token.

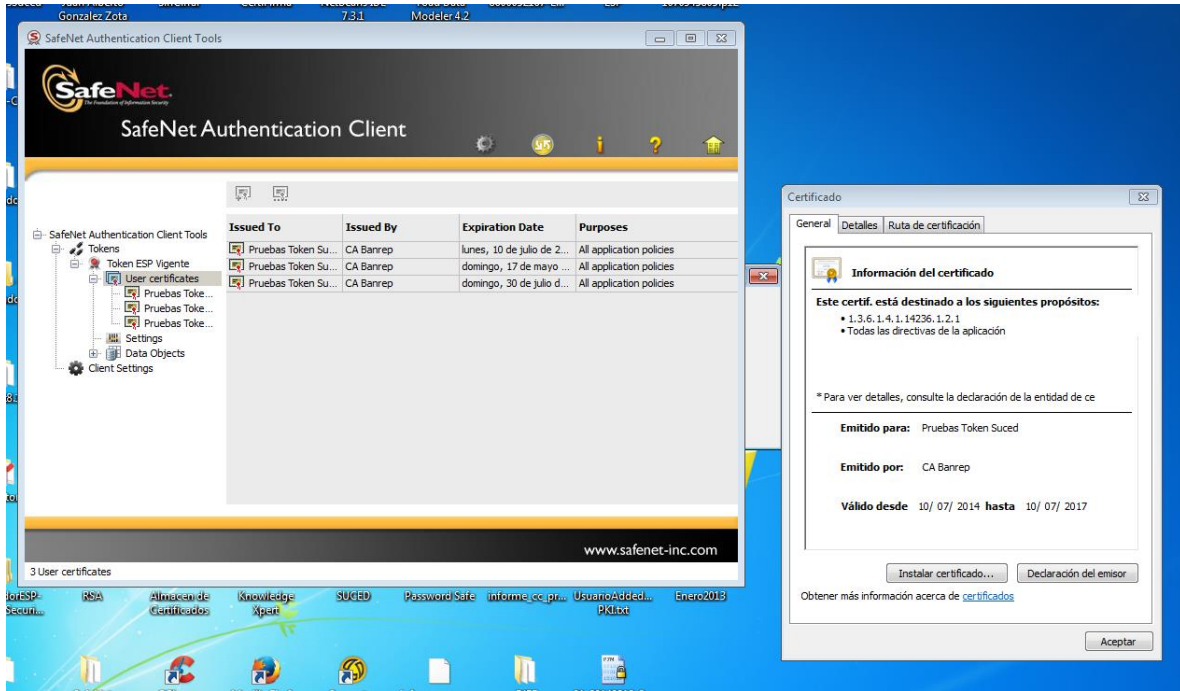


Seleccionar la opción , Se deben observar el par de certificados almacenados (para operaciones de firma y cifrado).



En esta sección podremos validar los datos del certificado, los cuales deben tener una relación directa con la solicitud realizada en el formato “Novedades de Suscriptor Entidad”


de Certificación - CA BANREP” (BR-3-598-0). Información que se consulta realizando doble clic sobre el certificado.

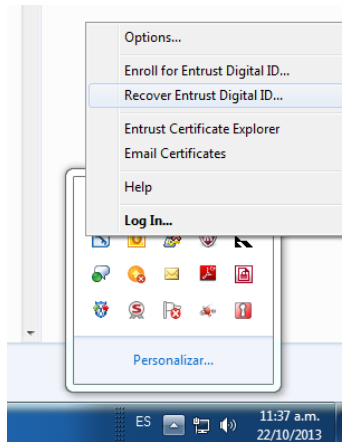


3.1.3 Recuperación de Certificado Digital para Suscriptores

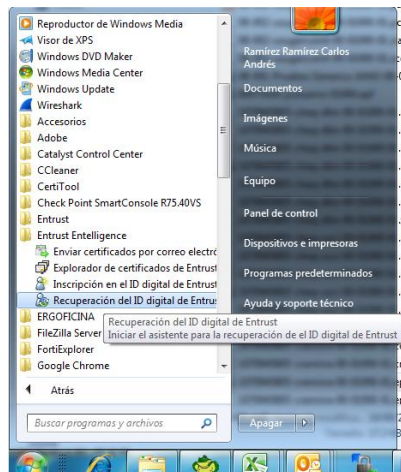
Para realizar este proceso se debe contar con la información de activación (el código de autorización y número de referencia suministrados por el Banco de la República) y con acceso a WSEBRA, y verificar la sección 2 (*Consideraciones Especiales*). El procedimiento de solicitud de recuperación del certificado se define en la Declaración de Practicas de Certificación DPC para la CA – BANREP. (<http://www.banrep.gov.co/es/contenidos/page/declaraci-n-pr-cticas-certificaci-n-ca-banrep>)

Existen dos opciones de iniciar el proceso de Recuperación del certificado, las cuales se describen a continuación:

Opción 1: Nos dirigimos a la parte inferior izquierda del escritorio de Windows y de clic derecho sobre el icono de ESP , procedemos a seleccionar la opción **Recover Entrust Digital ID**.



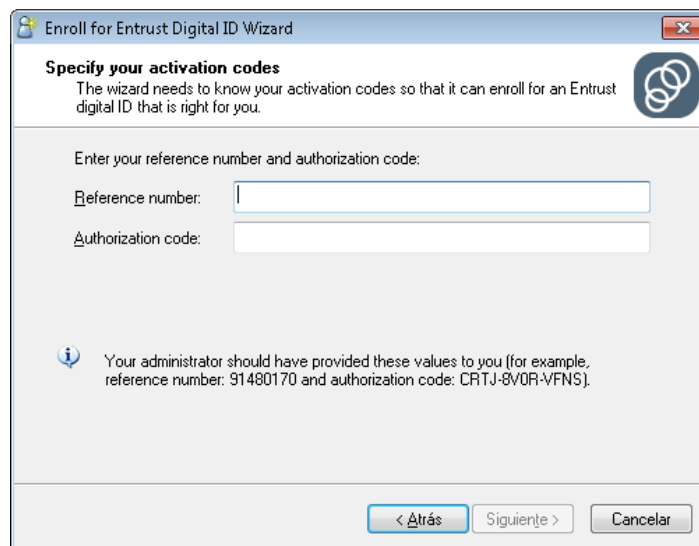
Opción 2: Diríjase a Inicio → Todos los programas → Entrust Entelligence → “*Recuperación del ID Digital de Entrust*”.



Una vez seleccionada esta opción, se abrirá la siguiente ventana, seleccionar “siguiente”.

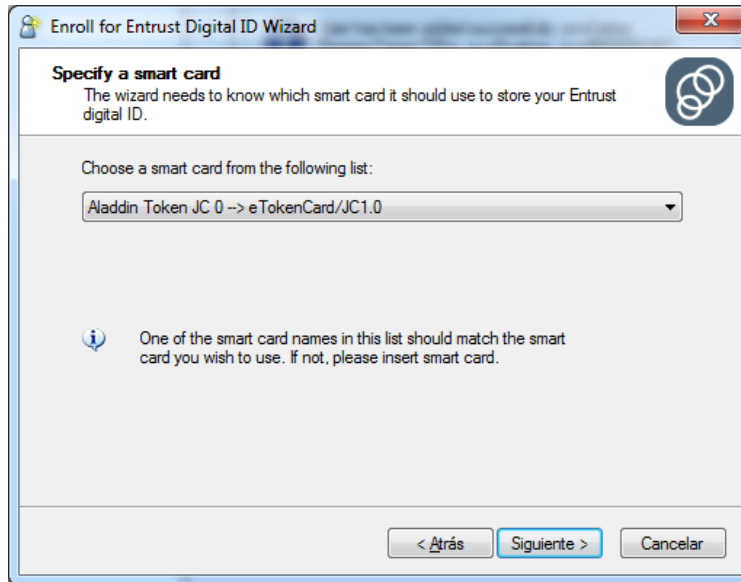


A continuación, se debe ingresar el código de autorización y número de referencia provistos por el Banco de la República y dar clic en “Siguiete”

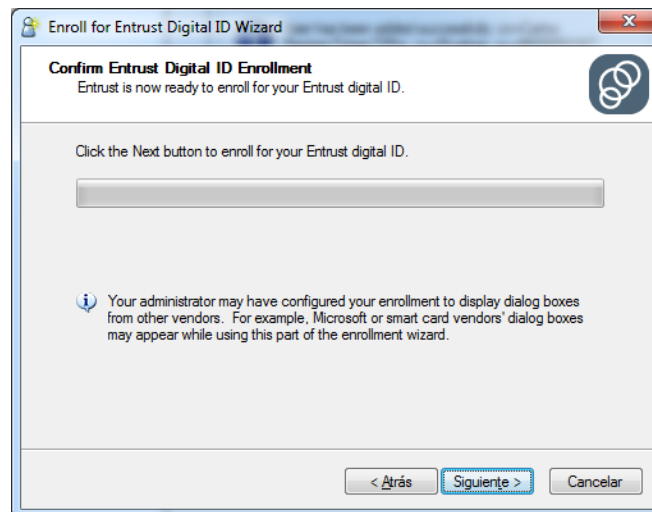


El sistema detectará que el Token está conectado en el PC.

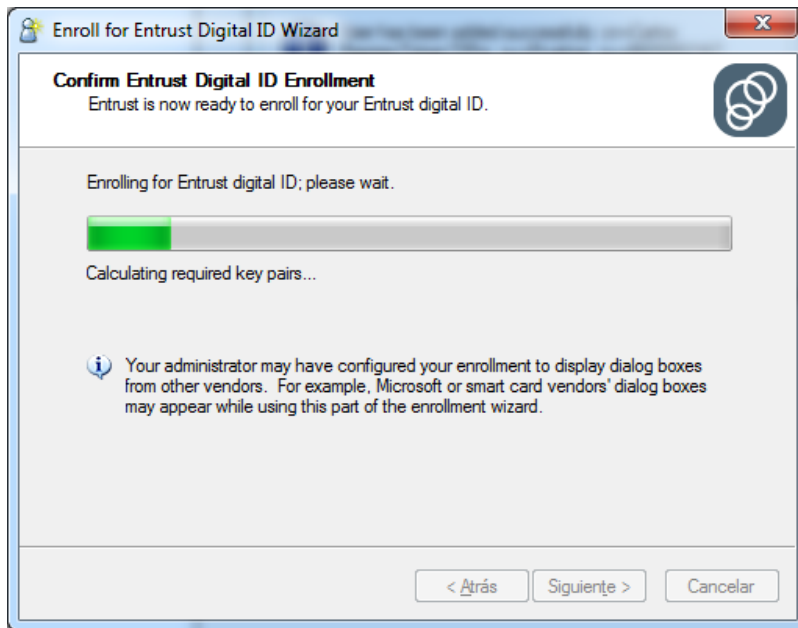
Seleccionar “Siguiete”.



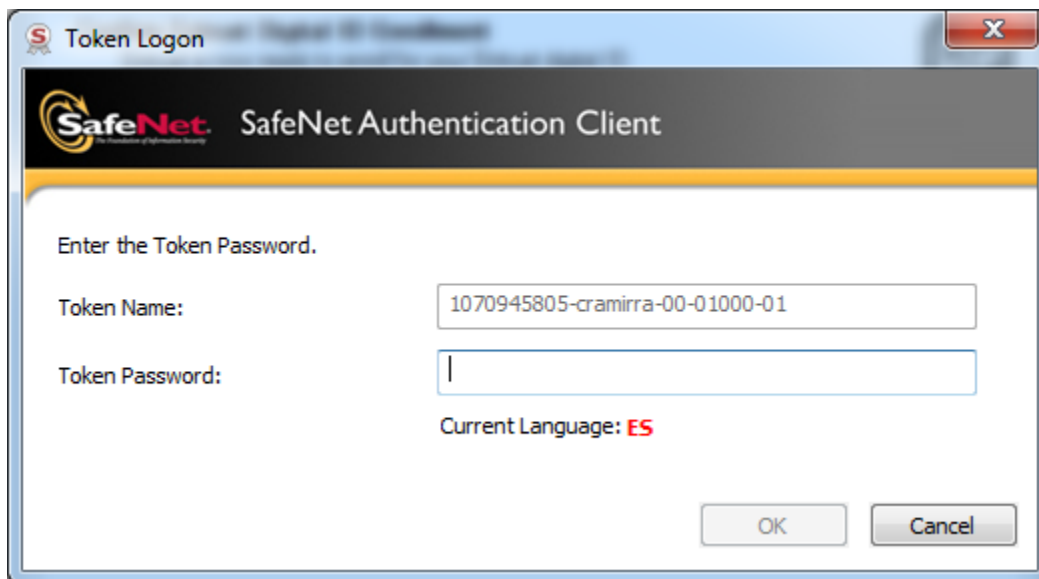
Seleccionar "Siguiete"



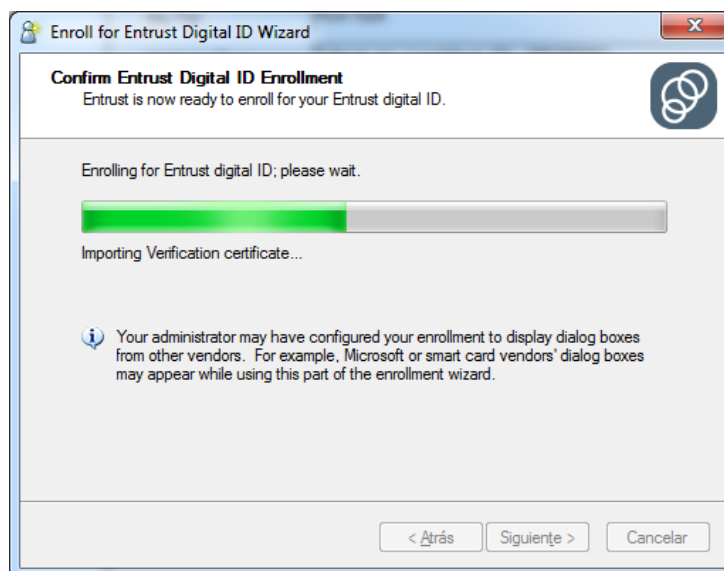
Al seleccionar "Siguiete" comenzara el proceso de Enroll del certificado.



El cliente SafeNet Authentication Client solicita la clave del token (Ver sección **3.1 Inicializar Token**), ingresarla y seleccionar OK.



Después de digitar la contraseña correspondiente, el sistema continuará con el proceso de creación.

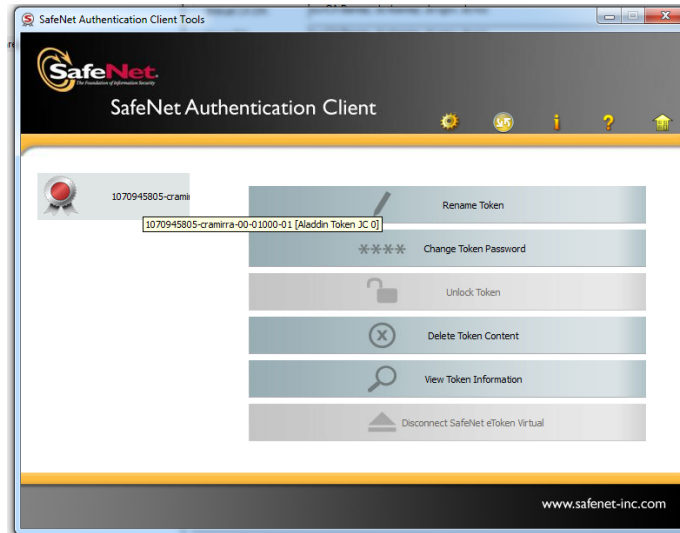



Una vez finalice, muestra la confirmación que el proceso ha terminado ***“The Recover Digital ID Wizard has completed”***

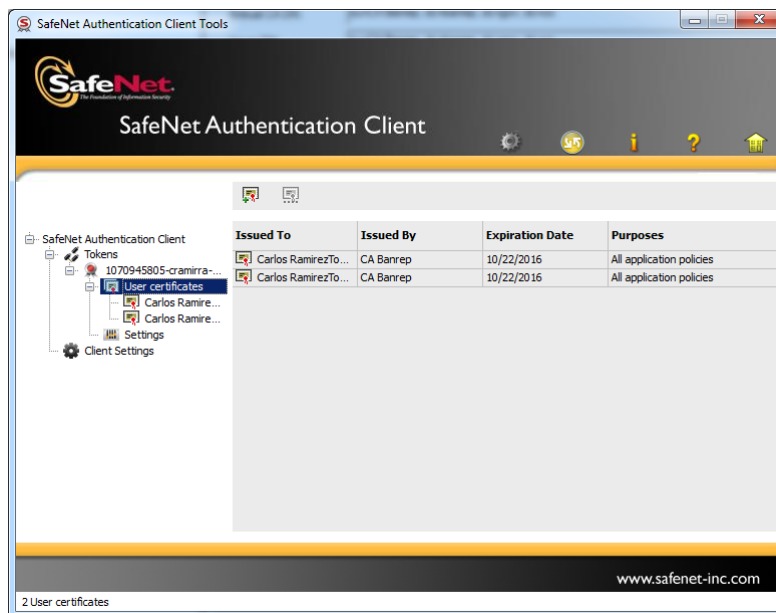


Nota: Si la creación del certificado no termino correctamente, debe verificar que se encuentra en línea a través de WSEBRA, si el problema continúa debe contactar a Soporte Informático del Banco de la República.

A continuación, deber verificar la creación del Profile abriendo el cliente “Safenet Authentication Client”, en la ventana principal (Parte Izquierda) puede ver la información del nombre del Token.




Seleccionar la opción , debe ver el par de certificados almacenados (para operaciones de firma y cifrado).

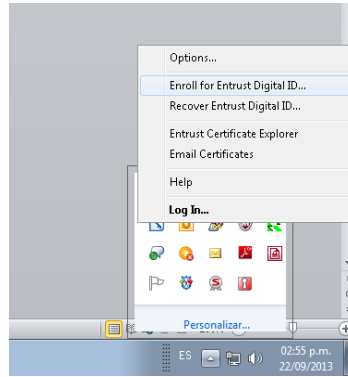


4. GENERACIÓN DE CREDENCIALES PARA PROCESOS AUTOMÁTICOS Y B2B (BUSINESS TO BUSINESS)

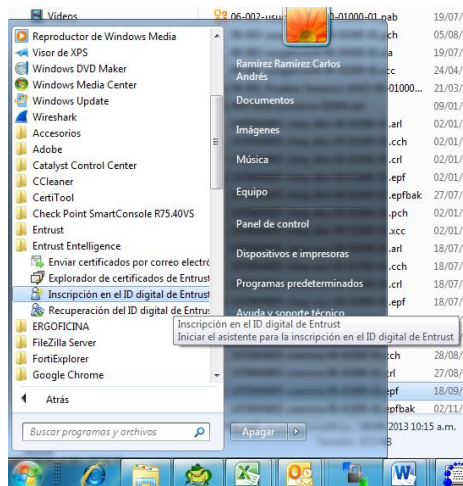
Para realizar este proceso se debe contar con la información de activación (el código de autorización y número de referencia suministrados por el Banco de la República) y con acceso a WSEBRA, y verificar la sección 2 (*Consideraciones Especiales*). El procedimiento de solicitud de recuperación del certificado se define en la Declaración de Prácticas de Certificación DPC para la CA – BANREP. (<http://www.banrep.gov.co/es/contenidos/page/declaracion-practicas-certificacion-ca-banrep>)

Existen dos opciones de iniciar el proceso de Enroll o creación del certificado, las cuales se describen a continuación:

Opción 1: En la parte inferior izquierda del escritorio de Windows hacer clic derecho sobre el icono de entrust  y seleccionar la opción Enroll for Entrust Digital ID.



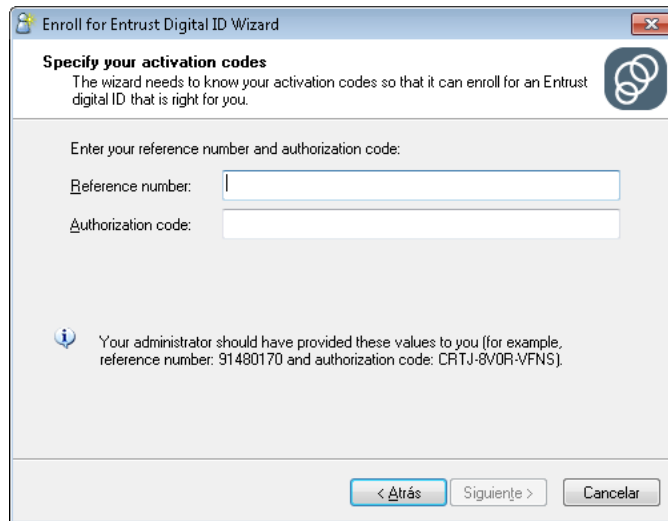
Opción 2: Ir a Inicio → Todos los programas → Entrust Entelligence → *“Inscripción en el ID Digital de Entrust”*.



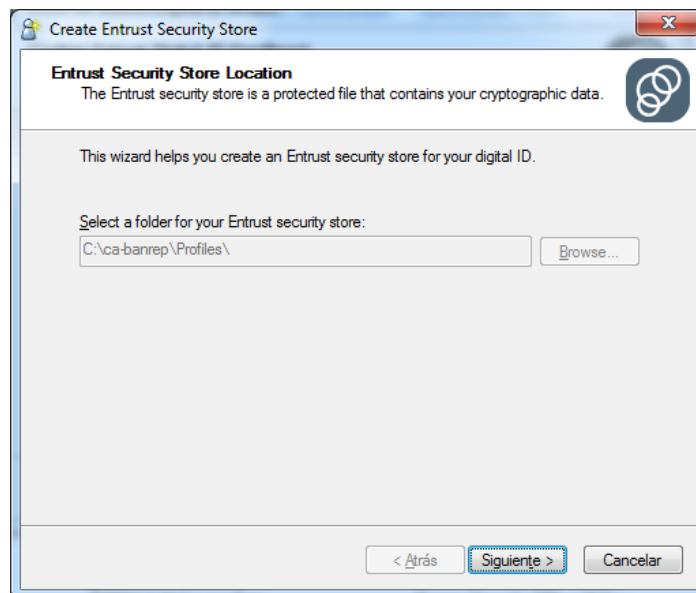
Una vez seleccionada esta opción, se abrirá la siguiente ventana. Seleccionar “siguiente”.



A continuación, debe ingresar el código de autorización y número de referencia provistos por el Banco de la República y dar clic en “Siguiente”



Después de ingresar el número de referencia y código de autorización, el proceso solicitará la ruta en donde se ubicará el profile (archivo con extensión .epf).



Se debe establecer la contraseña (password) de la credencial, que debe cumplir con las condiciones exigidas.

Create Entrust Security Store

Entrust Security Store Password
Password rules help ensure you select a secure password to protect your Entrust security store.

Please enter a password to protect your Entrust security store.

Password: [.....]

Confirm Password: [.....]

Your password must satisfy the following rules:

- ✓ must be at least 12 characters long
- ✓ must contain a non alphanumeric character
- ✓ must contain an uppercase character
- ✓ must contain a lowercase character
- ✓ must contain a numeric character
- ✓ must not contain a portion of security store name longer than half its length
- ✓ must not repeat a character more than half the length of password

< Atrás Finalizar Cancelar

Una vez la contraseña se ingrese exitosamente, se procede a establecer en nombre del profile, de la siguiente manera:

Certificados Business to Business (B2B):

SB-NIT Entidad-“Aplicación con la que va a interactuar”

Ejemplo: NIT Banco de la República es 860.005.216-7 y la aplicación con que va usar el certificado es Cuentas de Depósito CUD, el nombre del profile será: SB-8600052167-CUD

*Si el certificado es de pruebas se debe agregar la palabra -PRU al final del nombre.

Ejemplo: SB-8600052167-CUD-PRU

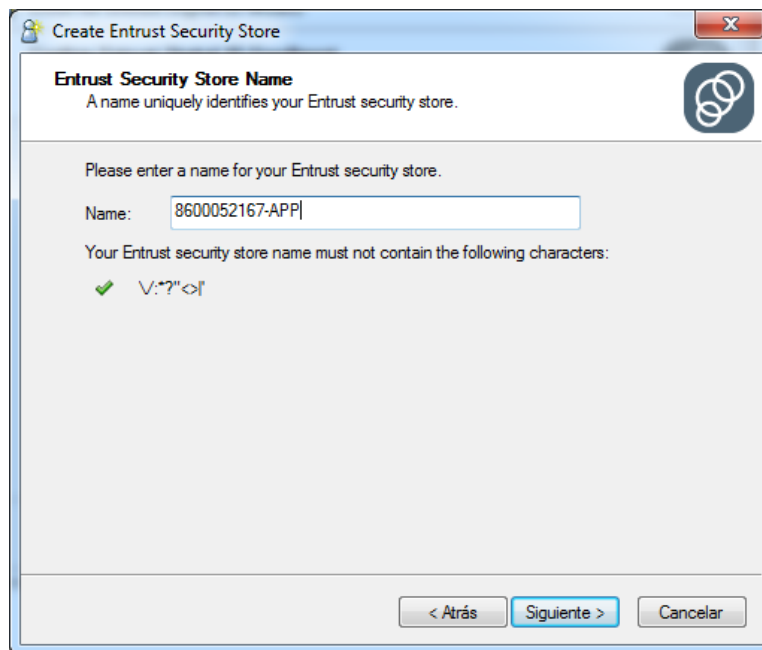
Certificados para Automatización de operaciones criptográficas

NIT Entidad-“Aplicación con la que va a interactuar”

Ejemplo: NIT Banco de la República es 860.005.216-7 y la aplicación con que va usar el certificado es Cuentas de Depósito CUD, el nombre del profile será: 8600052167-CUD

*Si el certificado es de pruebas se debe agregar la palabra -PRU al final del nombre.

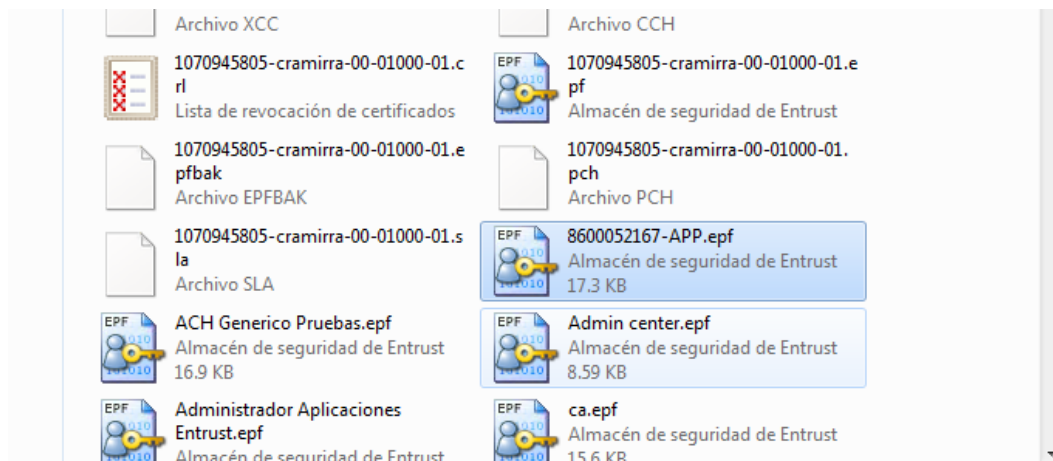
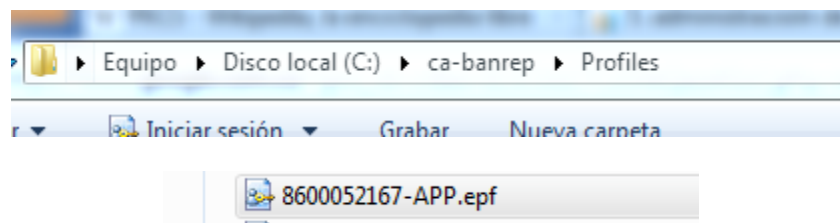
Ejemplo: 8600052167-CUD-PRU




En la opción siguiente muestra que el proceso de creación fue exitoso.

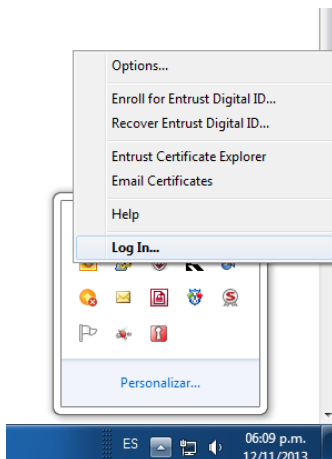


Por defecto ubicación del profile es la ruta `c:\ca-banrep\profiles\` o en la ruta establecida por el usuario en el proceso mencionado anteriormente, el archivo tendrá el nombre que el usuario haya establecido en el proceso de creación y extensión .epf.



Una vez identificada la ubicación del profile (.epf), se debe proceder a hacer el login con el profile previamente creado.

En la parte inferior izquierda del escritorio de Windows hacer clic derecho sobre el icono de entrust  y seleccionar la opción **Log In....**



En el botón “Browse” seleccionamos el profile correspondiente.



Ingrese la contraseña para hacer el Login.

5. TRANSFORMACIÓN DE CREDENCIALES

Es importante recordar que las responsabilidades y deberes descritos en la DPC cambian. El Banco de la República recomienda 1) revisar el escenario de uso y 2) que se realice la lectura detallada de dichas condiciones antes de solicitar credenciales con la capacidad de exportarse a otros formatos. (<http://www.banrep.gov.co/es/contenidos/page/declaracion-practicas-certificacion-ca-banrep>)

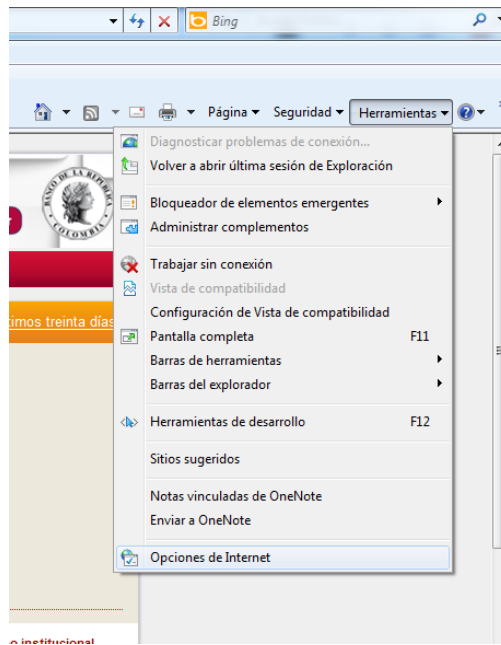
Después de realizar la creación del profile se procede a realizar la transformación de credenciales, a continuación se describe el procedimiento para convertir el profile en formato Entrust Archive (archivo con extensión .epf) en formato PKCS#12 (archivo con extensión .p12 o .pfx) o en formato Java key Store (archivo con extensión jks).

Antes de realizar los siguientes pasos, se debe garantizar que se realizó el Login de la credencial EPF en el cliente ESP .

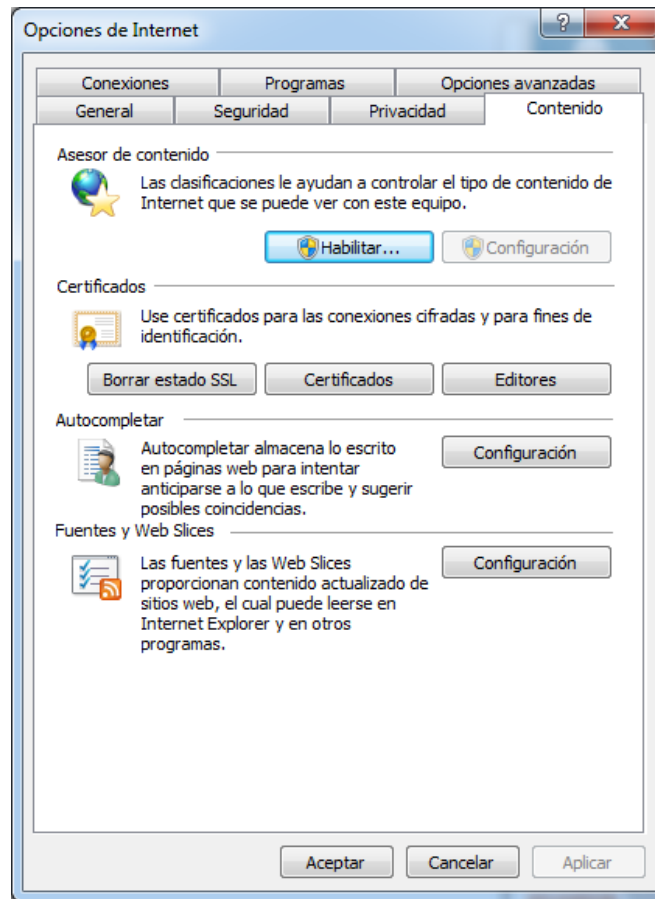
Ingresa al navegador “Internet Explorer”.

The screenshot displays the 'infoBANCO' intranet interface. At the top, there's a navigation bar with a search box and a 'Contáctenos' link. Below this is a menu with categories: 'Inicio', 'Ciudades y Dependencias', 'Directorio', 'Solicitud de Servicios', 'Usted en su labor', and 'Usted y su familia'. The main content area is divided into several sections: 'El Banco para el mundo' with news items, 'Atención al ciudadano' with a petition link, 'Lo más consultado' with a 'Noticias para usted en su labor' link, and 'Enlaces de interés'. The central 'Inicio' section features a large banner for 'Noticias para usted en su labor' with the headline 'Ya se encuentra disponible la Encuesta de valoración de liderazgo'. Below this are three 'Destacado' (Featured) news items: one about ecological Christmas, one about institutional mail, and one about vacation management. The footer shows 'Intranet local | Modo protegido: desactivado' and a 95% zoom level.

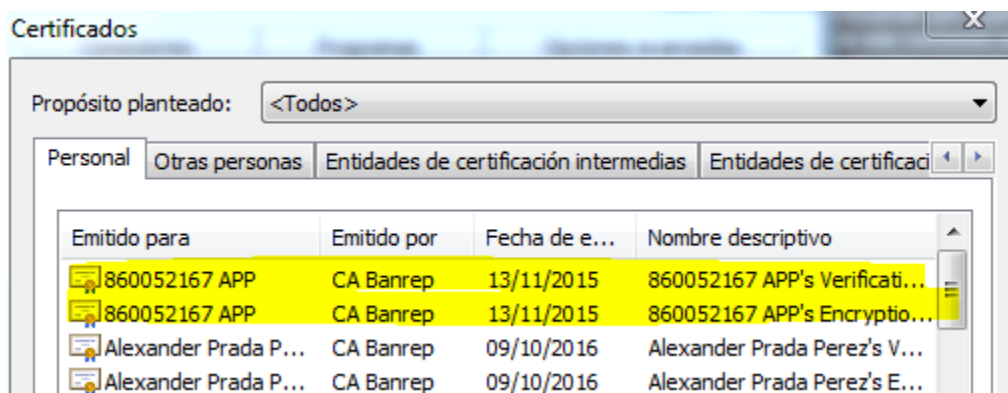
Ir a la sección Herramientas.



En Herramientas, ir a la sección Contenido → Certificados.



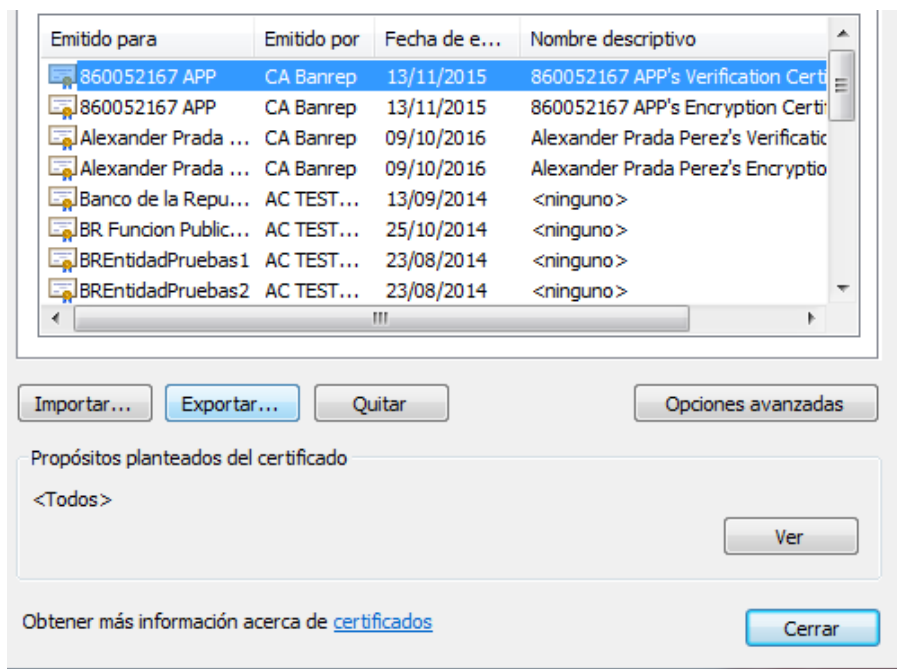
Una vez ubicado en la sección Certificados, se visualizarán los certificados correspondientes al profile que se creó.



Serán visibles dos certificados, uno utilizado para encriptar y otro para verificación de firma, por cada llave se debe realizar el proceso de exportar las llaves.

Exportar Llave Privada de Verificación de Firma:

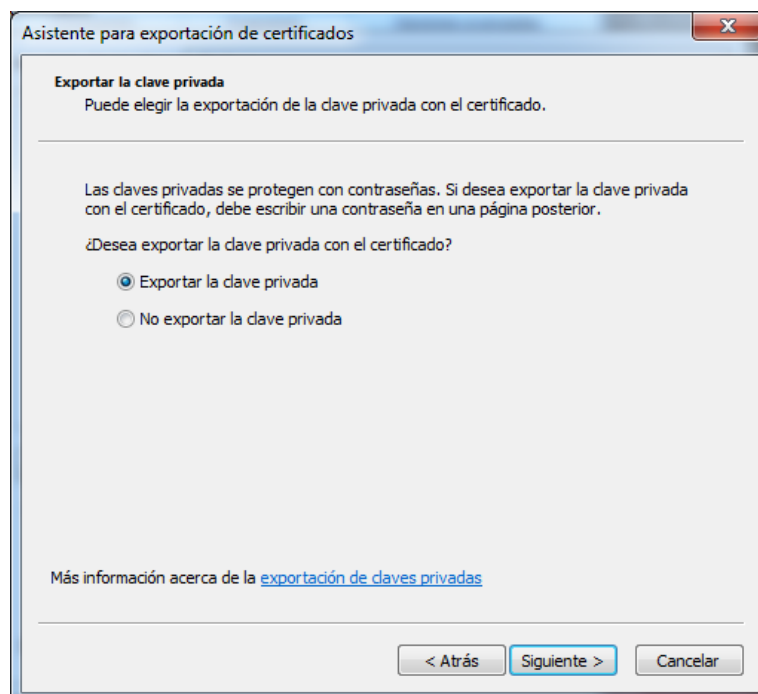
Seleccionar el certificado cuyo nombre descriptivo sea “Verification Certificate” y hacer clic en Exportar.



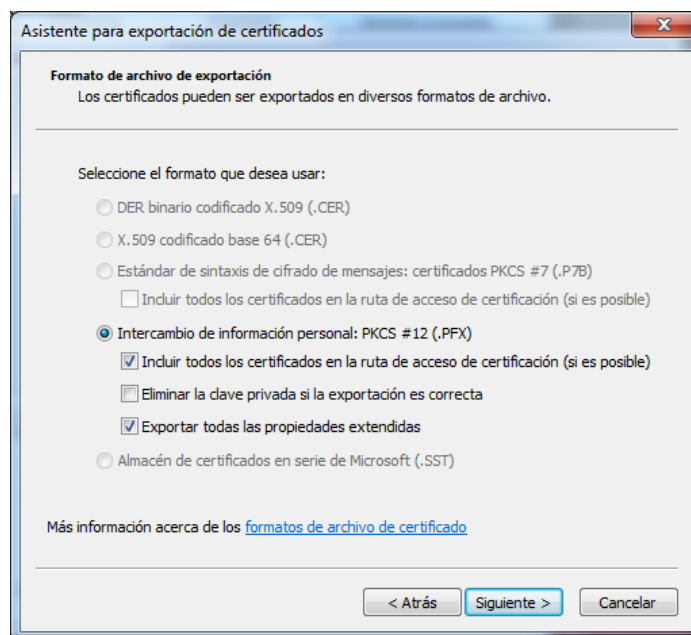
Se debe hacer click en siguiente.



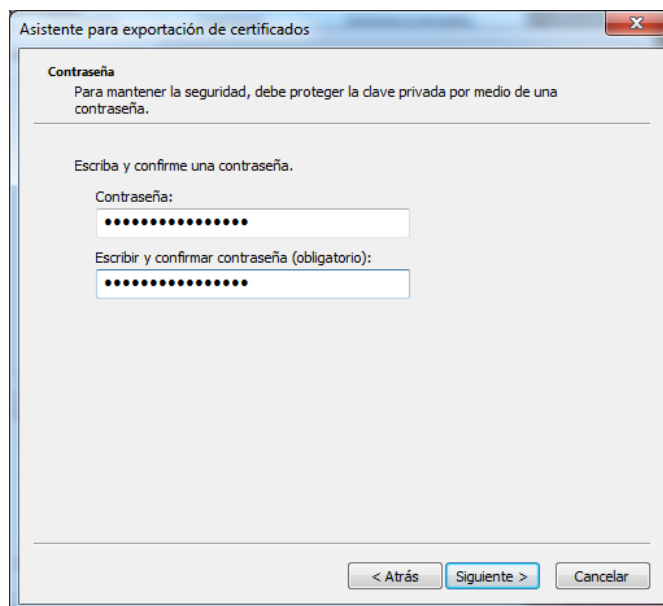
En la siguiente sección es indispensable seleccionar la opción “Exportar la llave privada”



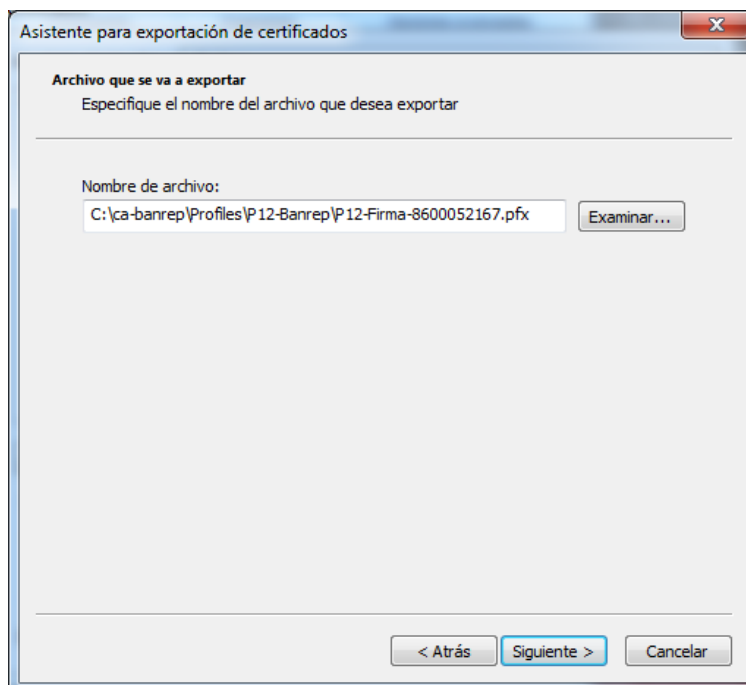
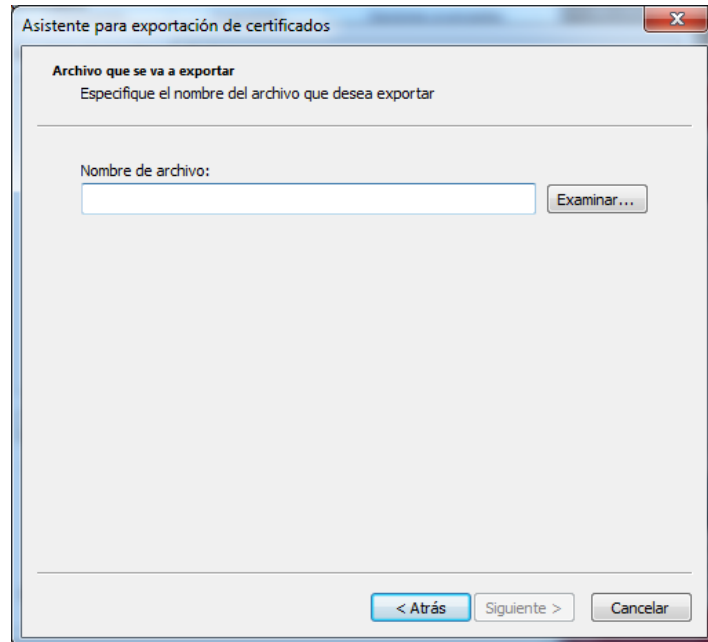
Se debe seleccionar las opciones mostradas a continuación:



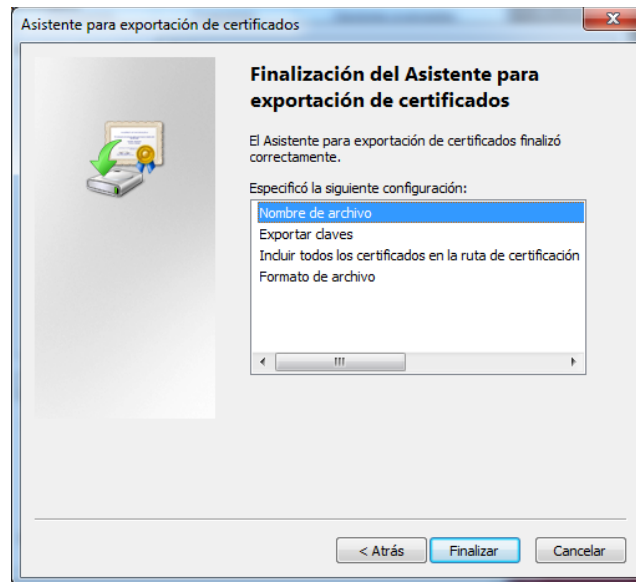
Se procede a establecer la contraseña del nuevo archivo PKCS#12 para realizar operaciones de firma. Es importante que esta contraseña cumpla con características mínimas de composición tales como número de caracteres, mayúsculas, minúsculas, números y caracteres especiales.



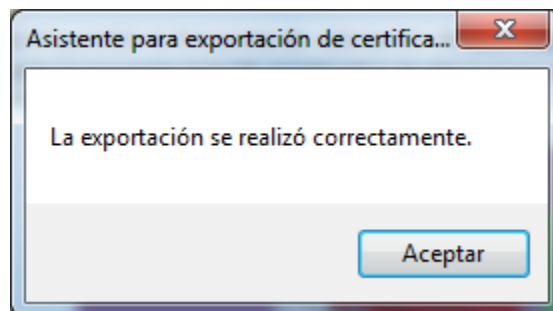
Proceder a establecer un nombre al archivo.



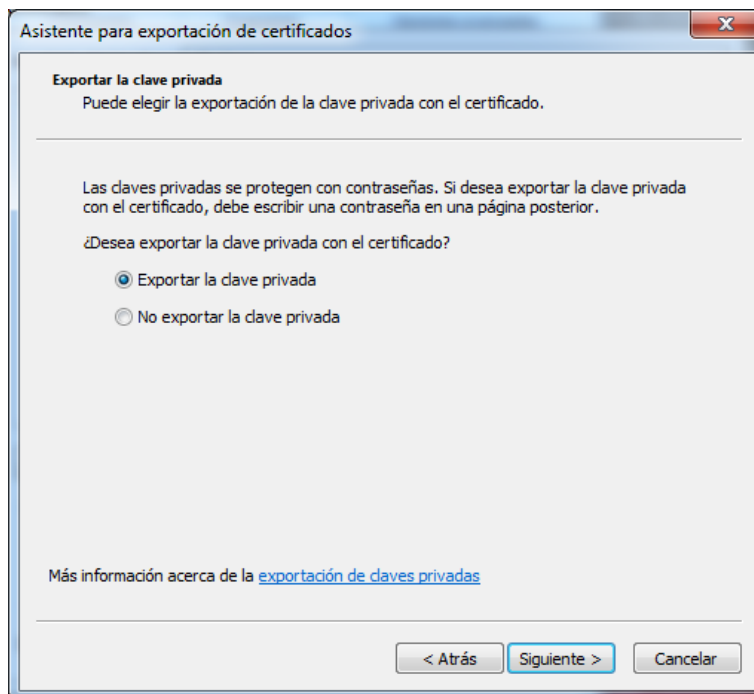
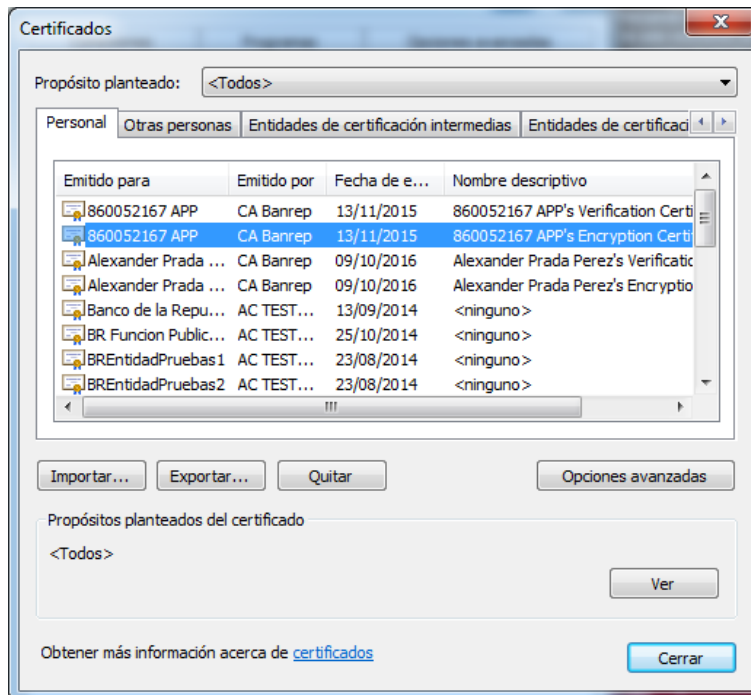
Pulsamos Finalizar para terminar el proceso de exportación.

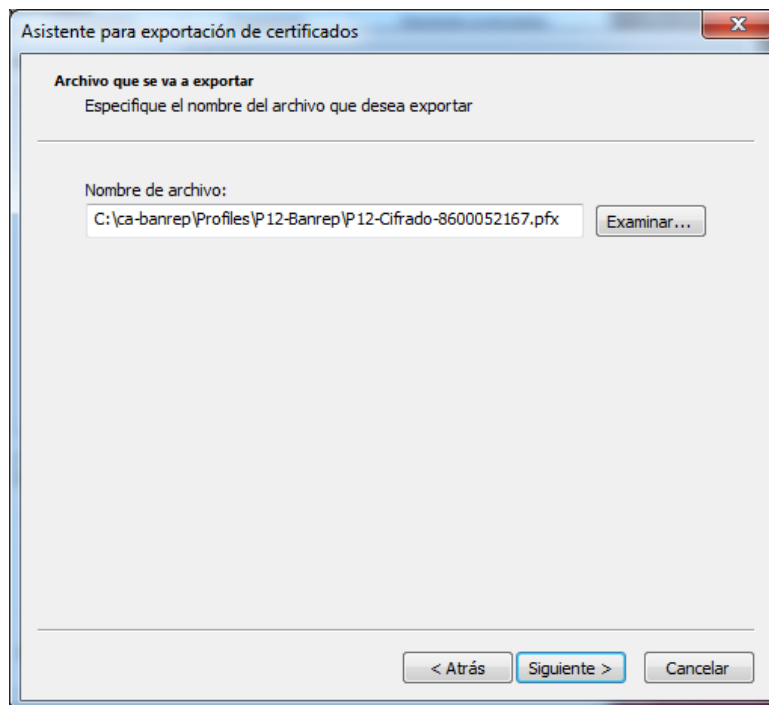
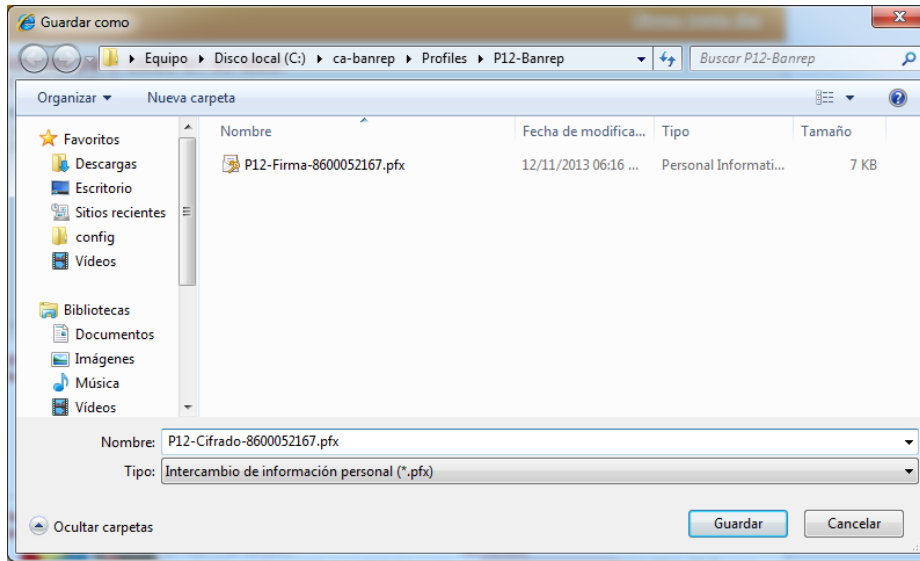


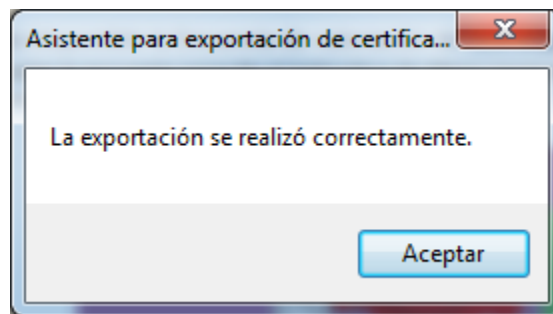
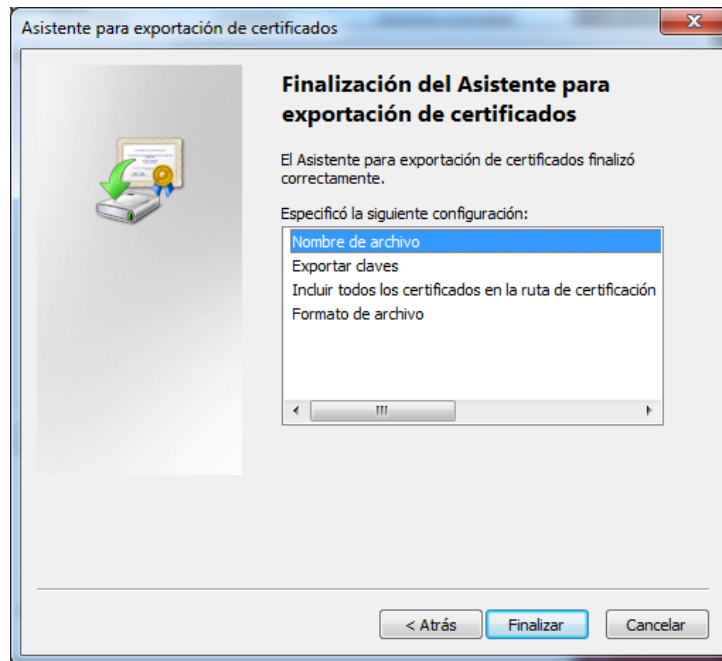
Verificamos que la exportación se realizó correctamente.



A continuación se debe realizar el mismo proceso para el certificado con Nombre descriptivo "Encryption Certificate"







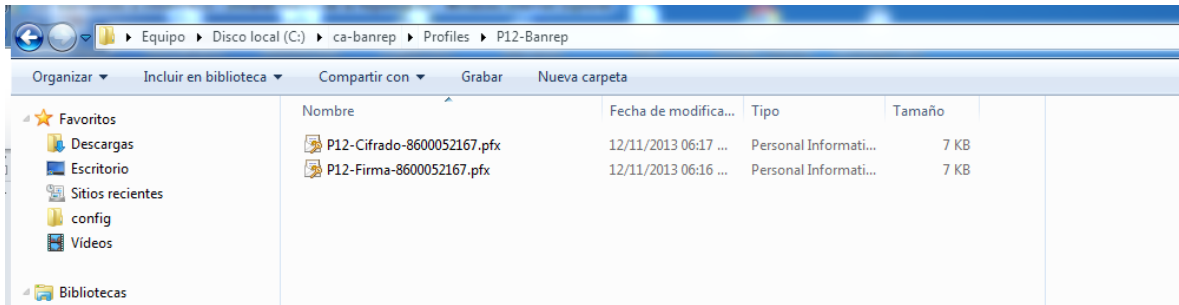
En la ruta seleccionada en el punto anterior, debemos tener dos archivos .pfx, correspondientes al resultado del proceso de exportación.

Para realizar un proceso de firma digital se debe usar la credencial .pfx correspondiente al proceso de exportación de la llave privada de firma.

Para realizar un proceso de cifrado se debe usar la credencial .pfx correspondiente al proceso de exportación de la llave privada de descifrado.

Después de tener los archivos en formato PKCS#12, podemos proceder con el cambio de formato a JKS, para realizar este proceso podemos utilizar las utilidades propias de java (herramienta *keytool*) o software utilitario como Portecle (distribución libre).

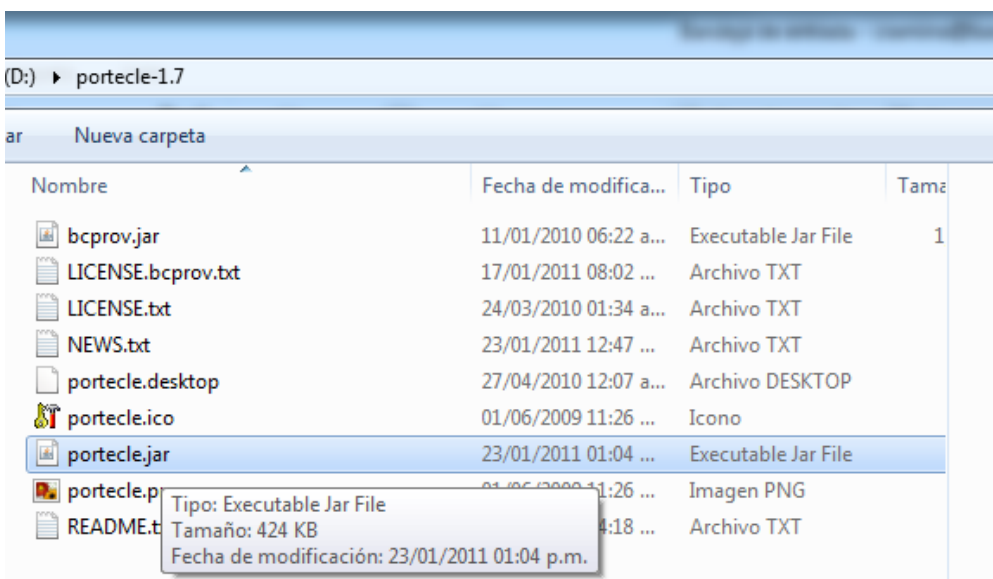
Para tener una mejor experiencia de usuario, se explica la forma como se realiza con portecle. Si requiere realizar la conversión de formato directamente con la funcionalidad propia de java puede ir a la documentación ofrecida por Oracle (<http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html>, https://blogs.oracle.com/shyamrao/entry/how_to_import_pfx_file, etc.)

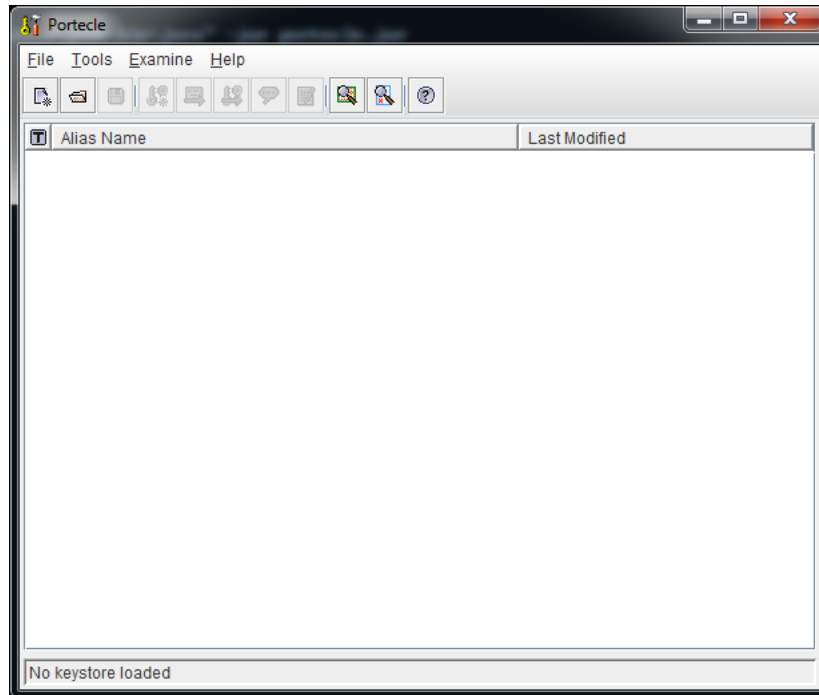


Procedemos a usar el Software “Portecle”:

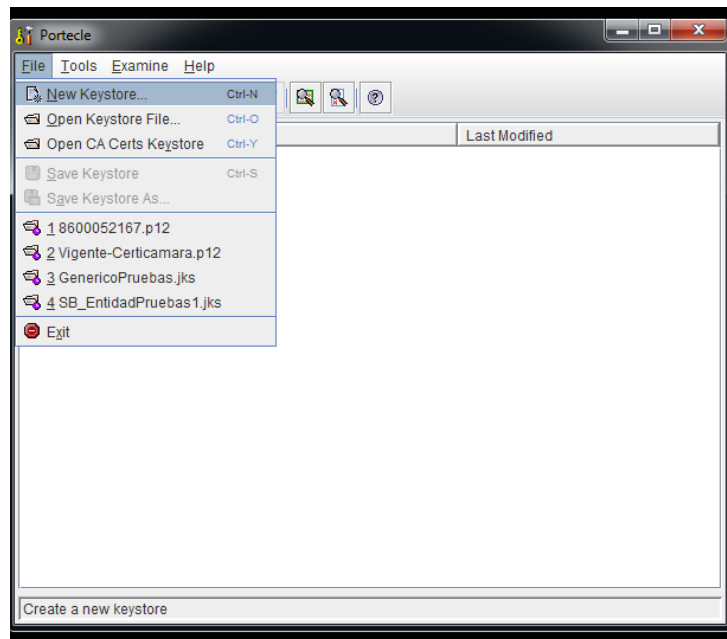
Portecle, es un software libre, el cual puede ser descargado de Internet.

Para abrir el software hacemos doble click en “portecle.jar”, según se muestra a continuación:

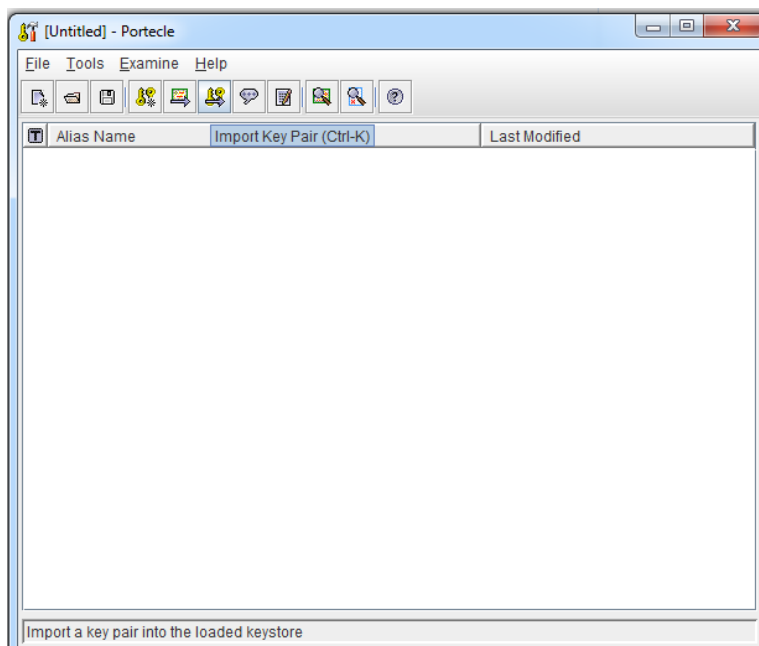
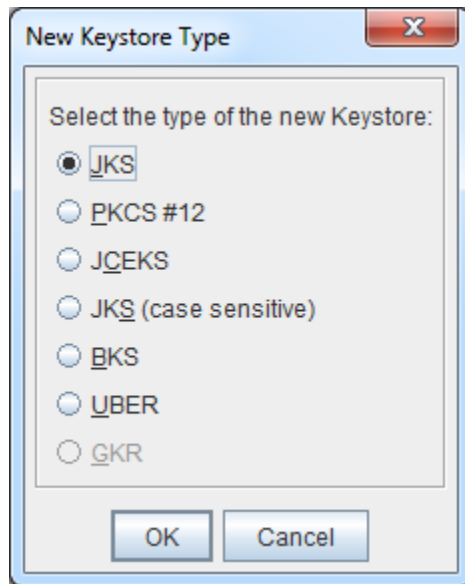




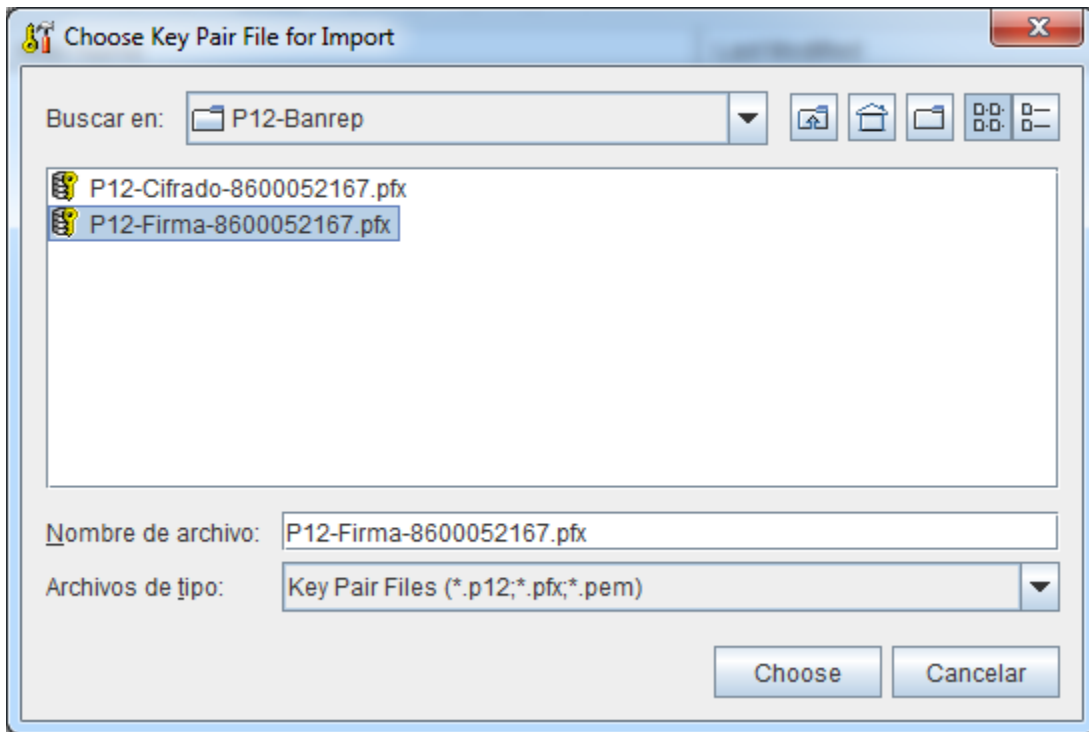
Se selecciona “New Keystore”



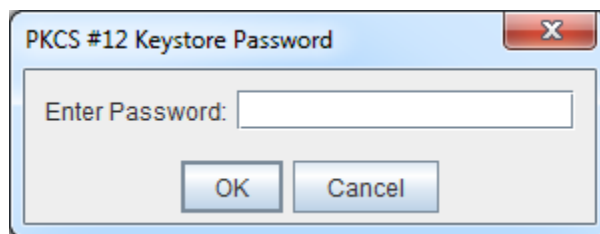
De las alternativas presentadas debe escoger tipo JKS.

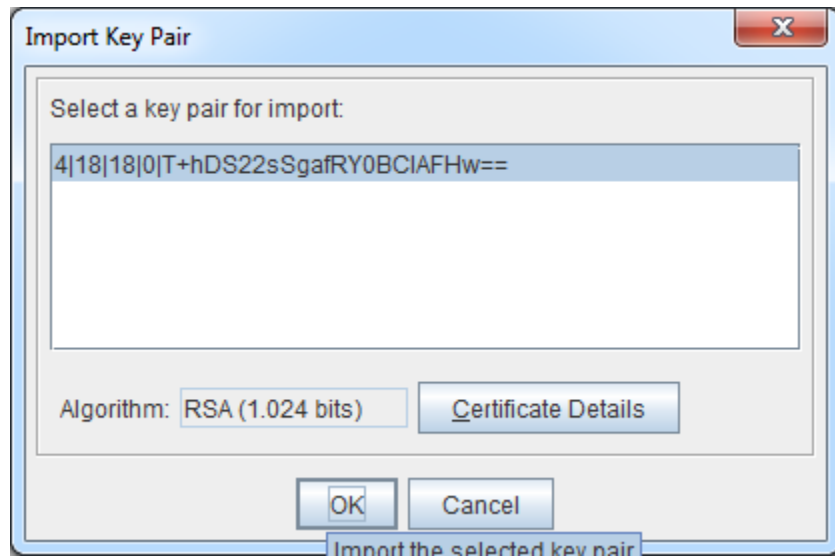


Seleccionar la opción “***Import Key Pair***”, en donde debe ubicar el archivo en formato PKCS12 correspondiente al key usage de Firma Digital

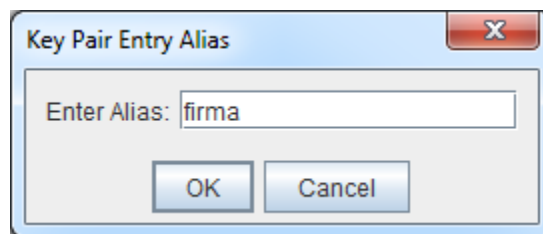
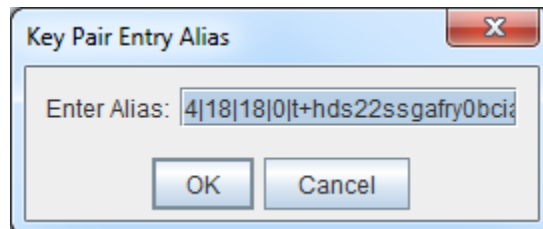


Se debe ingresar la contraseña usada en la conversión a formato PKCS12. Y haga clic en el botón “OK”

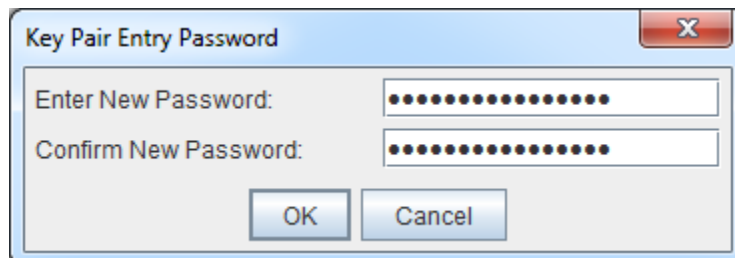


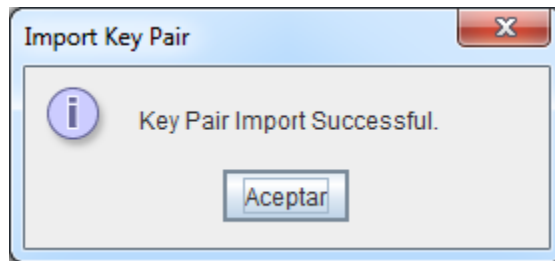


Cuando hacemos “OK” en la Sección Import Key Pair, podemos modificar el Alias de la llave (Corresponde a Key Usage de Firma Digital), es de gran ayuda establecer un nombre fácil de recordar, en este manual modificamos el alias de la llave a la palabra “*firma*”, como se muestra a continuación.

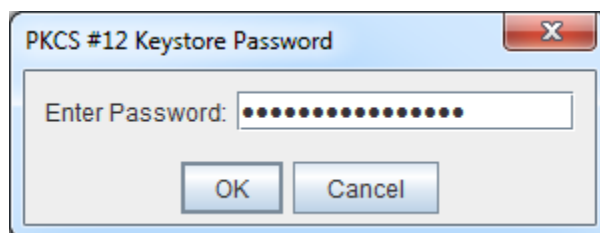
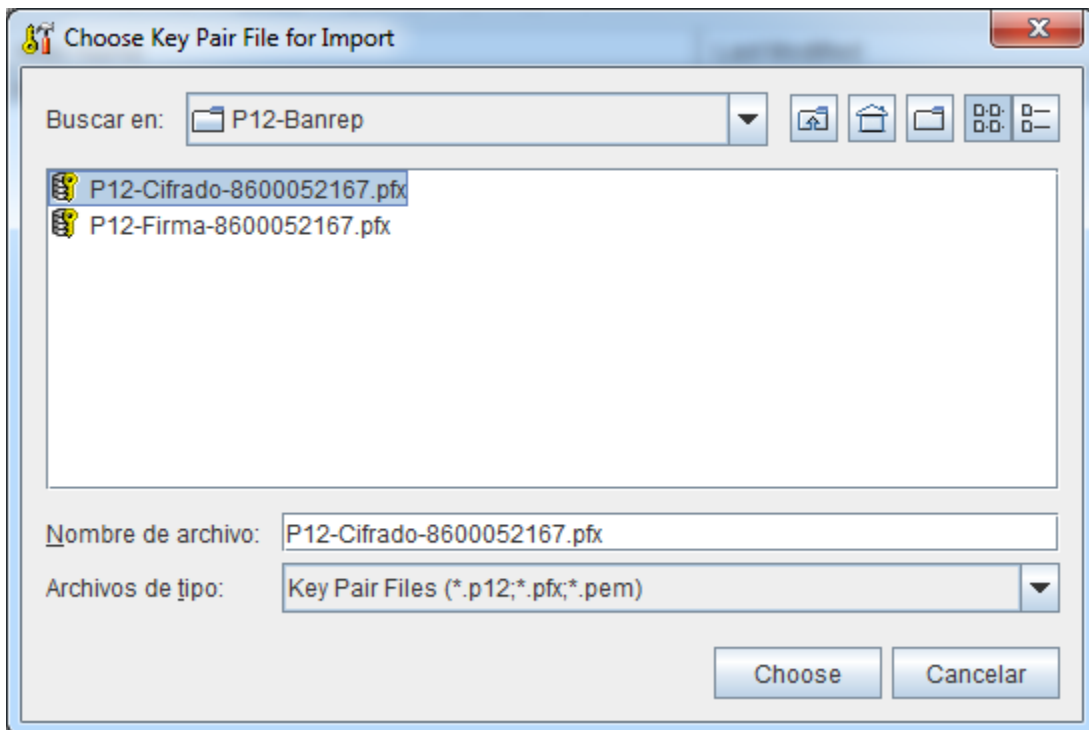


El sistema solicitará una contraseña para este alias.

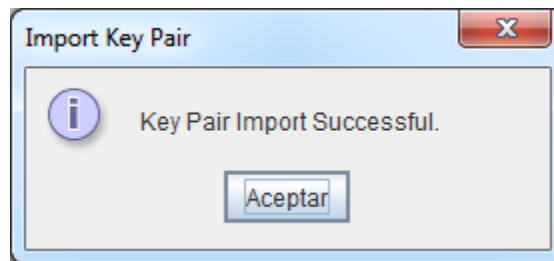
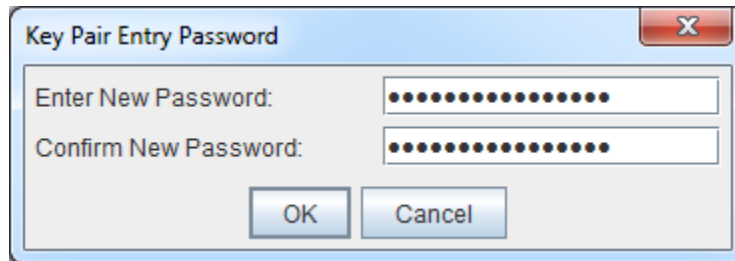
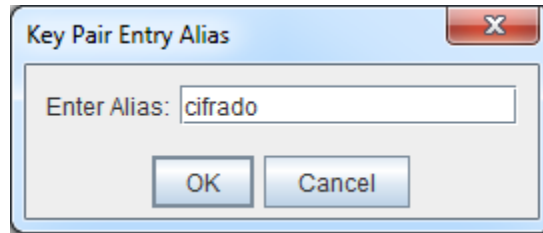




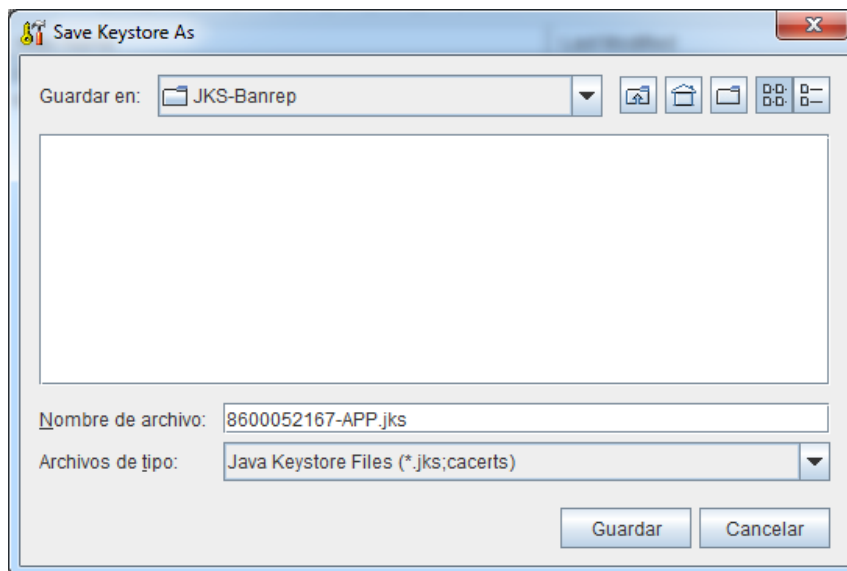
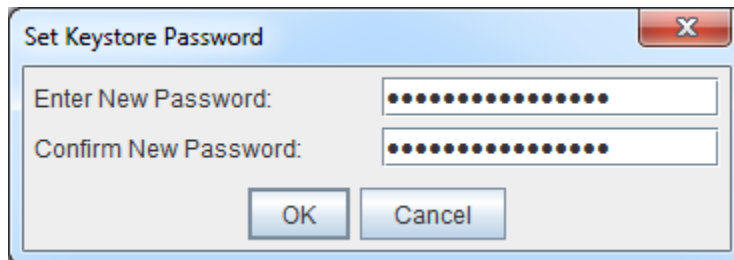
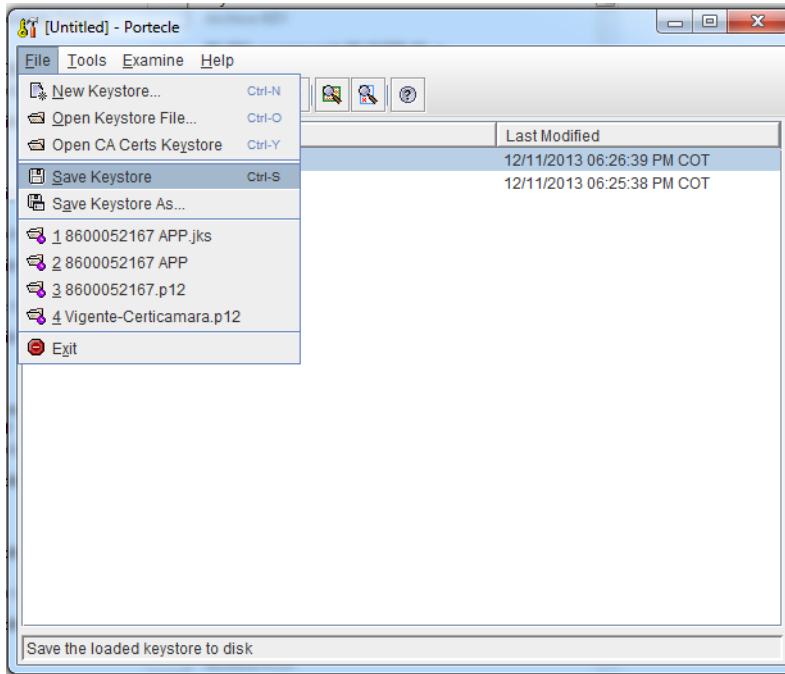
Realizamos la proceso de Import sobre la credencial PKCS12 correspondiente al key usage de cifrado o Key Encirphement.



De igual manera se puede establecer un nombre al alias de esta llave, para este caso la llamaremos "cifrado".

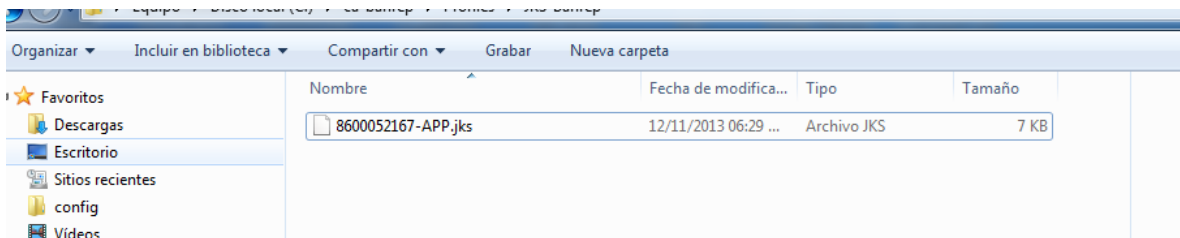


Se procede a salvar el Keystore, se solicita una contraseña para controlar el acceso a su contenido.



En la ruta establecida en el punto anterior ubicaremos el archivo JKS para ser usado en la aplicación,

En este caso en la ruta *C:\ca-banrep\Profiles\JKS-Banrep*, tenemos:



Nota: Debe verificar que se encuentre en línea a través de WSEBRA, si tiene algún problema puede contactar a Soporte Informático del Banco de la República.