Banco de la República
Bogotá D. C., Colombia

Dirección General de Tecnología
Departamento de Seguridad Informática

MANUAL PARA LA GESTIÓN DE INSTRUMENTOS DE FIRMA ELECTRÓNICA

DSI-GI-128

16 de febrero de 2024
Versión 2.0

CONTENIDO

Pág.

1 INTRODUCCIÓN

El propósito de este documento es dar a conocer los requisitos y procedimientos relacionados con la gestión de los instrumentos de firma electrónica que almacenan llaves criptográficas asociadas a las identidades electrónicas generadas por el Banco de la República (Banco).

1.1 AUDIENCIA

Este documento está dirigido a todas las entidades financieras que en su operación con el Banco hacen uso de las identidades electrónicas generados por éste para asegurar criptográficamente el intercambio de información.

1.2 ALCANCE

En este documento se describen los requerimientos necesarios para realizar procesos de creación y recuperación de claves criptográficas asociadas a las identidades electrónicas generadas por el Banco (Pertenecía a Empresa y Persona Jurídica Entidad Empresa) para cada uno de los Instrumentos de Firma Electrónica disponibles.

2 REQUISITOS

A continuación se presentan los requerimientos y consideraciones necesarias que se deben tener en cuenta para la generación, recuperación y transformación de las claves criptográficas generadas por la infraestructura PKI del Banco.

2.1 REALIZAR SOLICITUD DE CREACIÓN O RECUPERACIÓN

Los procedimientos para solicitud de creación y/o recuperación se encuentran especificados en la Circular Operativa y de Servicios DG-T-294 (https://www.banrep.gov.co/sites/default/files/reglamentacion/archivos/dgt-294.pdf). Como resultado de este procedimiento (creación o recuperación), el usuario dispondrá de los códigos de activación o recuperación (según sea el caso) para obtener las nuevas llaves criptográficas.

2.2 CONEXIÓN PORTAL WSEBRA

Para ejecutar el procedimiento de creación o recuperación, la Entidad debe tener conectividad con los servicios provistos por la plataforma PKI del Banco. Estos servicios podrán ser alcanzados a través del canal dedicado que tiene la Entidad con

el Banco, habilitando una sesión en el portal WSEBRA o mediante conexión vía Internet con este portal (https://wsebra.banrep.gov.co/internet), habilitando una sesión válida.

2.3 SOFTWARE

El equipo en donde se desee hacer la creación o recuperación de las llaves criptográficas debe tener instalados los componentes de software descritos a continuación.

- Entrust Security Provider (ESP - última Versión disponible en: DescargasSUCED/PKI/ESP en https://caribe.banrep.gov.co/emisor).
- Safenet Authentication Client (SAC – Software que se obtiene con la adquisición del token criptográfico).
- Portecle (Distribución libre).

2.4 TOKEN CRIPTOGRÁFICO

La generación de llaves criptográficas para identidades electrónicas de tipo Pertenencia a Empresa podrán realizarse sobre un Instrumento de Firma Electrónica correspondiente a un dispositivo físico denominado Token Criptográfico.

Los Tokens Certificados y homologados por las llaves criptográficas que generan el Banco son:

- Safenet ***eToken Pro 72k***
- Safenet ***eToken 5100***
- Safenet ***eToken 5110***

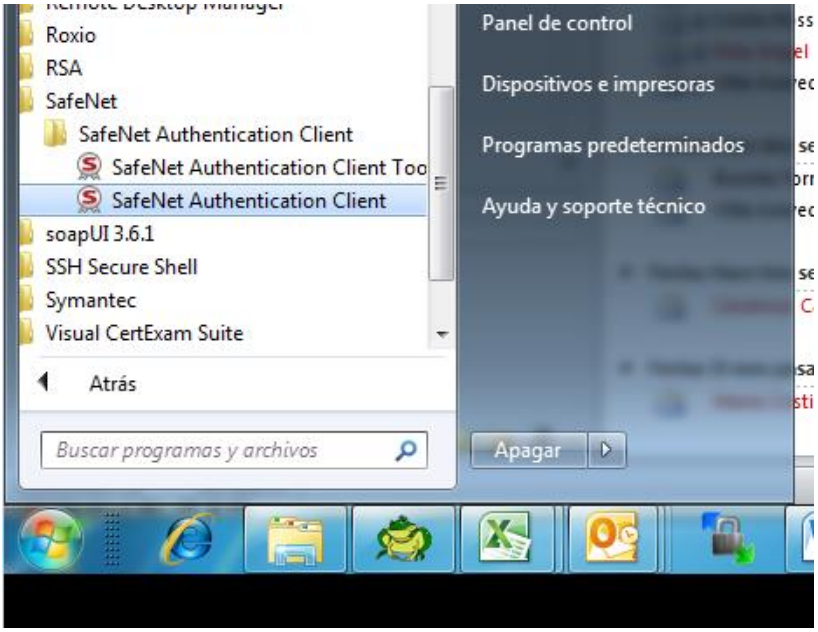
3 GENERACIÓN DE LLAVES CRIPTOGRÁFICAS PARA IDENTIDAD ELECTRÓNICA TIPO PERTENENCIA A EMPRESA

La generación de llaves criptográficas para el suscriptor contempla dos escenarios: creación (Enroll) y Recuperación (Recover) de la Identidad Electrónica (denominada técnicamente en este documento como "*Profile*"). En ambos casos se debe realizar el proceso de inicialización del Instrumento de Firma (Token Criptográfico). Este procedimiento se describe a continuación.

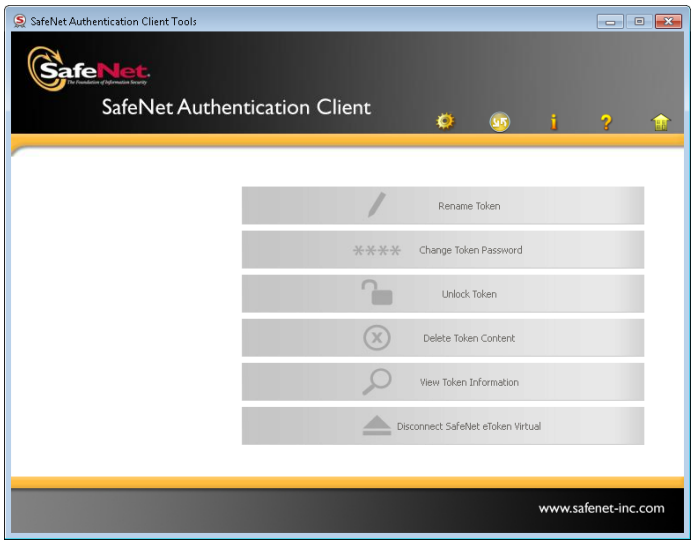
3.1 PROCEDIMIENTO PARA INICIALIZAR EL TOKEN CRIPTOGRÁFICO

Para empezar con el proceso de creación o recuperación de las llaves criptográficas para un suscriptor se debe realizar la operación ***Inicializar Token***:

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:

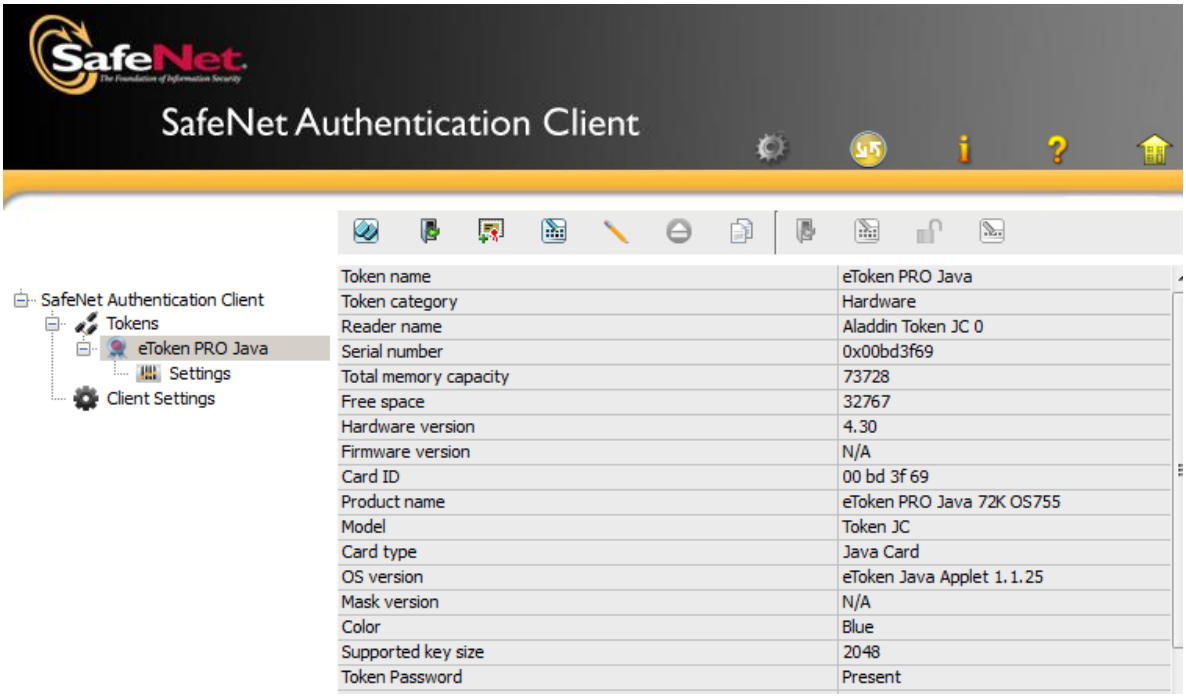


2. Cuando ingresa a esta aplicación se observa la siguiente pantalla:



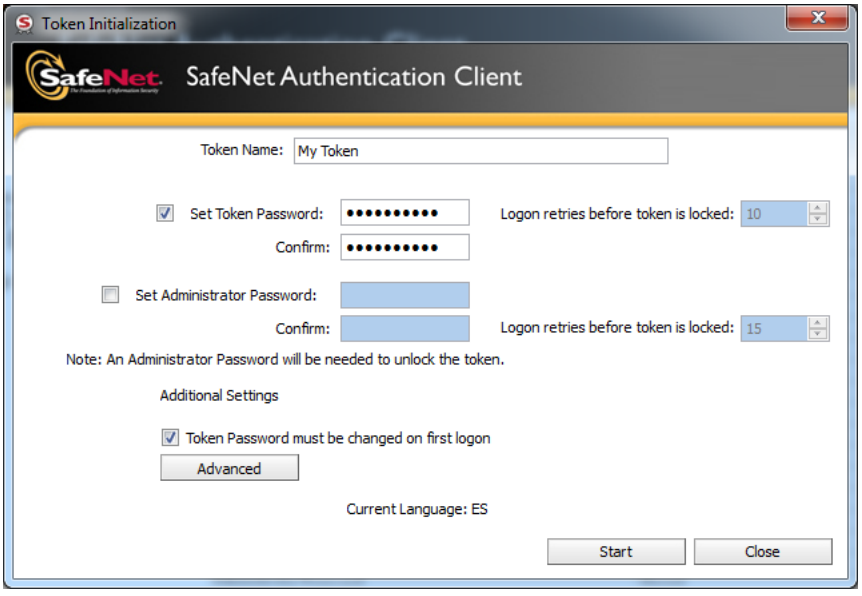
Se debe hacer clic en el icono de "***configuración***" 

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



Haga clic en el icono "***Inicializar Token***" 

4. En la siguiente ventana de inicialización del token:



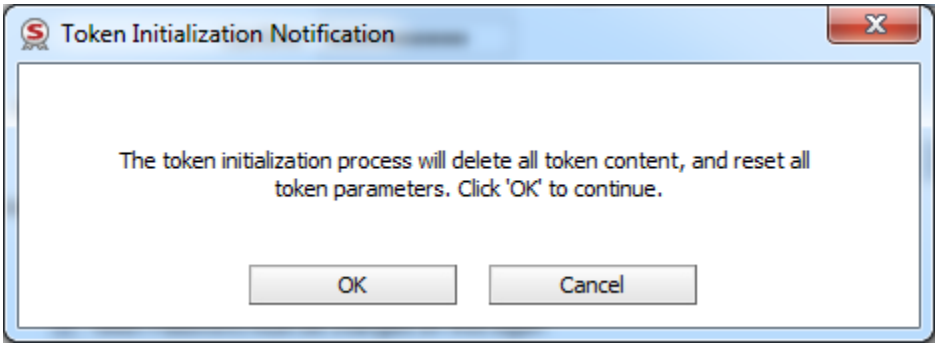
En este paso debemos indicar el Nombre del Token, el cual debe seguir la siguiente estructura: "**Cedula de ciudadanía –Login– tipo de sector -codigoEntidad – código de ciudad**".

Ejemplo: 1070945805-cramirra-00-01000-01

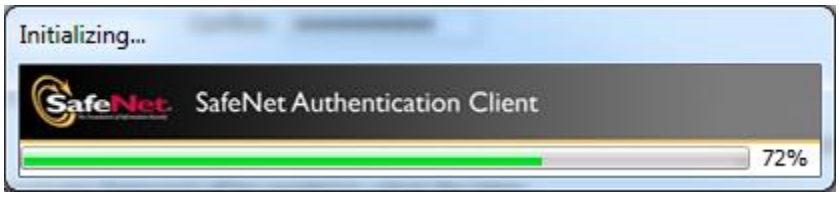
Se debe establecer la contraseña en la Opción "***Establecer Contraseña***" o "***Set Token Password***" y confirmarlo.

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

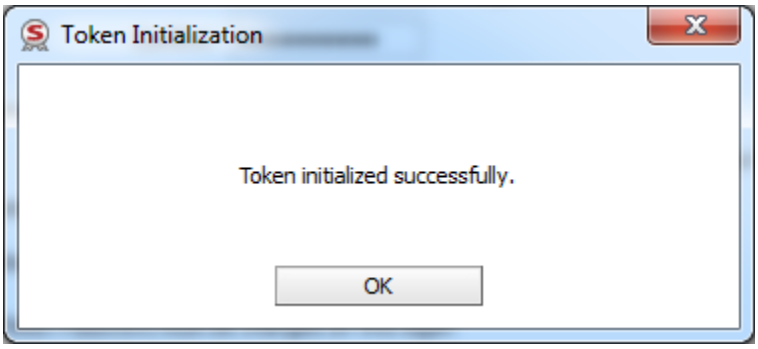
En la siguiente ventana, se solicita confirmación de la operación de inicialización. Se debe dar clic en el botón "**OK**" para proceder.



Se inicia el procedimiento de inicialización del Token (se eliminan todas las llaves criptográficas almacenadas en el Token).



Al terminar debe presentar un mensaje de inicialización exitosa.

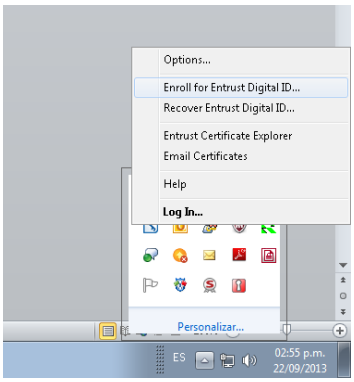


3.2 CREACIÓN DE LLAVES CRIPTOGRÁFICAS PARA IDENTIDAD ELECTRÓNICA TIPO PERTENENCIA EMPRESA

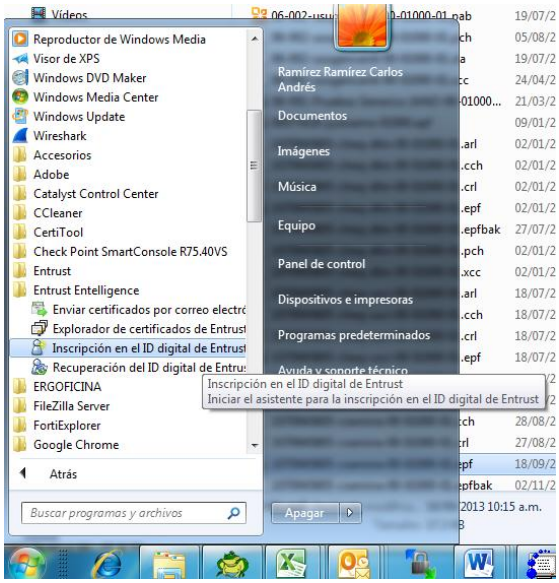
Para realizar este proceso se debe contar con la información de activación (el código de autorización y número de referencia suministrados por el Banco de la República) y con acceso a WSEBRA, y verificar la sección 2 (***Requisitos***). El Token Criptográfico deberá estar conectado al equipo en donde se realiza la operación y debe haberse ejecutado en forma previa su inicialización de acuerdo a lo descrito en la anterior sección.

Existen dos opciones para iniciar el proceso de Creación del Profile (Enroll), 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***, tal como se ilustra en la siguiente imagen.

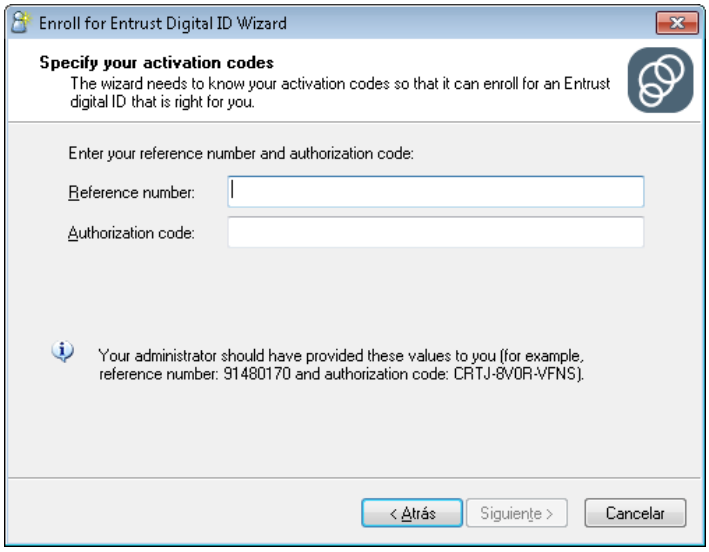


Opción 2: Nos dirigimos Inicio → Todos los programas → Entrust Entelligence → "***Inscripción en el ID Digital de Entrust***".



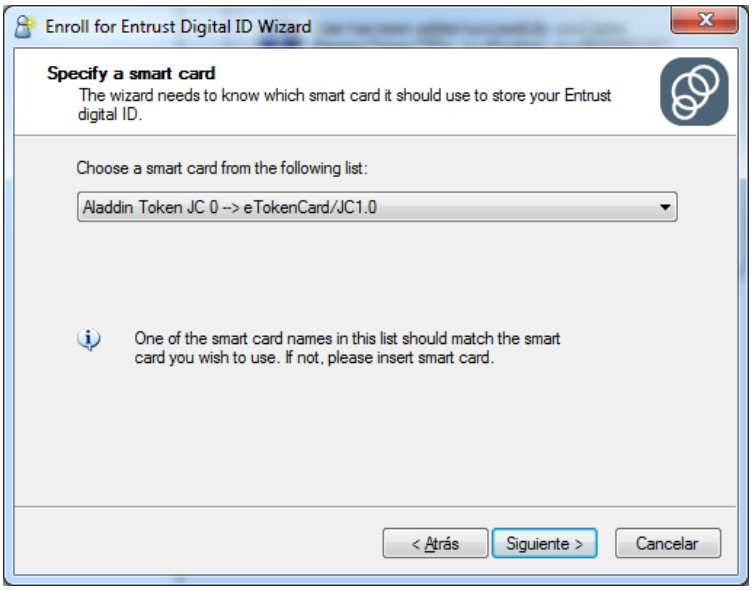
Una vez seleccionada esta opción, se abrirá la siguiente ventana. Haga clic en "siguiente".

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”

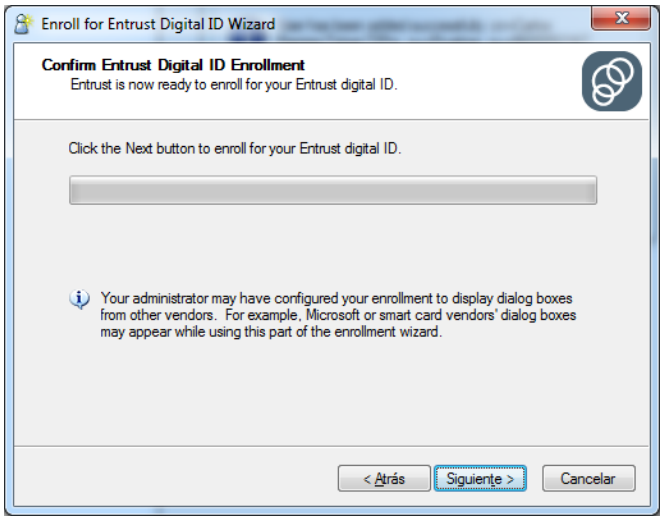


El sistema detectará que el Token está conectado en el PC.

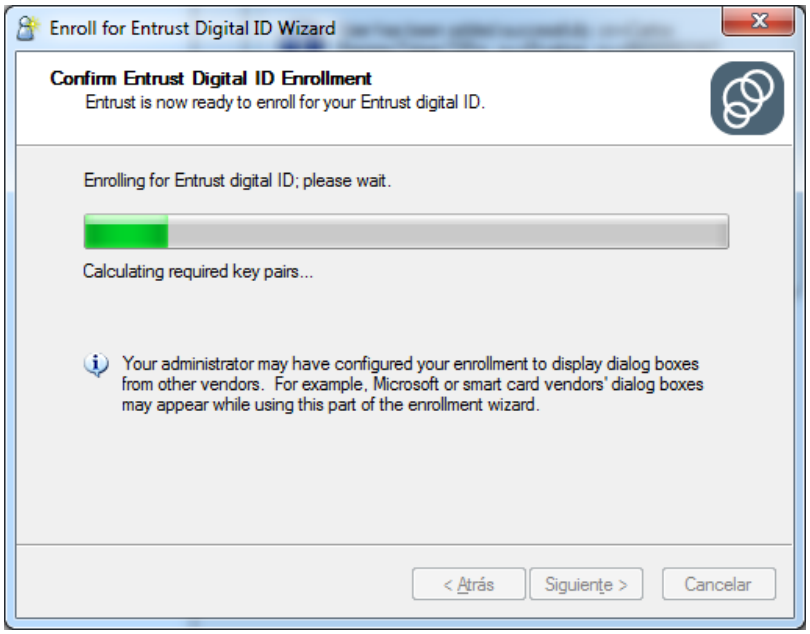
Hacer clic en “Siguiente”.



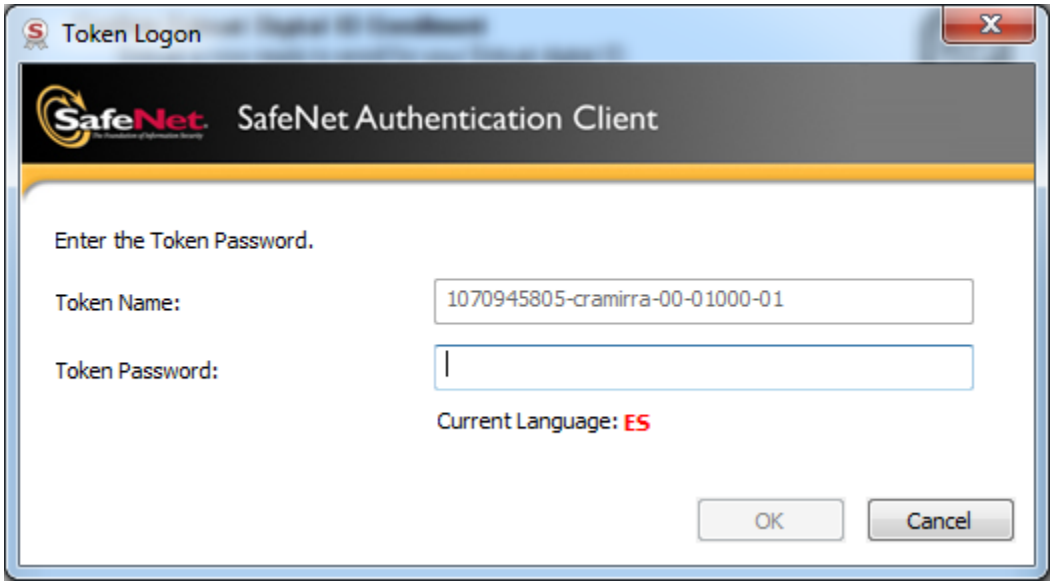
En el proceso de creación, el software se comunica con la infraestructura tecnológica del Banco por lo que debe tener abierta la sesión de WSEBRA, dar clic en “Siguiente”



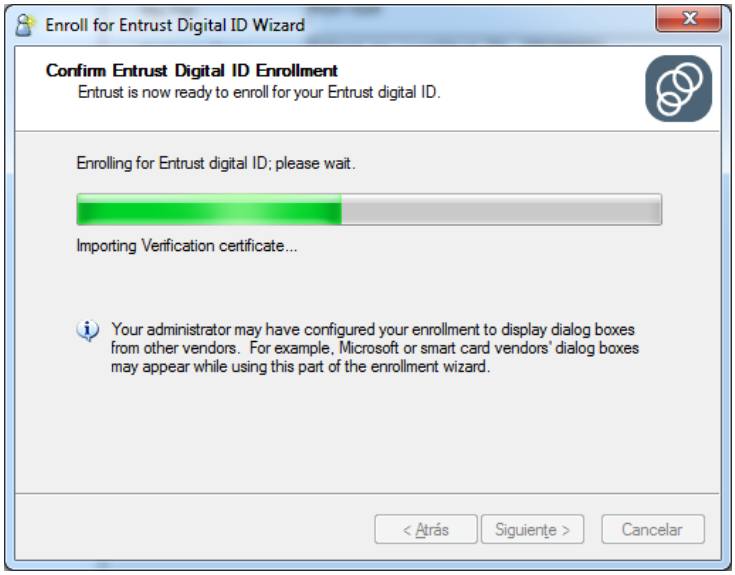
Se iniciará el proceso de Enroll (creación de las llaves criptográficas).



Para poder almacenar las llaves criptográficas asociadas a la Identidad Electrónica del suscriptor en el Token, el software SafeNet Authentication Client solicitará la clave del Dispositivo (Ver sección ***3.1 Inicializar Token***), por favor ingresar la clave del Token y dar clic en "OK".



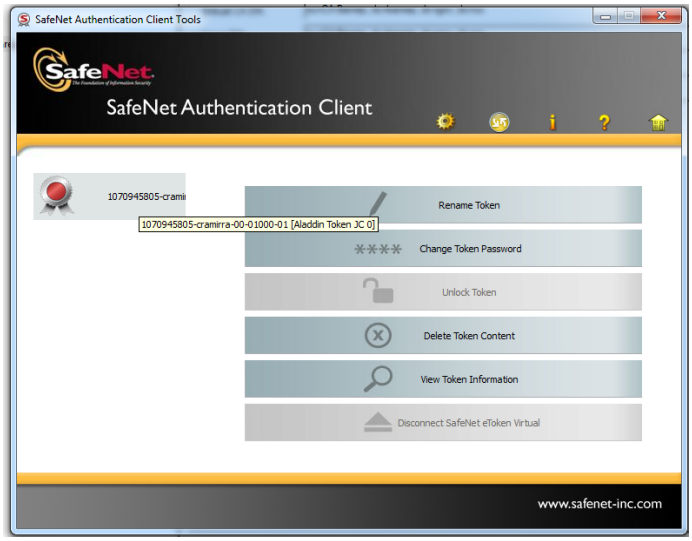
Si la contraseña ingresada corresponde a la especificada para el Token, el sistema continuará con el proceso de creación.



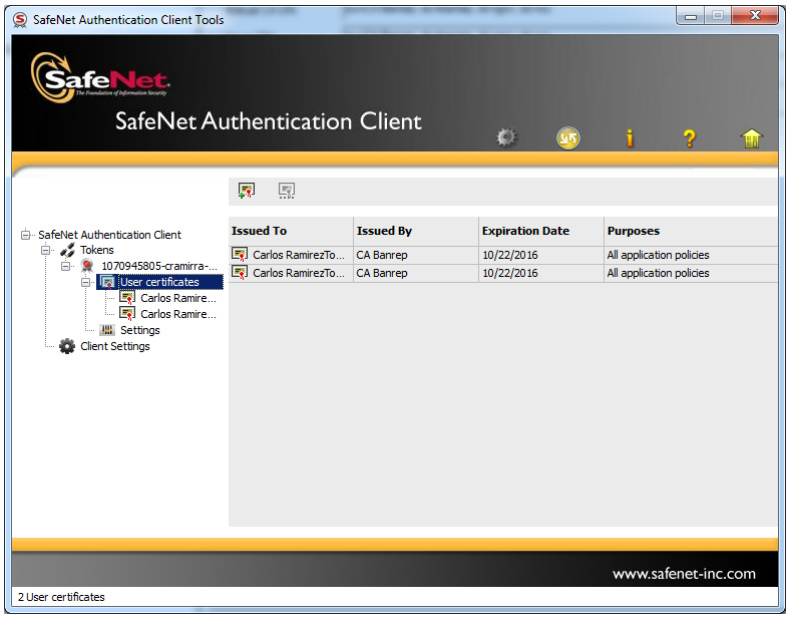
Una vez finalice, se indica que el proceso ha terminado "***The Enroll for Entrust Digital ID Wizard has completed***", de clic en "Finalizar"

Nota: Si el proceso de Creación no terminó correctamente deberá verificar que el equipo se encuentra en línea a través de WSEBRA. Si el problema continúa debe contactar a Soporte Informático del Banco de la República.

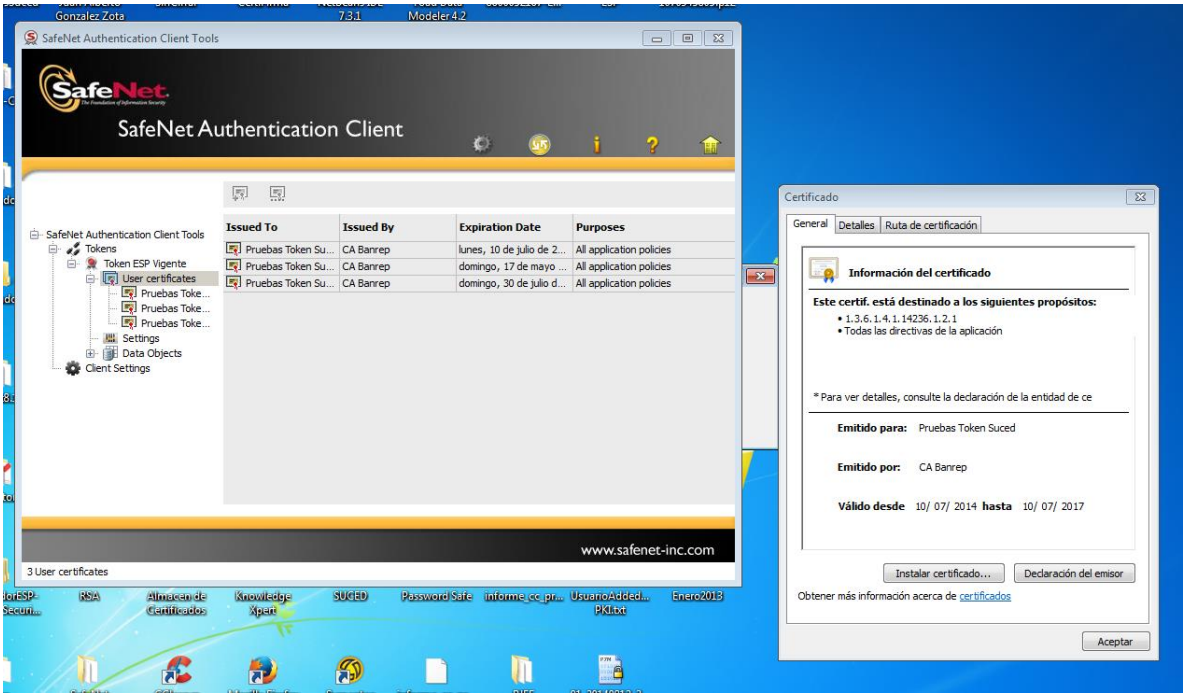
A continuación, debe verificar la creación de las llaves criptográficas abriendo el cliente "Safenet Authentication Client". En la ventana principal (Parte Izquierda) se ve la información del nombre del Token.



Seleccionar la opción  . Se debe observar el par de llaves criptográficas almacenadas en el Token (para operaciones de firma y cifrado).



En esta sección podremos validar los datos de las llaves, los cuales deben tener una relación directa con la solicitud realizada al Banco.



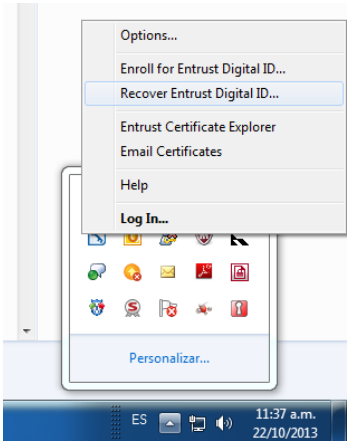
3.3 RECUPERACIÓN DE LLAVES CRIPTOGRÁFICAS PARA IDENTIDAD ELECTRÓNICA TIPO PERTENENCIA EMPRESA

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***).

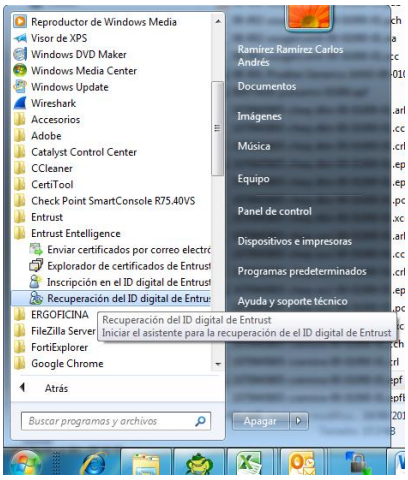
Existen dos opciones para iniciar el proceso de Recuperación del Profile (Recover), las cuales se describen a continuación:

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, tal como se ilustra en la siguiente imagen.

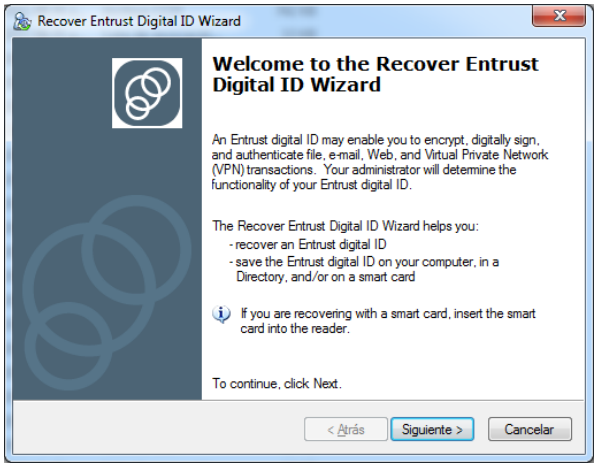
.



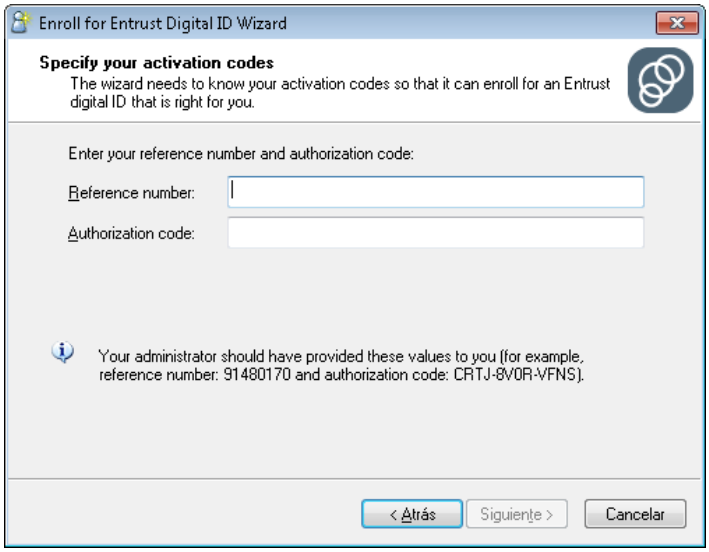
Opción 2: Diríjase a Inicio → Todos los programas → Entrust Entelligence → "Recuperación del ID Digital de Entrust".



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

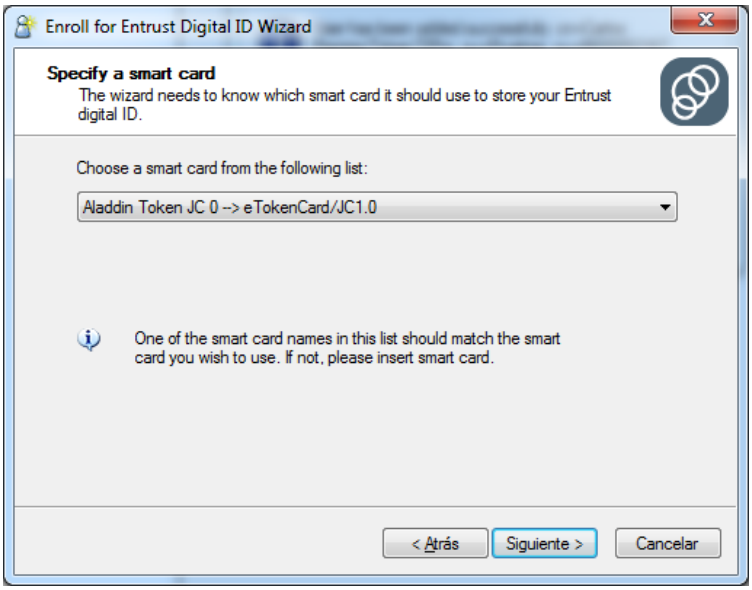


A continuación, se debe ingresar el código de autorización y número de referencia provistos por el Banco de la República y dar clic en “Siguiente”

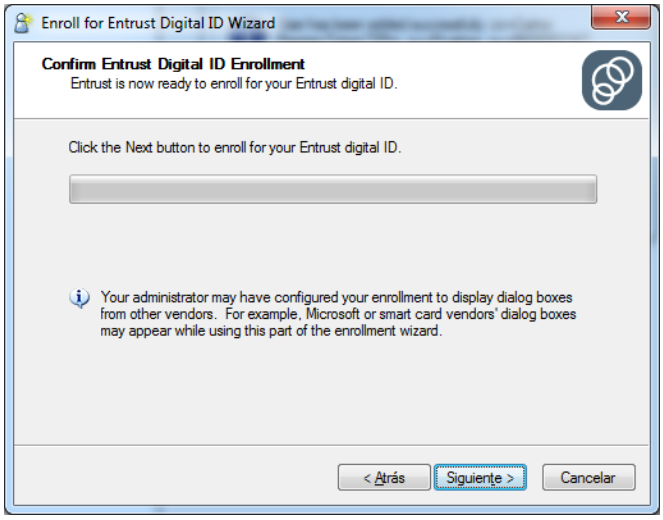


El sistema detectará que el Token está conectado en el PC.

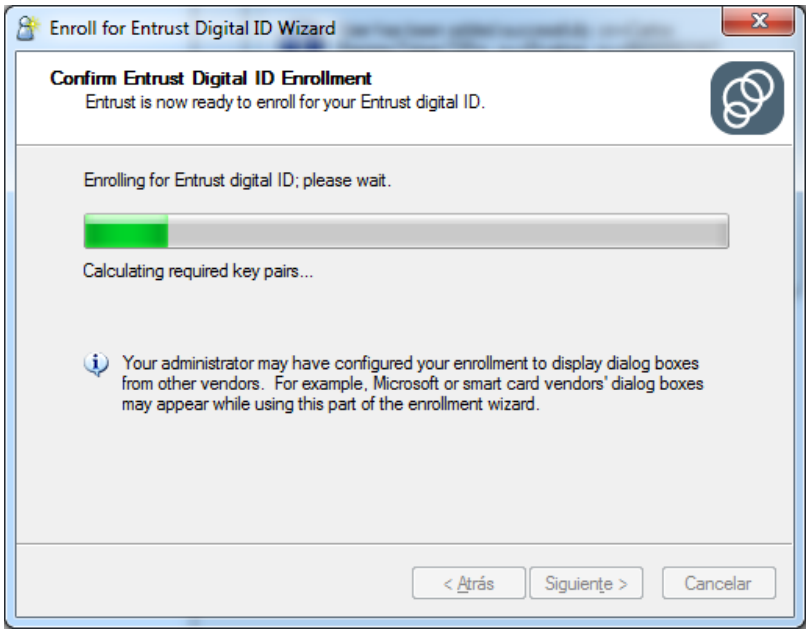
Seleccionar “Siguiente”.



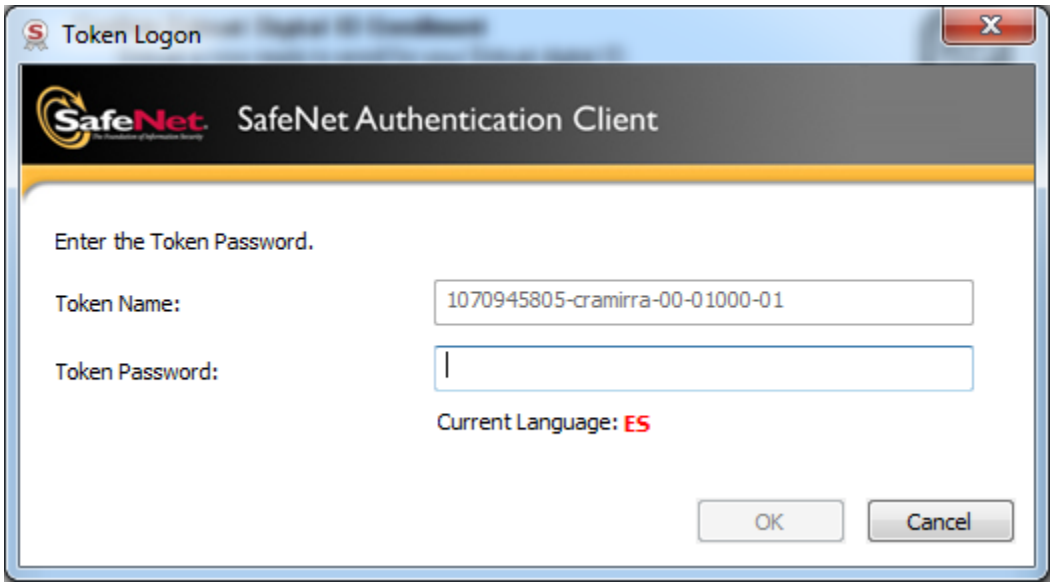
Seleccionar “Siguiente”



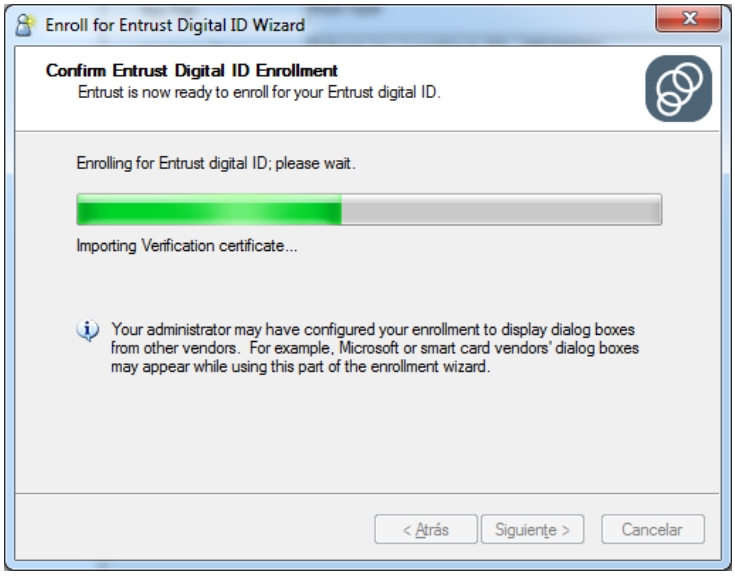
Al seleccionar “Siguiente” comenzara el proceso de Recuperación (creación de nuevas llaves criptográficas para la Identidad Electrónica).



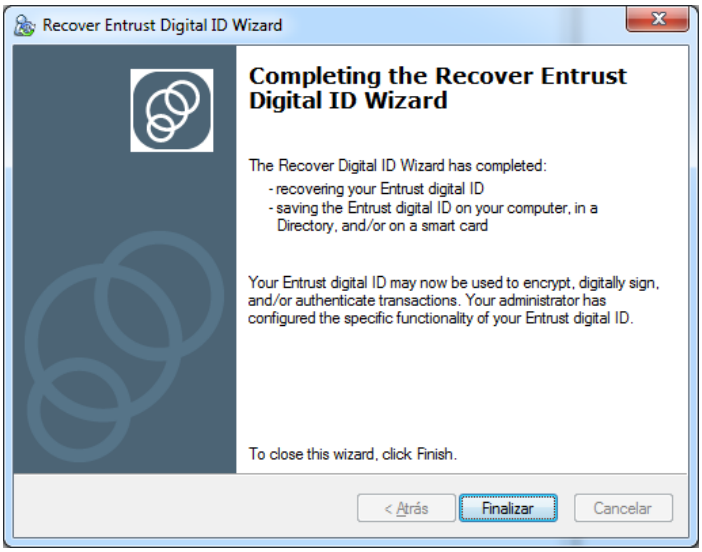
El cliente SafeNet Authentication Client solicita la clave del token (Ver sección ***3.1 Inicializar Token***), ingresarla y seleccionar OK.



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

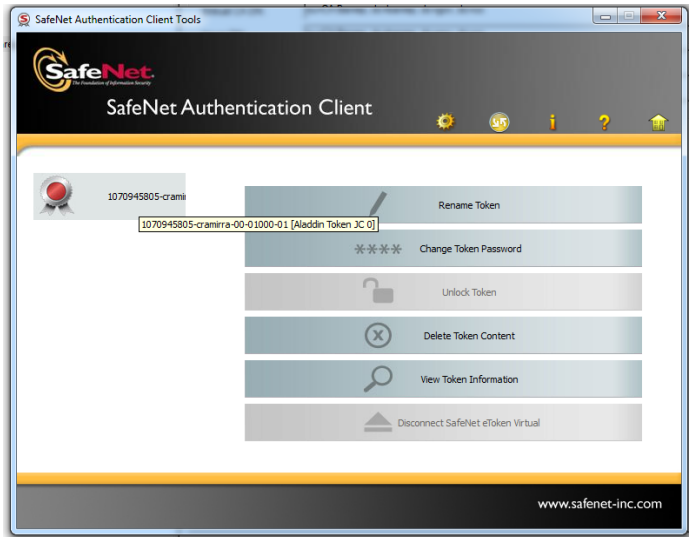


Una vez finalice el proceso, se mostrará la confirmación que el proceso ha terminado "***The Recover Digital ID Wizard has completed***"

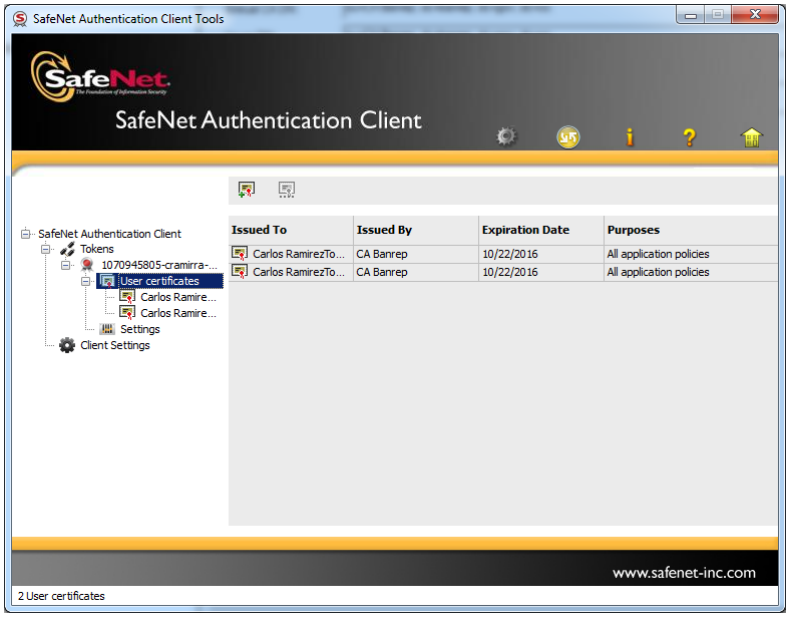


Nota: Si el proceso de Recuperación no termino correctamente deberá verificar que se encuentra en línea a través de WSEBRA. Si el problema continúa debe contactar a Soporte Informático del Banco de la República.

A continuación, deber verificar la creación de las nuevas llaves abriendo el cliente "Safenet Authentication Client", en la ventana principal (Parte Izquierda) puede ver la información del nombre del Token.



Seleccionar la opción  . Se debe ver el par de llaves criptográficas almacenadas (para operaciones de firma y cifrado).



4 GENERACIÓN DE LLAVES CRIPTOGRÁFICAS PARA IDENTIDAD ELECTRÓNICA TIPO PERSONA JURIDICA ENTIDAD EMPRESA

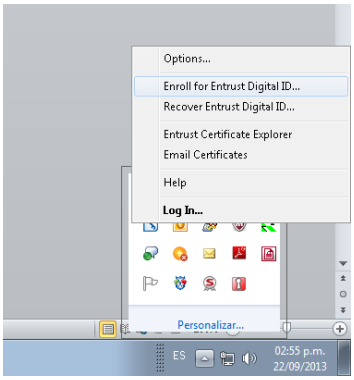
Para realizar este proceso se debe contar con la información de activación (el código de autorización y número de referencia suministrados por el Banco de la República) y con acceso a WSEBRA, y verificar la sección 2 (***Requisitos***).

A diferencia de la Identidad Electrónica tipo Pertenencia a Empresa, este tipo de Identidad Electrónica utiliza como repositorio de llaves criptográficas un Instrumento de Firma tipo **Contenedor Digital** (archivo electrónico que se genera y almacena en el equipo del suscriptor).

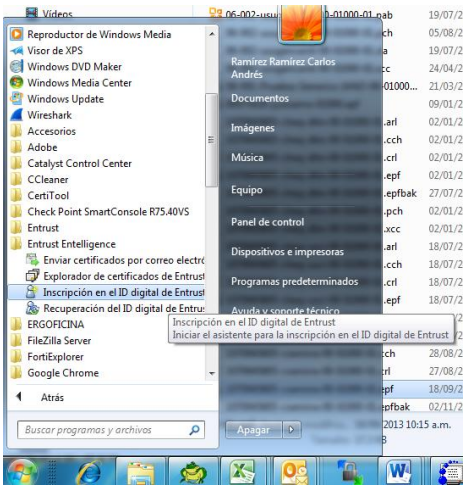
4.1 CREACIÓN DE LLAVES CRIPTOGRÁFICAS PARA IDENTIDAD ELECTRÓNICA TIPO PERSONA JURÍDICA ENTIDAD EMPRESA

Existen dos opciones de iniciar el proceso de Creación (Enroll) de llaves criptográficas asociadas a este tipo de Identidad Electrónica, a saber:

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.

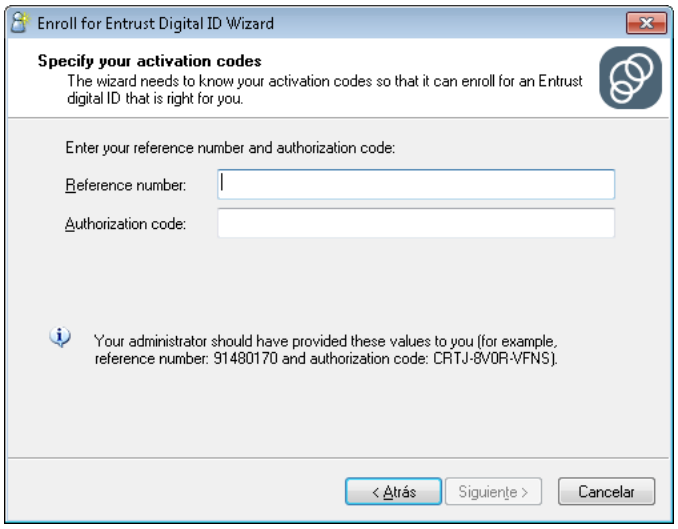


Opción 2: Ir a Inicio → Todos los programas → Entrust Entelligence → "Inscripción en el ID Digital de Entrust".

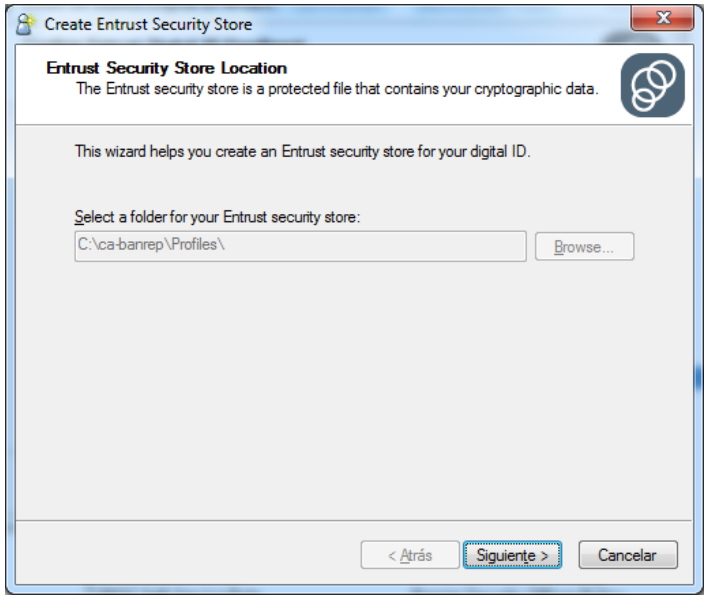


Una vez seleccionada esta opción, se abrirá la siguiente ventana. Seleccionar "siguiente".

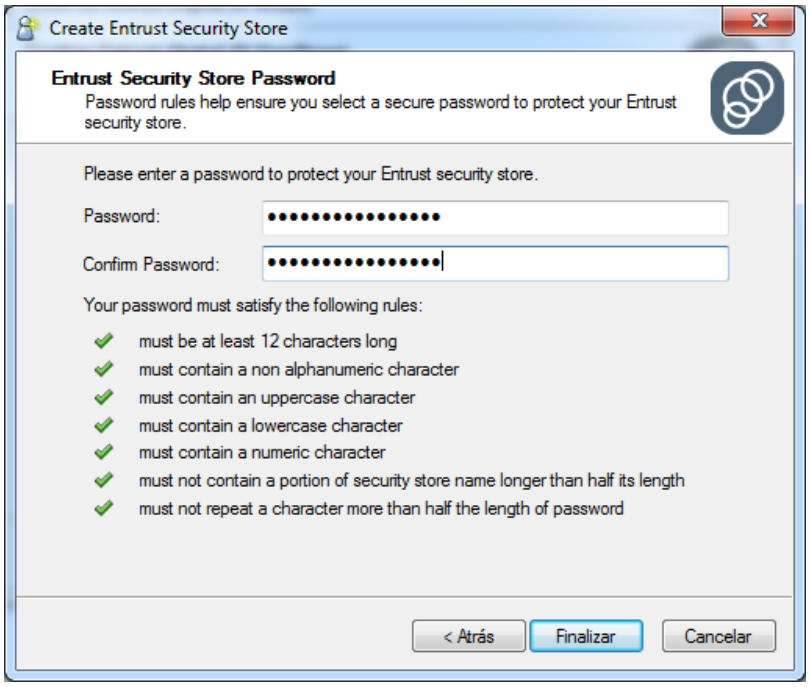
A continuación, debe ingresar el código de autorización y número de referencia provistos por el Banco de la República y dar clic en "Siguiente"



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



Se debe establecer la contraseña (Entrust Security Store Password) del Profile, la cual deberá cumplir con las condiciones exigidas.



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

Para Certificados Persona Jurídica Entidad Empresa para comunicaciones 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

Para Certificados Persona Jurídica Entidad Empresa para Automatización de operaciones criptográficas:

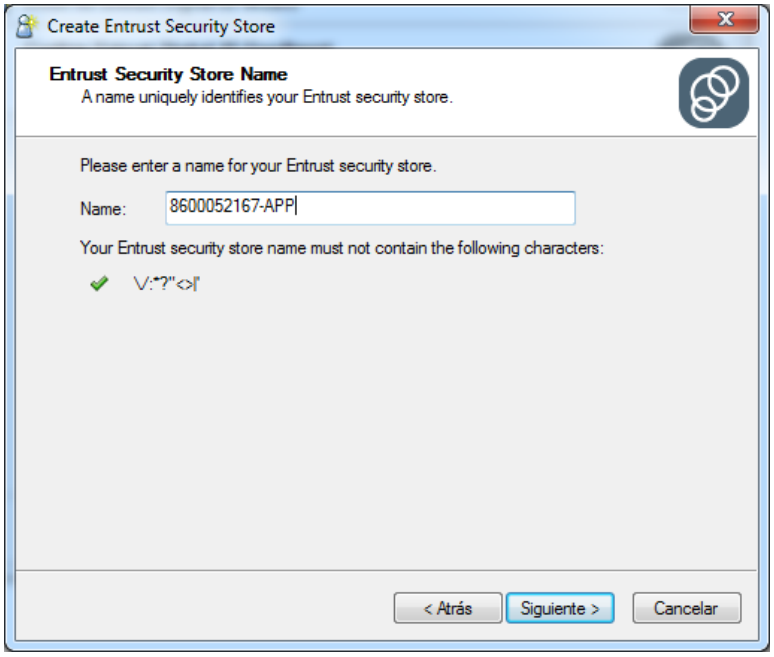
NIT Entidad-"Aplicación con la que va a interactuar"

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

Para Certificados Persona Jurídica Entidad Empresa para Consumo de Servicios de Mensajería:

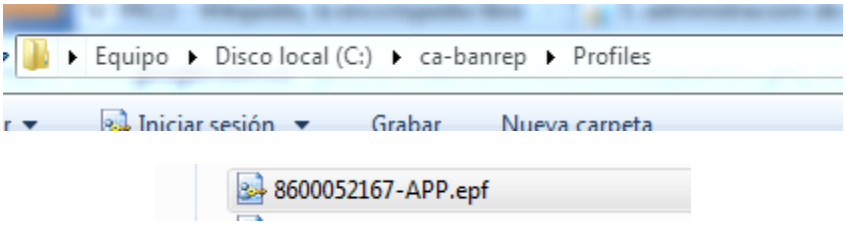
MBR-NIT Entidad-“Aplicación con la que va a interactuar”

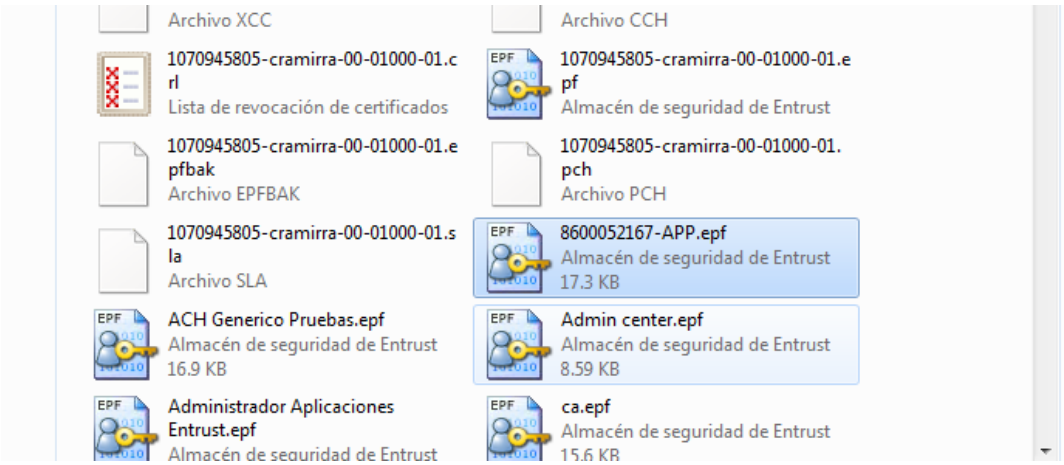
Ejemplo: NIT Banco de la República es 860.005.216-7 y la aplicación con que va usar el certificado es Cuentas de Depósito CUD, el nombre del profile será: MBR-8600052167-CUD



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

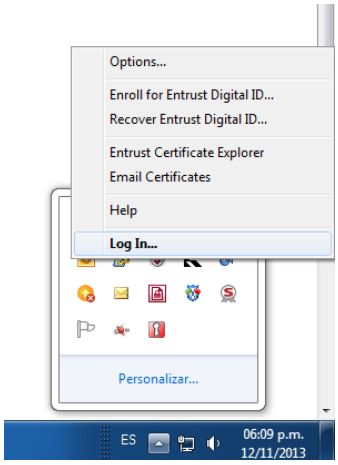
Por defecto la ubicación del Profile será la ruta ***c:\ca-banrep\profiles\.*** La ruta podrá ser modificada a la establecida por el usuario en el proceso mencionado anteriormente. El archivo tendrá el nombre que el usuario haya establecido en el proceso de creacion y la extension definida para este tipo de archivo (.epf).



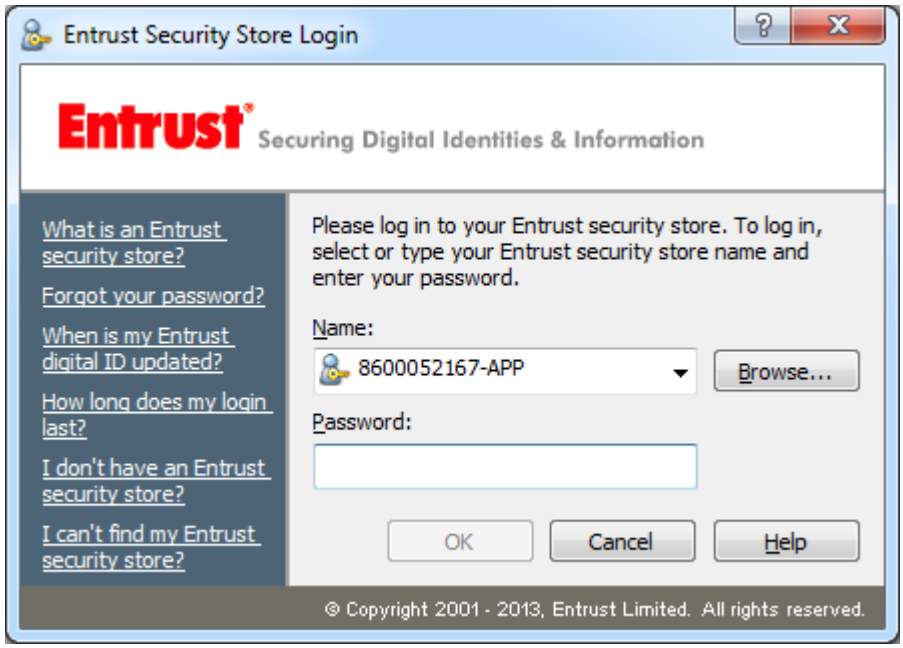


Una vez identificada la ubicación del profile se debe proceder a hacer el login con el profile previamente creado.

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 nombre del profile correspondiente.

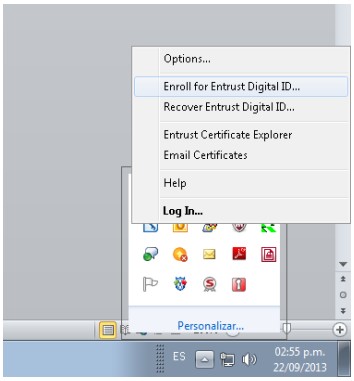


Ingrese la contraseña del Profile para hacer el Login.

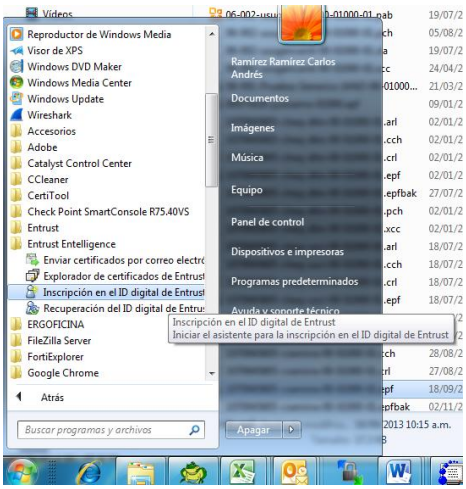
4.2 RECUPERACIÓN DE LLAVES CRIPTOGRÁFICAS PARA IDENTIDAD ELECTRÓNICA TIPO PERSONA JURÍDICA ENTIDAD EMPRESA

Existen dos opciones de iniciar el proceso de Recuperación (Recover) de llaves criptográficas asociadas a este tipo de Identidad Electrónica, a saber:

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.

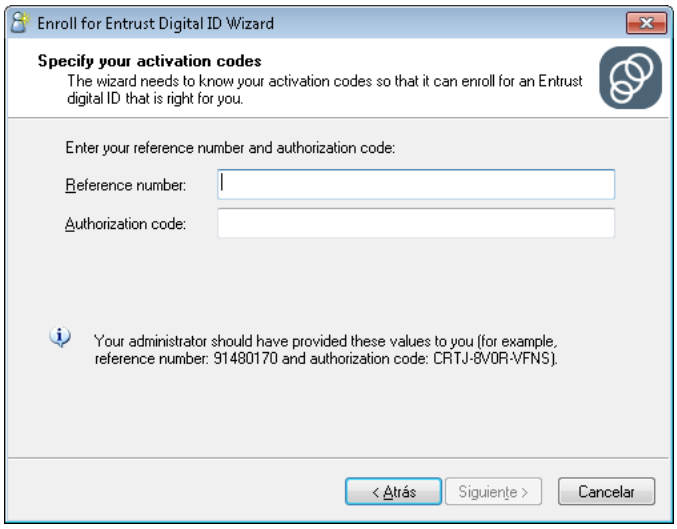


Opción 2: Ir a Inicio → Todos los programas → Entrust Entelligence → "Recuperación del ID Digital de Entrust".

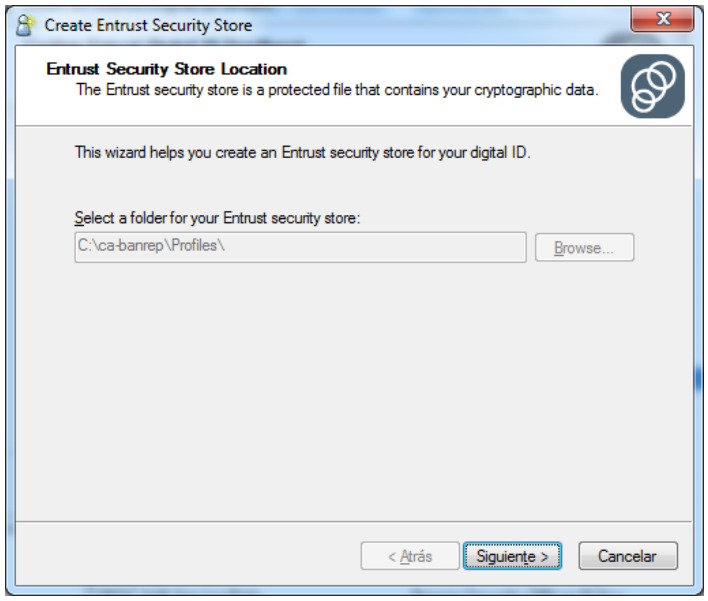


Una vez seleccionada esta opción, se abrirá la siguiente ventana. Seleccionar “siguiente”.

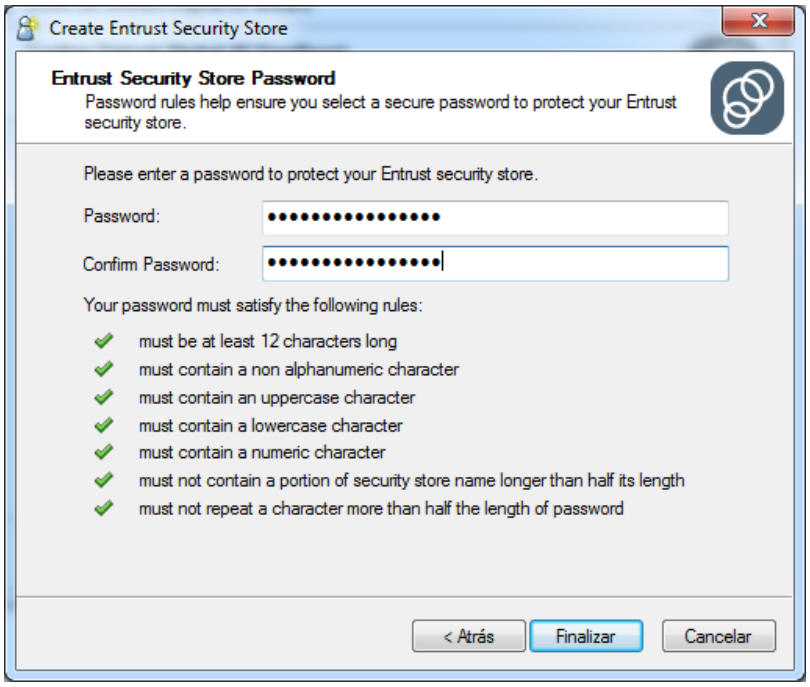
A continuación, debe ingresar el código de autorización y número de referencia provistos por el Banco de la República y dar clic en “Siguiente”



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 (Entrust Security Store Password) del Profile, la cual deberá cumplir con las condiciones exigidas.



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

Para Certificados Persona Jurídica Entidad Empresa (PJEE) para comunicaciones 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

Para Certificados Persona Jurídica Entidad Empresa (PJEE) para Automatización de operaciones criptográficas:

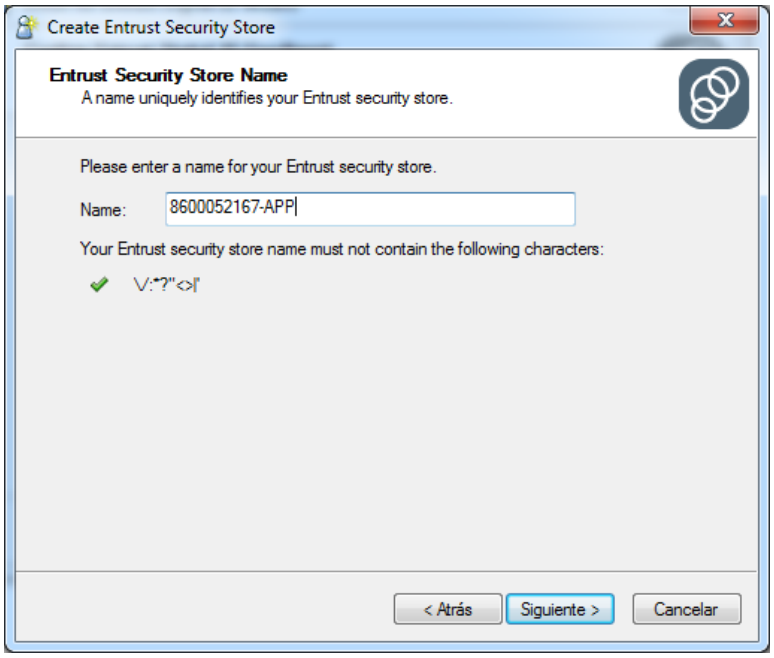
NIT Entidad-"Aplicación con la que va a interactuar"

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

Para Certificados Persona Jurídica Entidad Empresa para Consumo de Servicios de Mensajería:

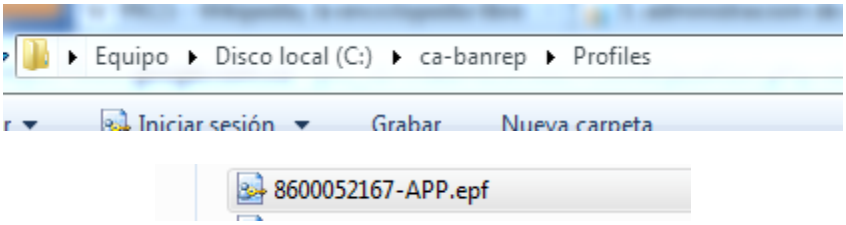
MBR-NIT Entidad-"Aplicación con la que va a interactuar"

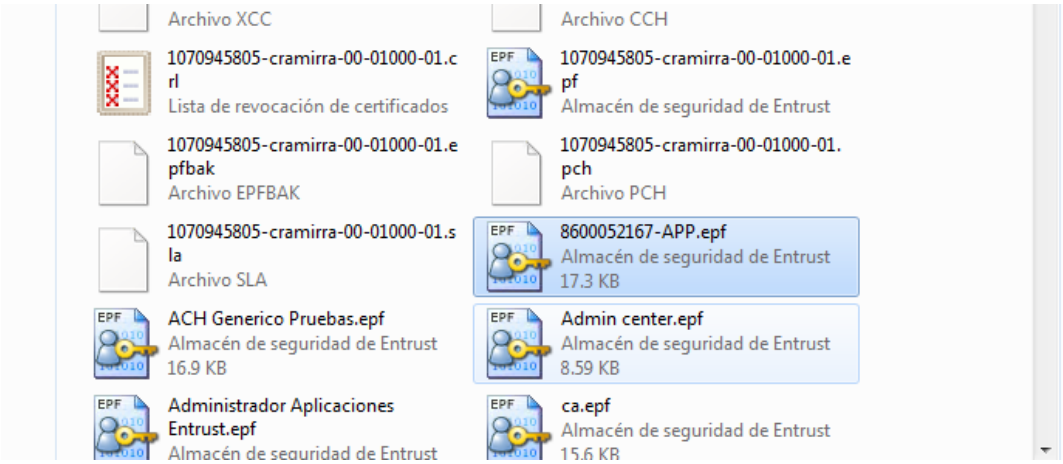
Ejemplo: NIT Banco de la República es 860.005.216-7 y la aplicación con que va usar el certificado es Cuentas de Depósito CUD, el nombre del profile será: MBR-8600052167-CUD



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

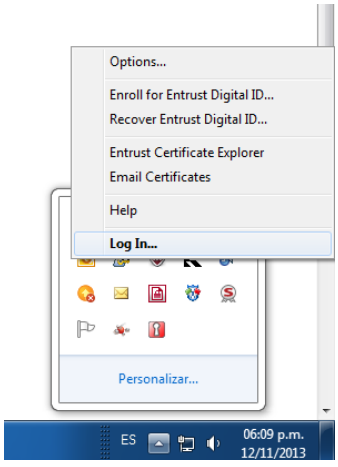
Por defecto la ubicación del Profile será la ruta ***c:\ca-banrep\profiles\.*** La ruta podrá ser modificada a la establecida por el usuario en el proceso mencionado anteriormente. El archivo tendrá el nombre que el usuario haya establecido en el proceso de recuperación y la extension definida para este tipo de archivo (.epf).



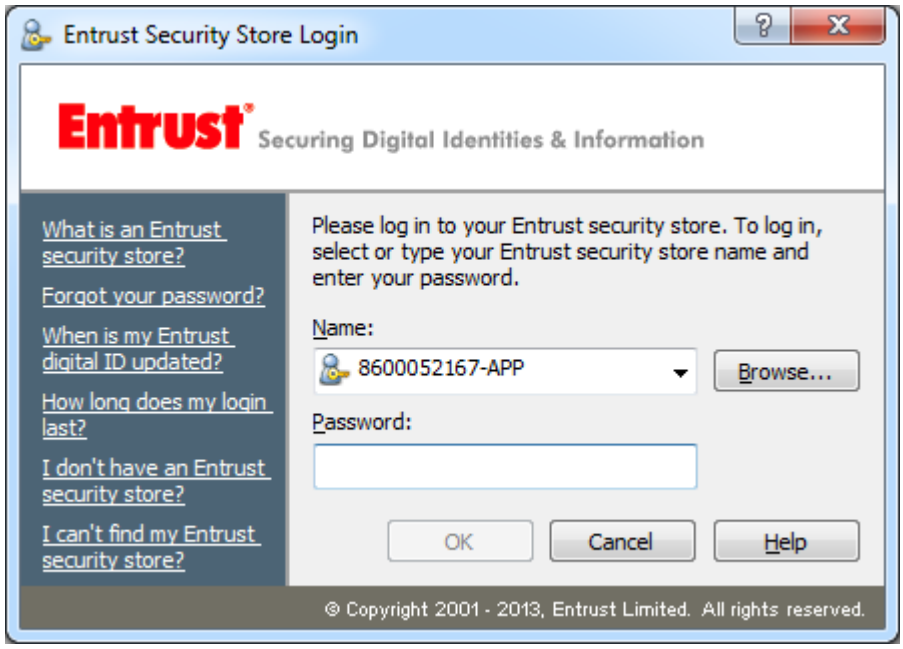


Una vez identificada la ubicación del profile (.epf), se debe proceder a hacer el login con el profile previamente creado.

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.



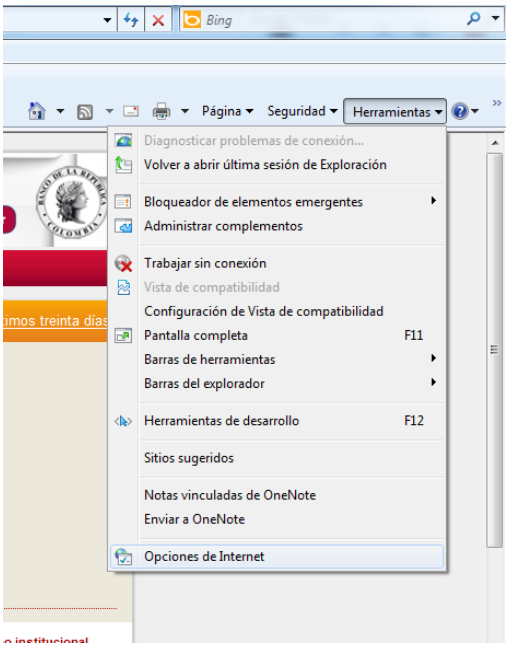
Ingrese la contraseña para hacer el Login.

5 TRANSFORMACIÓN DE CREDENCIALES

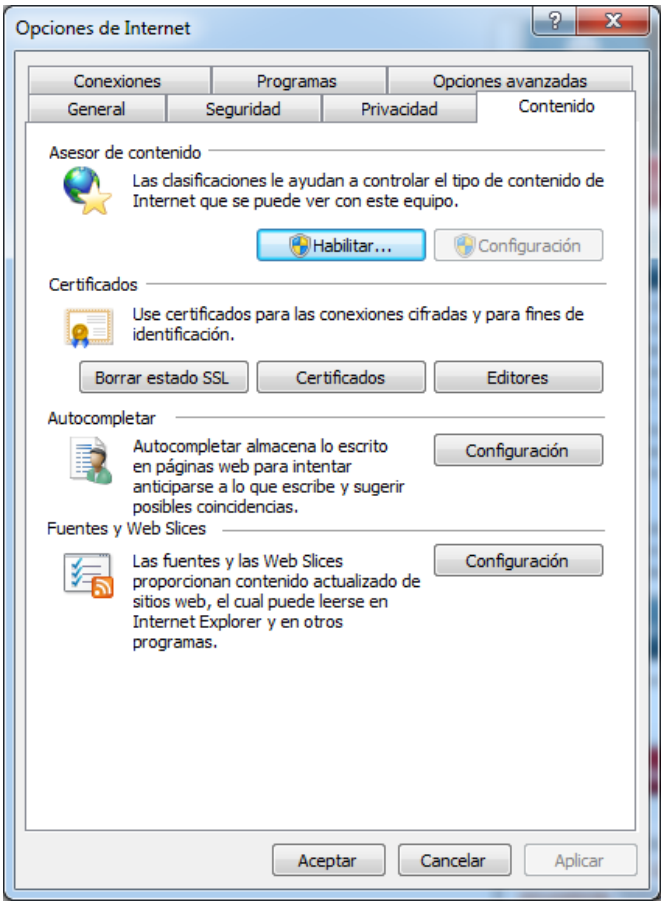
Después de realizar la creación del profile y por requiermientos de interoperabilidad se podrá realizar el procedimiento de Transformación de Credenciales que se detalla en esta sección. Este procedimiento permite exportar las llaves criptográficas del Profile a contenedores digitales en formato PKCS#12 (archivo con extensión ".p12 o .pfx) o en formato Java key Store (archivo con extensión ".jks"). Antes de ejecutar este procedimiento se debe haber realizado el Login en el Profile respectivo de acuerdo a lo ilustrado en la sección anterior.

Ingresar al navegador "Internet Explorer".

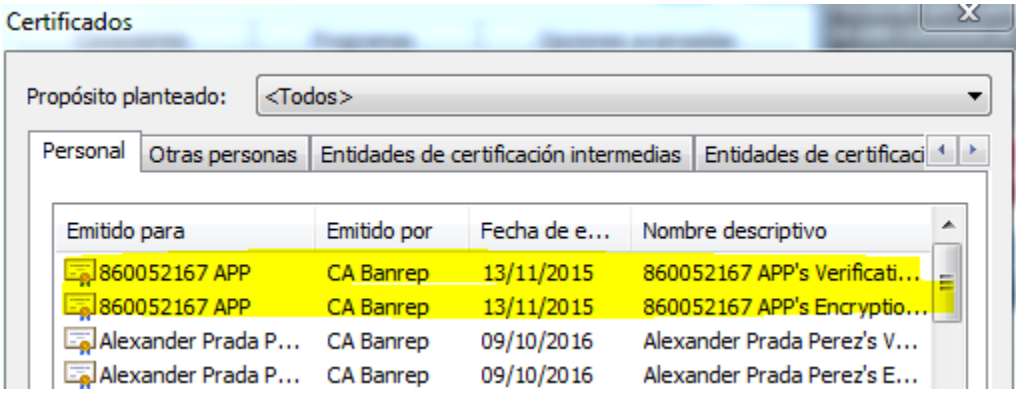
Ir a la sección Herramientas.



En Herramientas, ir a la sección Contenido → Certificados.



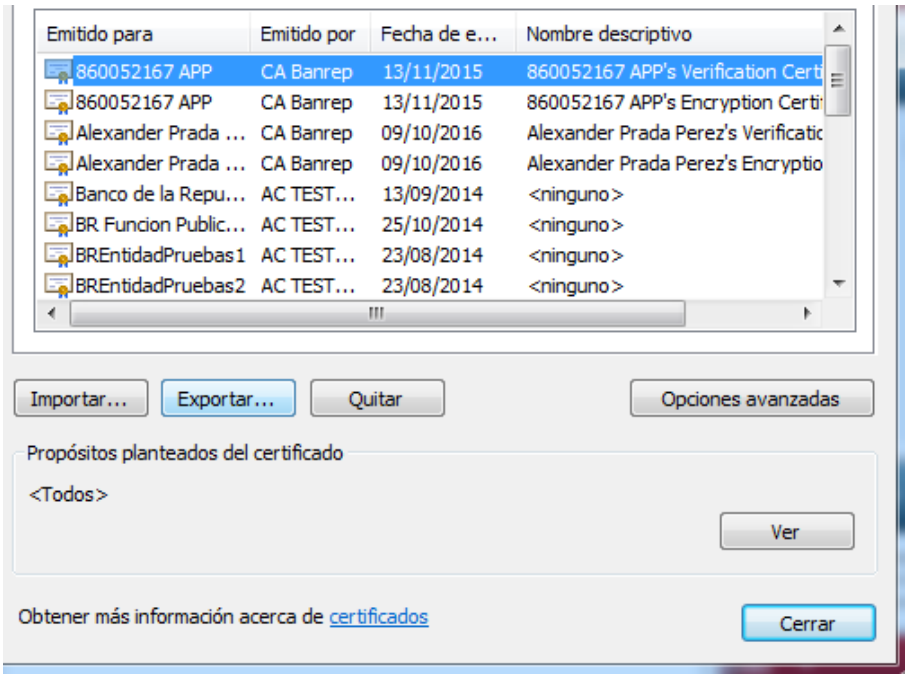
Una vez ubicado en la sección Certificados, se visualizarán las llaves criptográficas correspondientes al Profile creado.



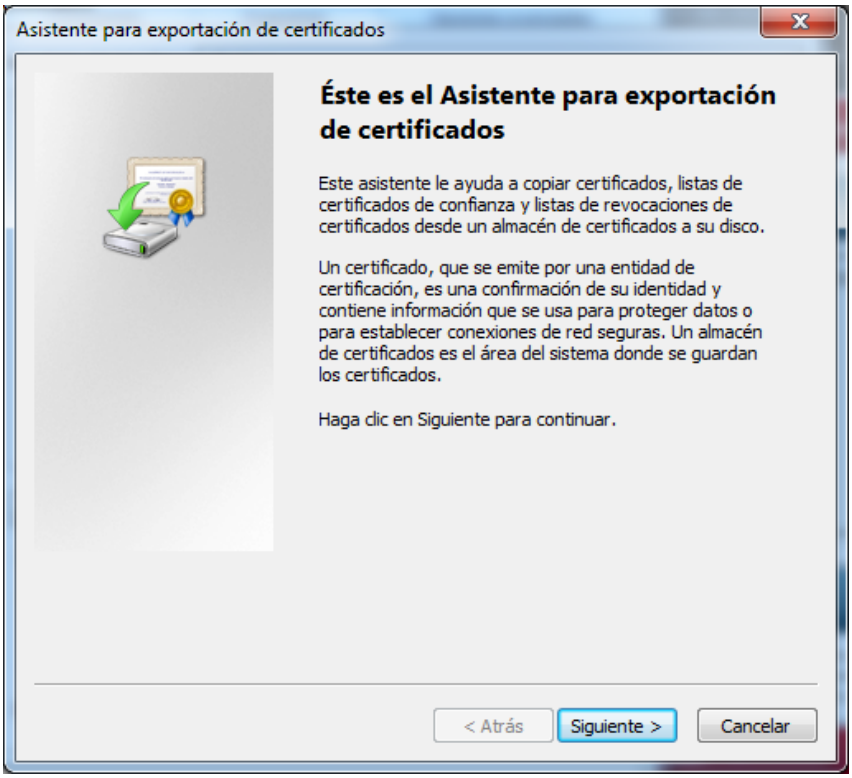
Serán visibles dos llaves, una utilizada para encriptar y otra para verificación de firma. Para cada una de estas llaves se deberá ejecutar la exportación de llaves.

Exportar Llave de Verificación de Firma:

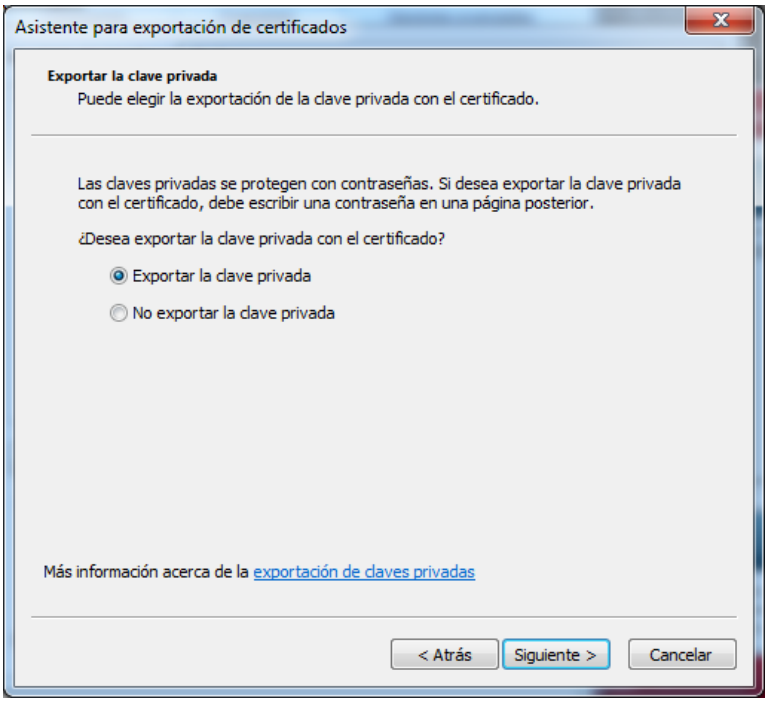
Seleccionar la llave cuyo nombre descriptivo sea “Verification Certificate” y hacer clic en Exportar.



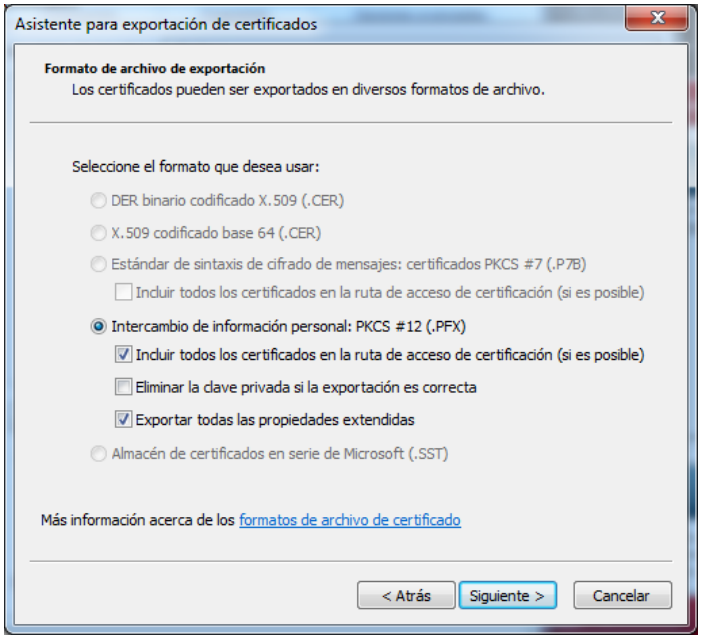
Se debe hacer click en siguiente.



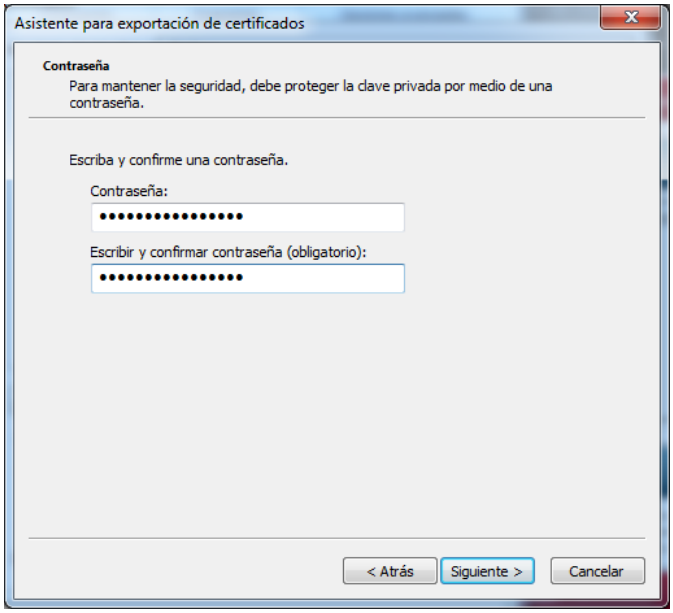
A continuacipon, se deberá seleccionar la opción “Exportar la llave privada”



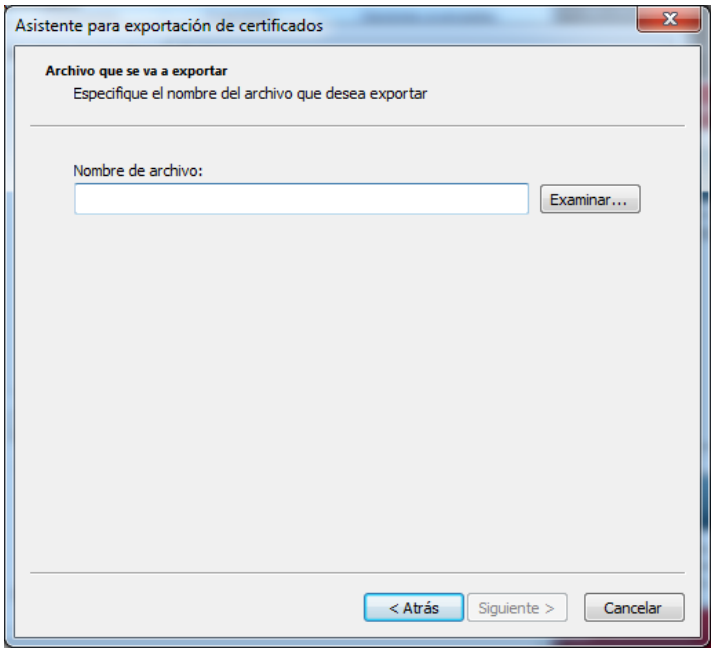
Se debe seleccionar las opciones mostradas a continuación:

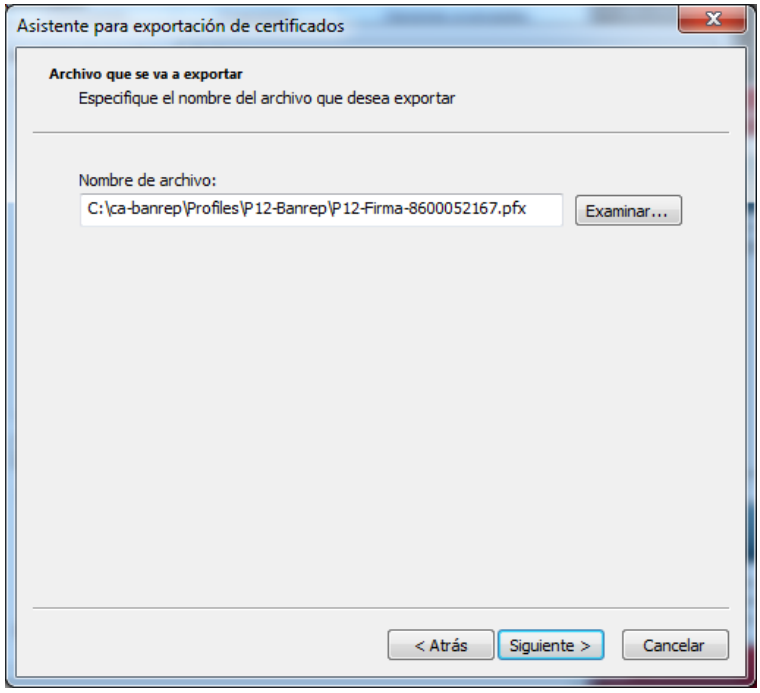


Se procede a establecer la contraseña del nuevo archivo PKCS#12 para realizar operaciones de firma. Es importante que esta contraseña cumpla con características minimas de composición tales como número de caracteres, mayusculas, minusculas, numeros y caracteres especiales.

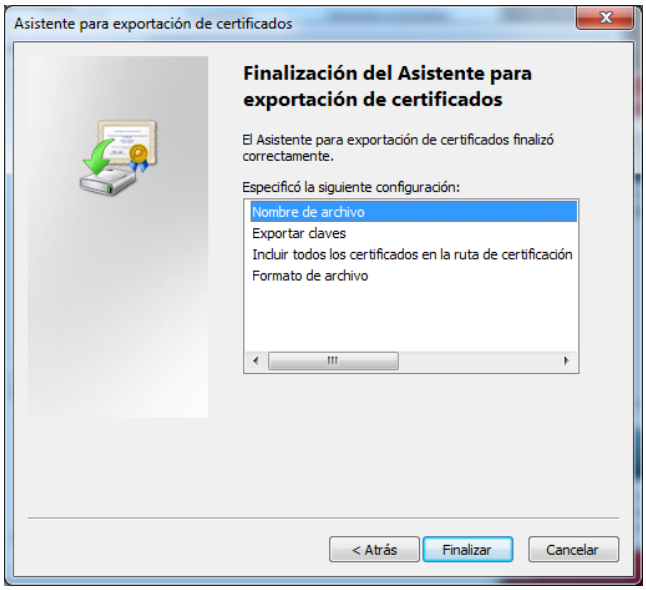


Proceder a establecer un nombre al archivo.

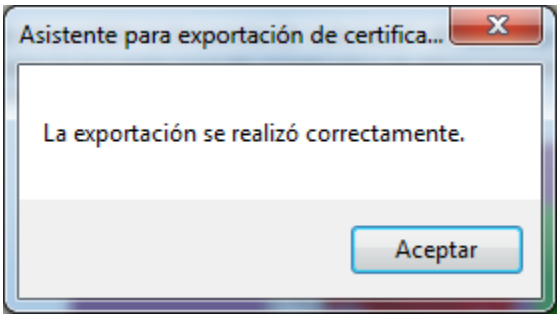




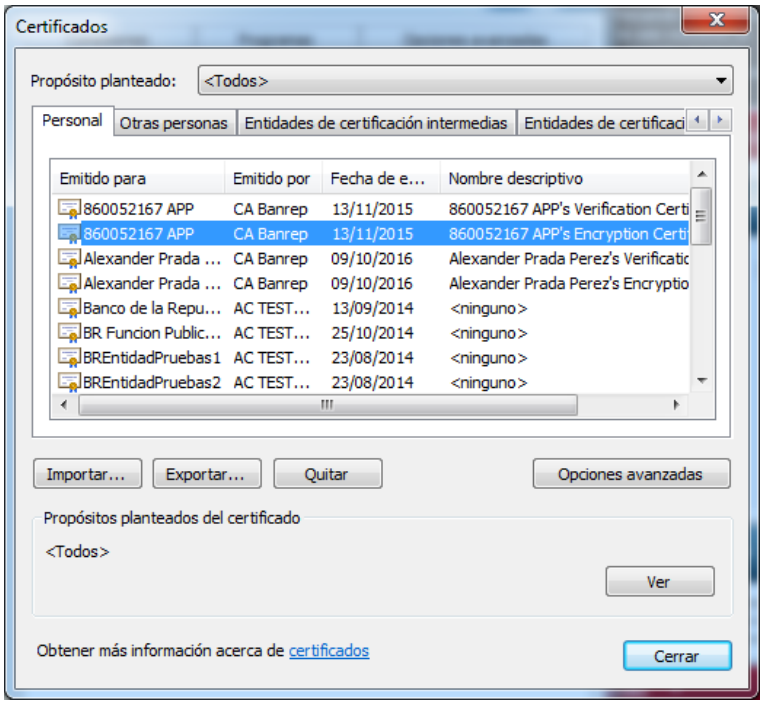
Pulsamos Finalizar para terminar el proceso de exportación.

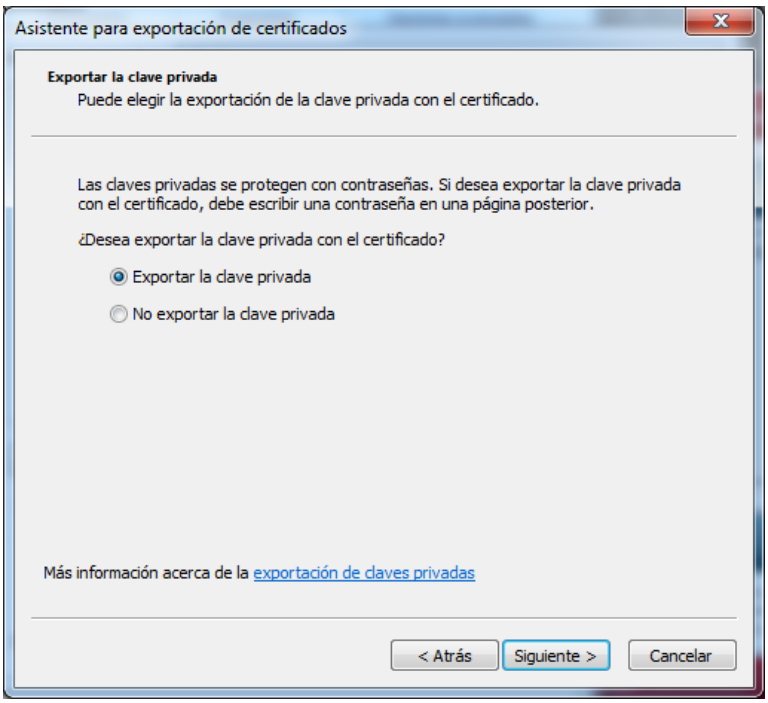


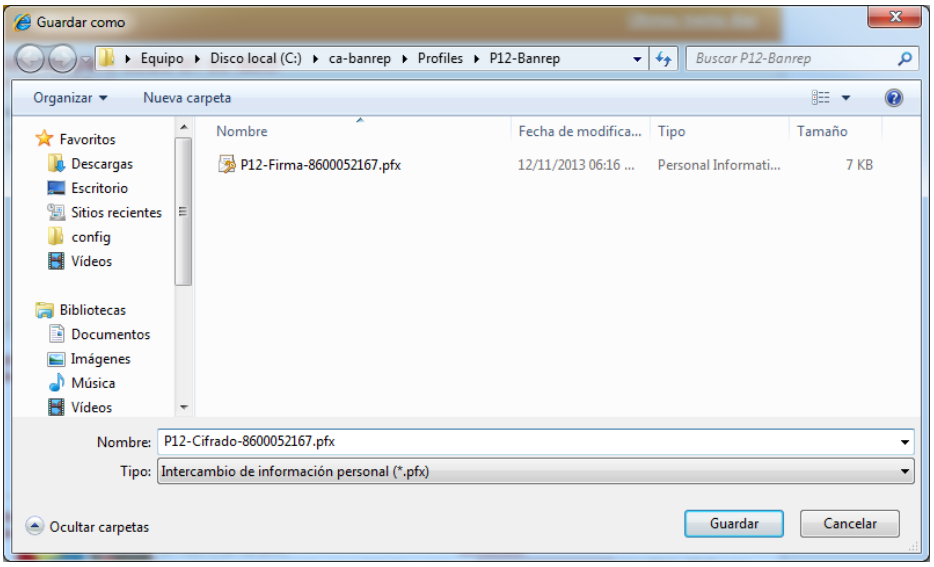
Verificamos que la exportación se realizo correctamente.

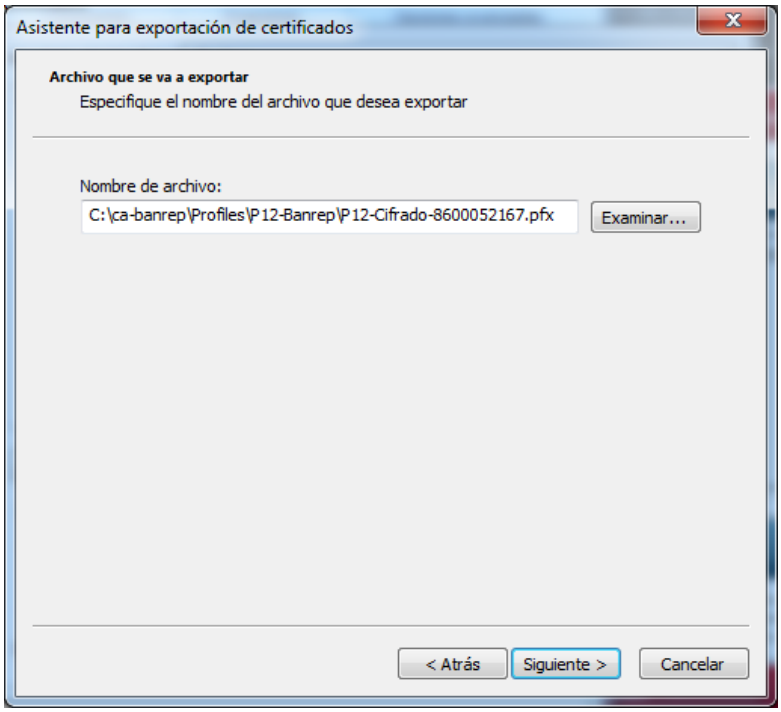


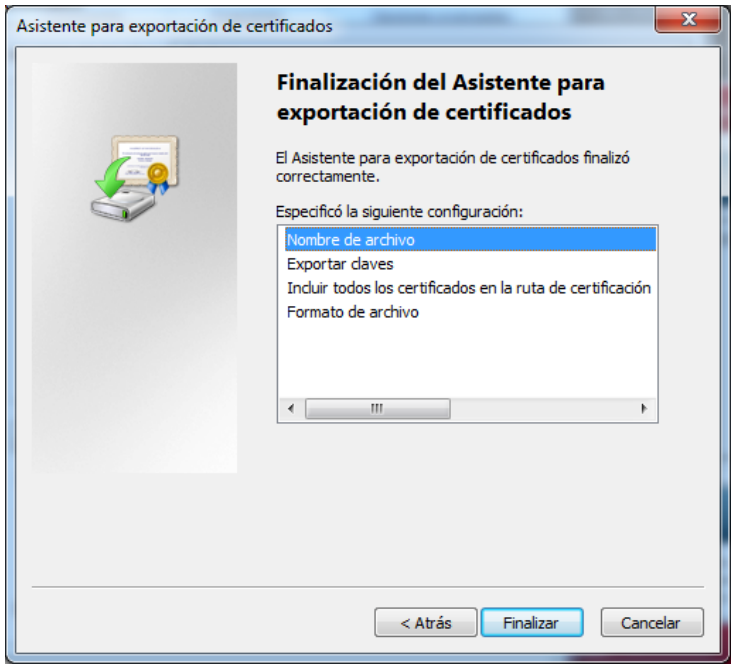
A continuación se debe realizar el mismo proceso para la llave con Nombre descriptivo "**Encryption Certificate**"

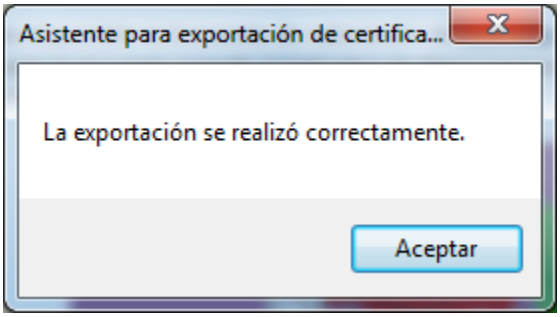

Certificados
Propósito planteado:
<Todos>
Personal
Otras personas
Entidades de certificación intermedias
Entidades de certificaci
Emitido para
Emitido por
Fecha de e...
Nombre descriptivo
860052167 APP
CA Banrep
13/11/2015
860052167 APP's Verification Certi
860052167 APP
CA Banrep
13/11/2015
860052167 APP's Encryption Certi
Alexander Prada ...
CA Banrep
09/10/2016
Alexander Prada Perez's Verificatic
Alexander Prada ...
CA Banrep
09/10/2016
Alexander Prada Perez's Encryptio
Banco de la Repu...
AC TEST...
13/09/2014
<ninguno>
BR Funcion Public...
AC TEST...
25/10/2014
<ninguno>
BREntidadPruebas1
AC TEST...
23/08/2014
<ninguno>
BREntidadPruebas2
AC TEST...
23/08/2014
<ninguno>
Importar...
Exportar...
Quitar
Opciones avanzadas
Propósitos planteados del certificado
<Todos>
Ver
Obtener más información acerca de certificados
Cerrar


Asistente para exportación de certificados
Exportar la clave privada
Puede elegir la exportación de la clave privada con el certificado.
Las claves privadas se protegen con contraseñas. Si desea exportar la clave privada con el certificado, debe escribir una contraseña en una página posterior.
¿Desea exportar la clave privada con el certificado?
Exportar la clave privada
No exportar la clave privada
Más información acerca de la exportación de claves privadas
< Atrás
Siguiente >
Cancelar


Guardar como
Equipo ▸ Disco local (C:) ▸ ca-banrep ▸ Profiles ▸ P12-Banrep
Buscar P12-Banrep
Organizar
Nueva carpeta
Favoritos
Descargas
Escritorio
Sitios recientes
config
Vídeos
Bibliotecas
Documentos
Imágenes
Música
Vídeos
Nombre
Fecha de modifica...
Tipo
Tamaño
P12-Firma-8600052167.pfx
12/11/2013 06:16 ...
Personal Informati...
7 KB
Nombre: P12-Cifrado-8600052167.pfx
Tipo: Intercambio de información personal (*.pfx)
Ocultar carpetas
Guardar
Cancelar


Asistente para exportación de certificados
Archivo que se va a exportar
Especifique el nombre del archivo que desea exportar
Nombre de archivo:
C:\ca-banrep\Profiles\P12-Banrep\P12-Cifrado-8600052167.pfx
Examinar...
< Atrás
Siguiente >
Cancelar





En la ruta seleccionada en el punto anterior, se deben encontrar tener dos archivos con extensión ".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 exportacion de la llave de firma.

Para realizar un proceso de descifrado de información se deberá usar la credencial .pfx correspondiente al proceso de exportacion de la llave de cifrado o encripción.

Exportación a formato Java key Store - JKS

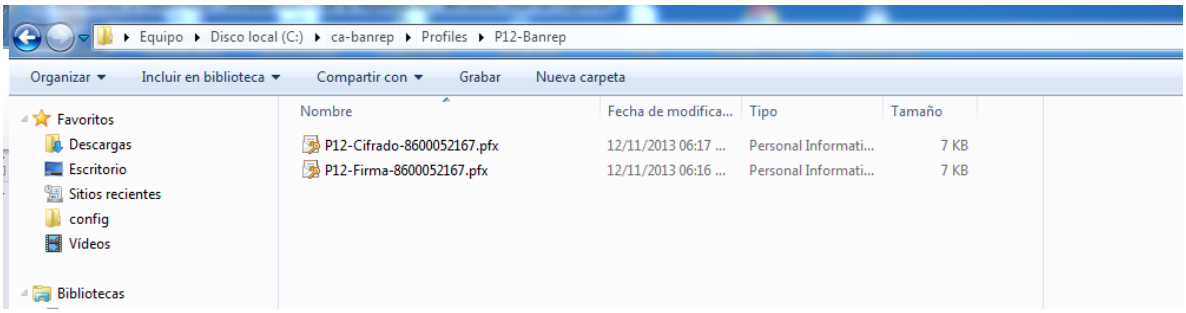
Después de tener los archivos en formato PKCS#12 es posible exportar las llaves a un formato tipo JKS. Para realizar este proceso se puede emplear la utilidad ***keytool*** o el software utilitario Portecle de distribución libre.

Toda vez que Portecle provee una interfaz gráfica que facilita el proceso de exportación de llaves, se presenta a continuación este procedimiento. Si requiere realizar la conversión de formato directamente con la funcionalidad propia de java se podrá recurrir a la documentación ofrecida por Oracle:

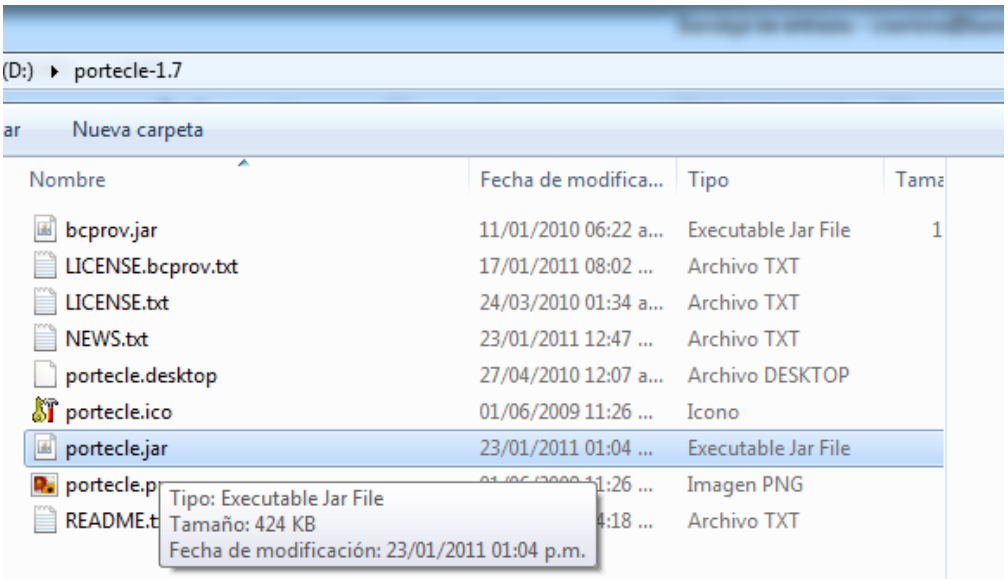
http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html
https://blogs.oracle.com/shyamrao/entry/how_to_import_pfx_file

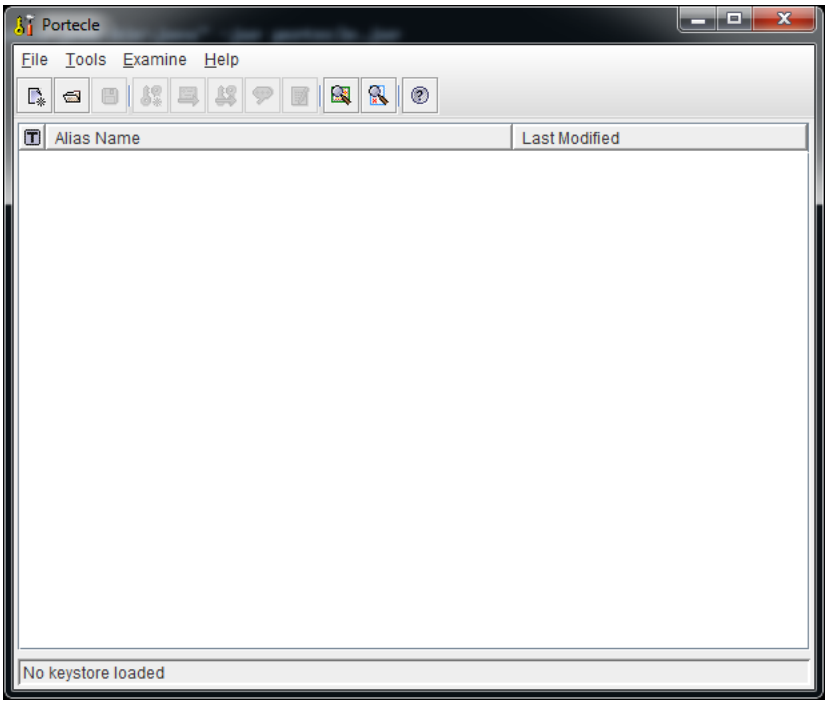
Exportación a JKS con Portecle

Se debe tener conocimiento de la ruta en la que se exportaron las llaves del Profile (según descripción de la sección anterior).

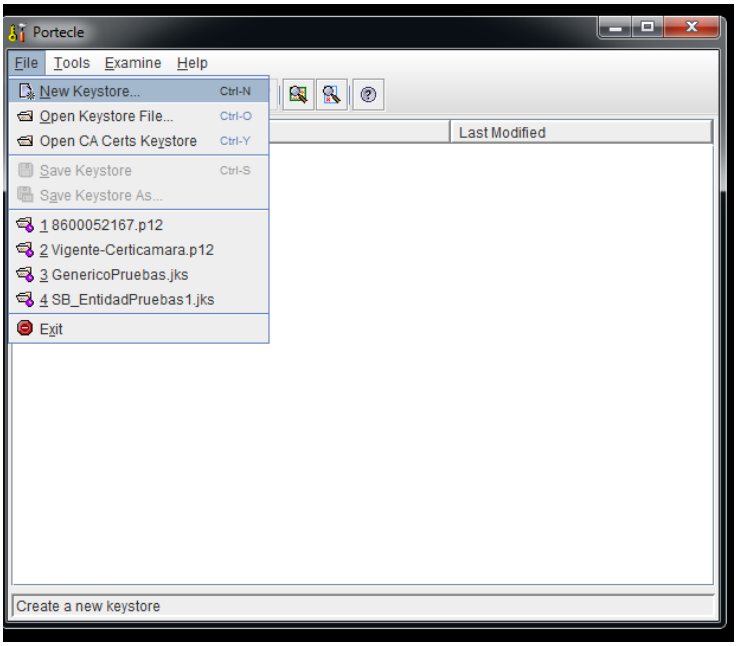


Para abrir el sofware se hace doble click en “portecle.jar”, según se muestra a continuación:

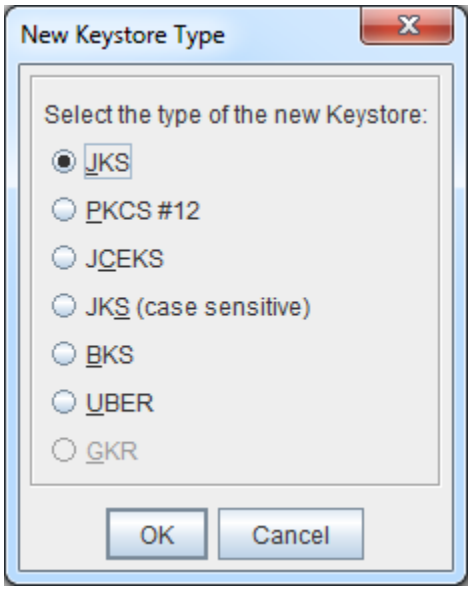


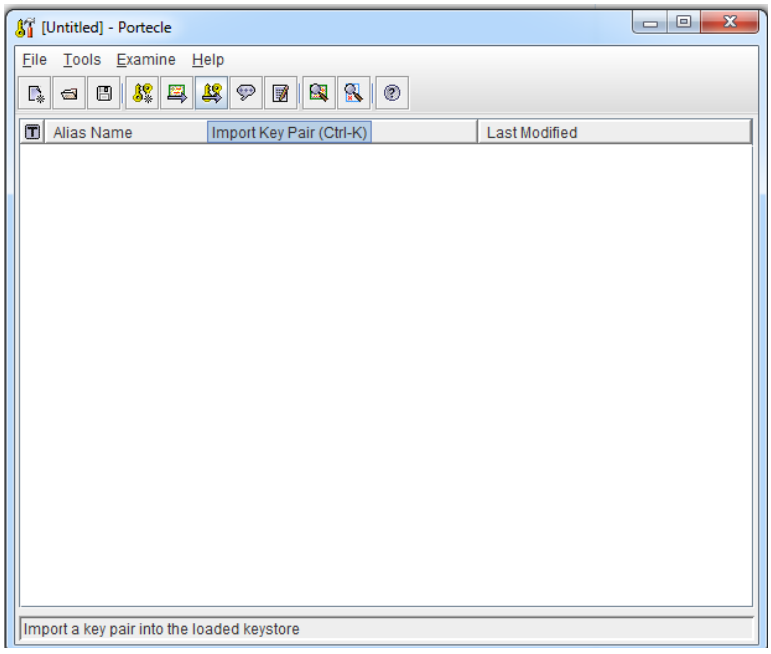


Se selecciona “New Keystore”

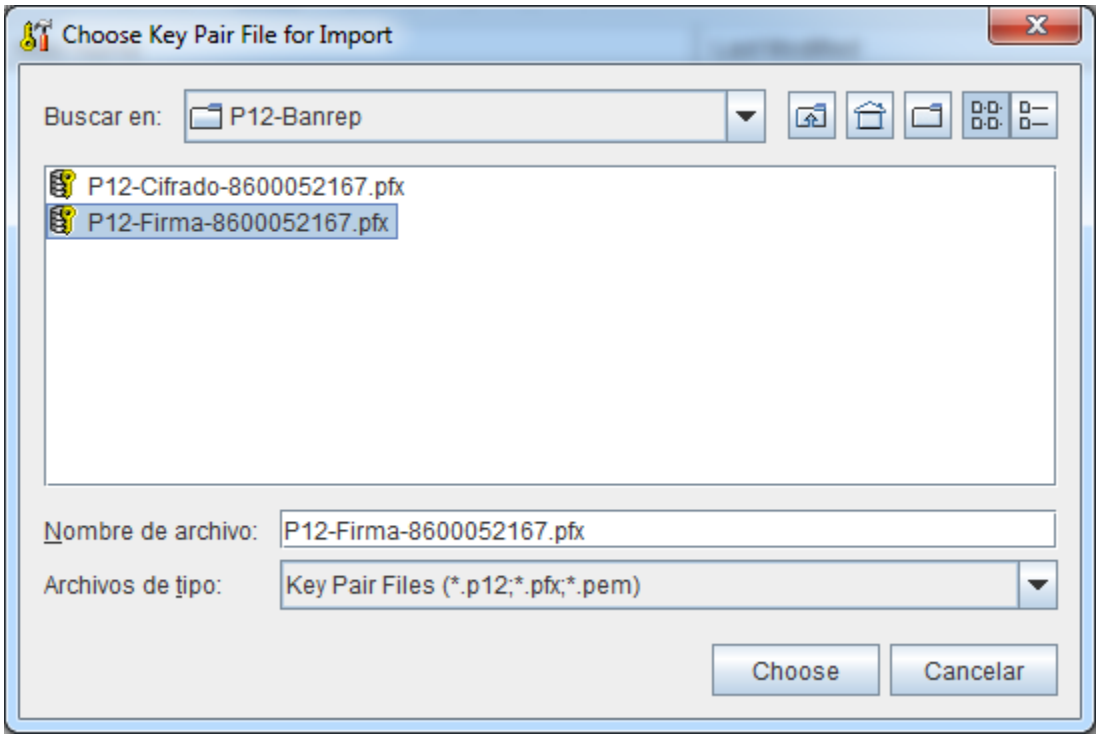


De las alternativas presentadas, se debe escoger el tipo JKS:

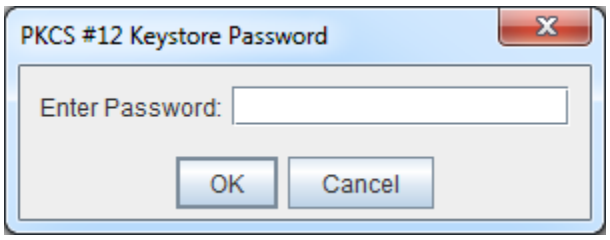


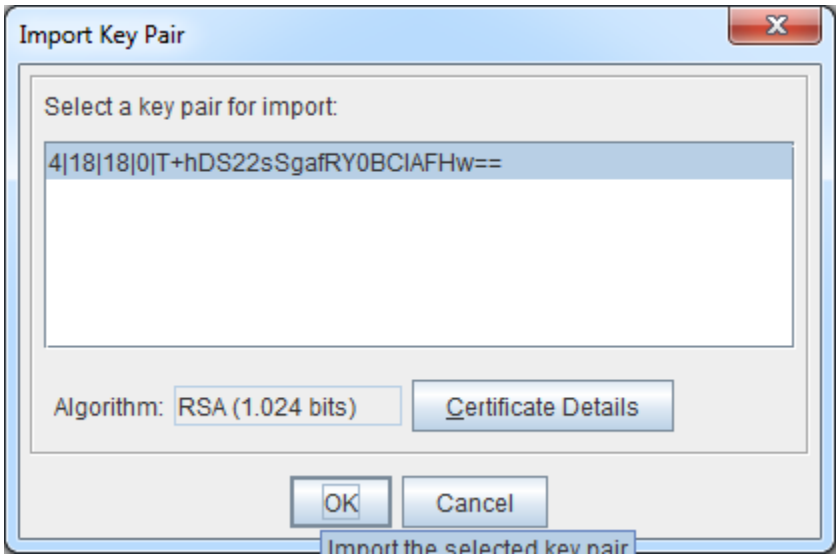


Seleccionar la opción "***Import Key Pair***", en donde debe ubicar el archivo en formato PKCS12 correspondiente al key usage de Firma Digital

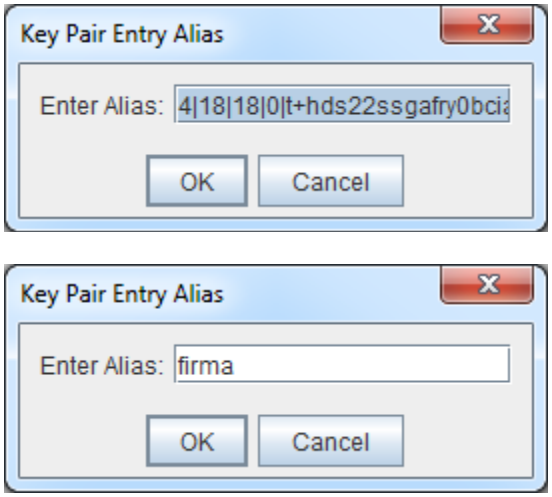


Se debe ingresar la contraseña usada en la conversión a formato PKCS12. Posteriormente, se debe hacer clic en el botón “OK”:

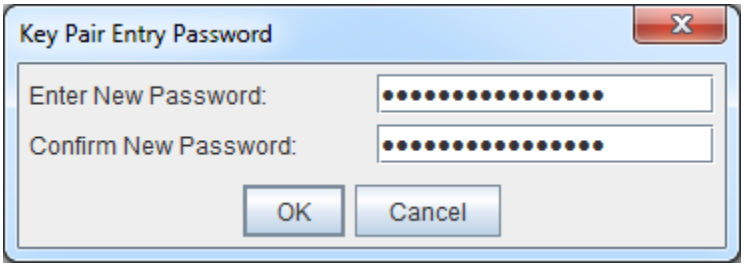


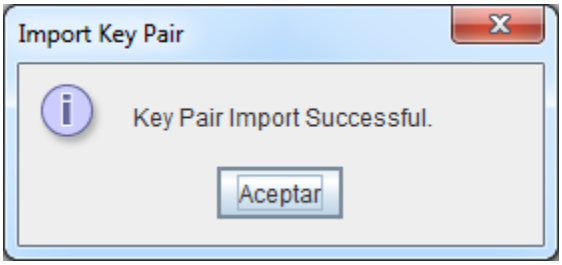


En la Seccion Import Key Pair se podrá modificar el Alias de la llave (en “Certificate Details” esta llave debe tener un Key Usage de Firma Digital). Es de gran ayuda establecer un nombre facil de recordar. En este manual se modifica el alias de la llave a “***firma***” como se muestra a continuacion.

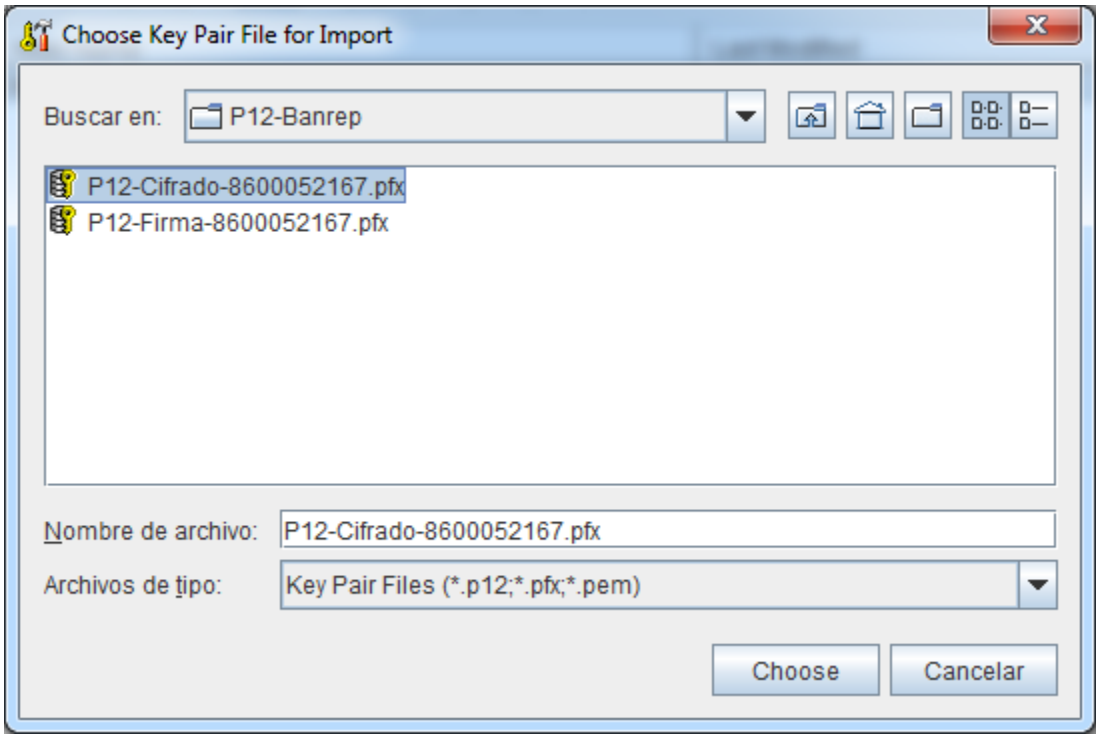


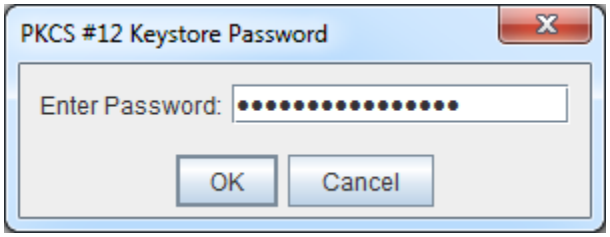
Portecle solicitará una contraseña para este alias.



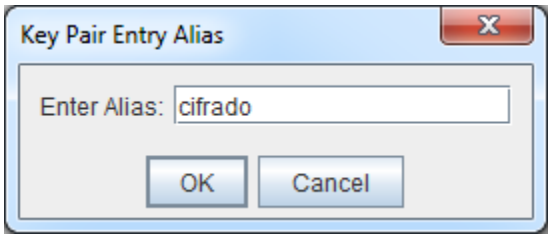


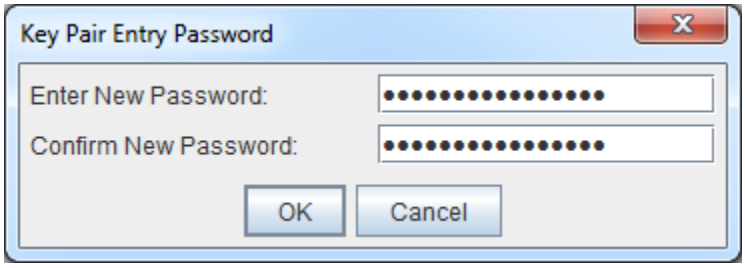
Se realiza el proceso de importación (Import) sobre la credencial PKCS12 correspondiente al *key usage* de cifrado o *Key Encirphement*.

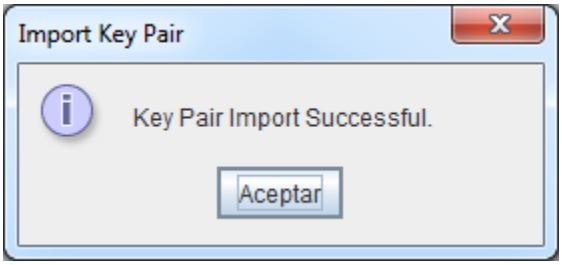




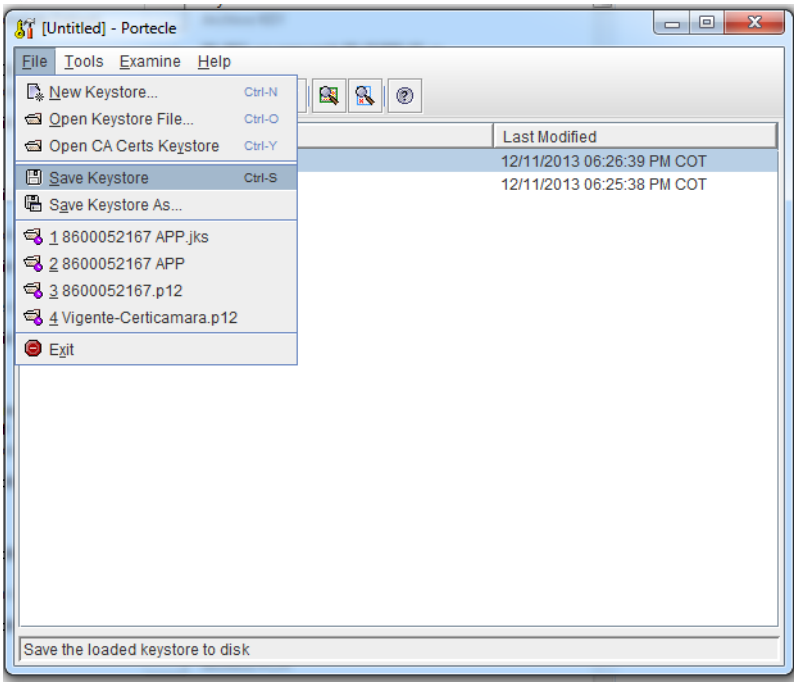
De igual manera se puede establecer un nombre al alias de esta llave, para este caso “cifrado”.

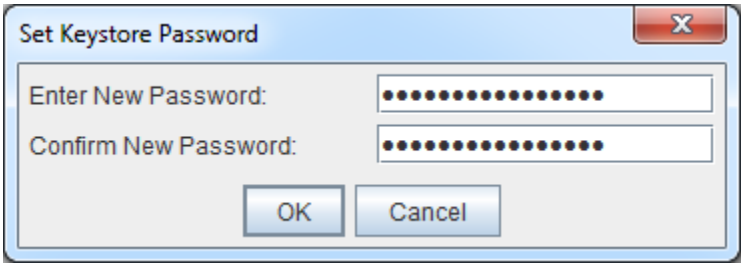


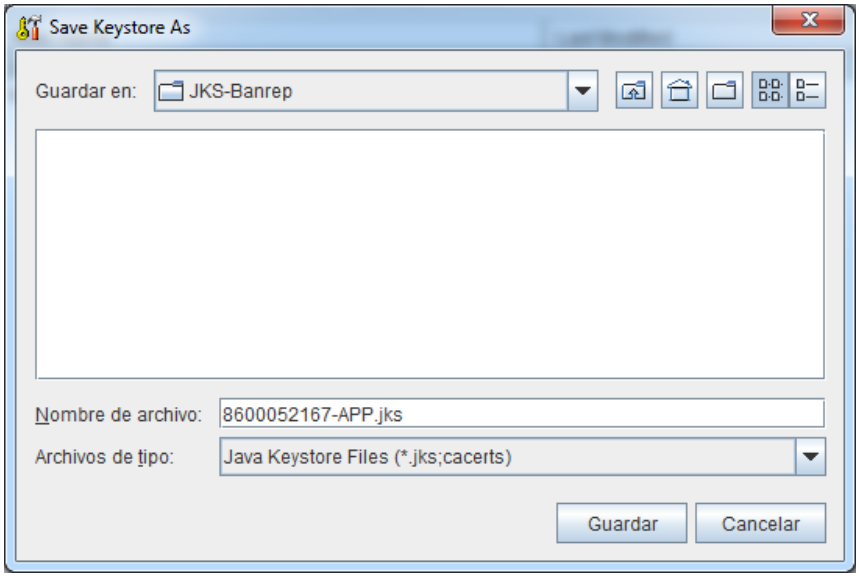




Se procede a guardar el Keystore. Portecle solicita una contraseña para controlar el acceso al contenido del archivo.

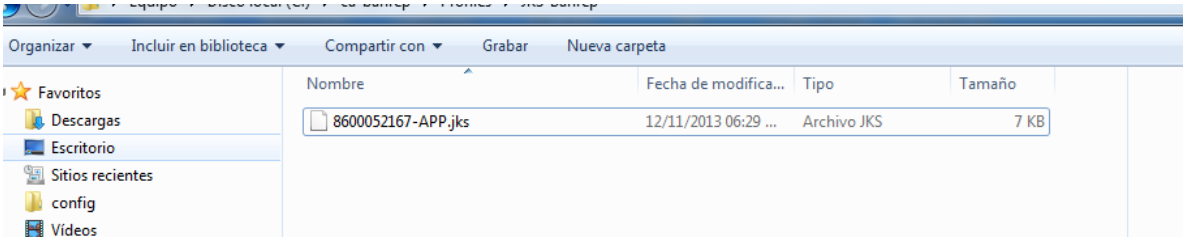

[Untitled] - Portecle
File Tools Examine Help
New Keystore... Ctrl-N
Open Keystore File... Ctrl-O
Open CA Certs Keystore Ctrl-Y
Save Keystore Ctrl-S
Save Keystore As...
1 8600052167 APP.jks
2 8600052167 APP
3 8600052167.p12
4 Vigente-Certicamara.p12
Exit
Last Modified
12/11/2013 06:26:39 PM COT
12/11/2013 06:25:38 PM COT
Save the loaded keystore to disk


Set Keystore Password
Enter New Password:
Confirm New Password:
OK
Cancel


Save Keystore As
Guardar en:
JKS-Banrep
Nombre de archivo:
8600052167-APP.jks
Archivos de tipo:
Java Keystore Files (*.jks;cacerts)
Guardar
Cancelar

En la ruta establecida en el punto anterior queda almacenado el archivo JKS para ser usado por las aplicaciones.

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

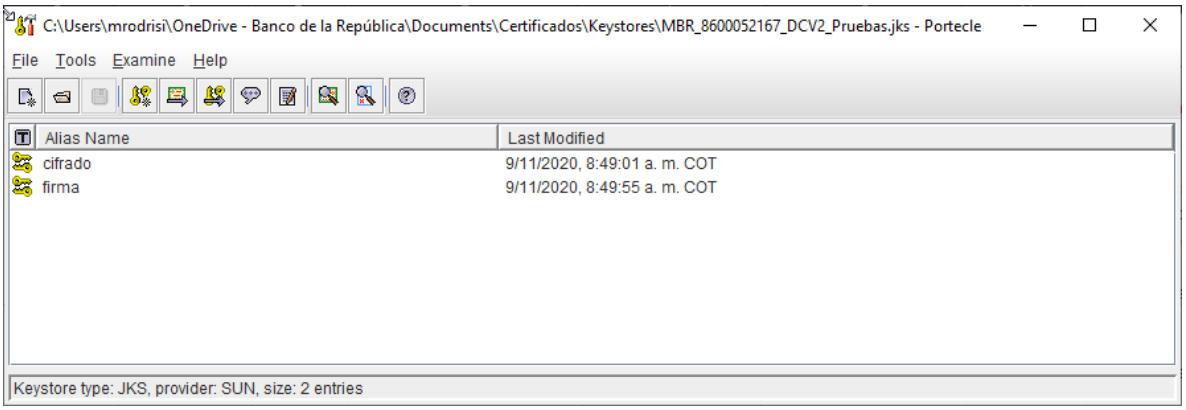


5.1 CONECTIVIDAD CON EL MOM[1]

A continuación presentamos las instrucciones que pueden seguir para exportar dicha llave pública que se requiere para la configuración en el MOM.

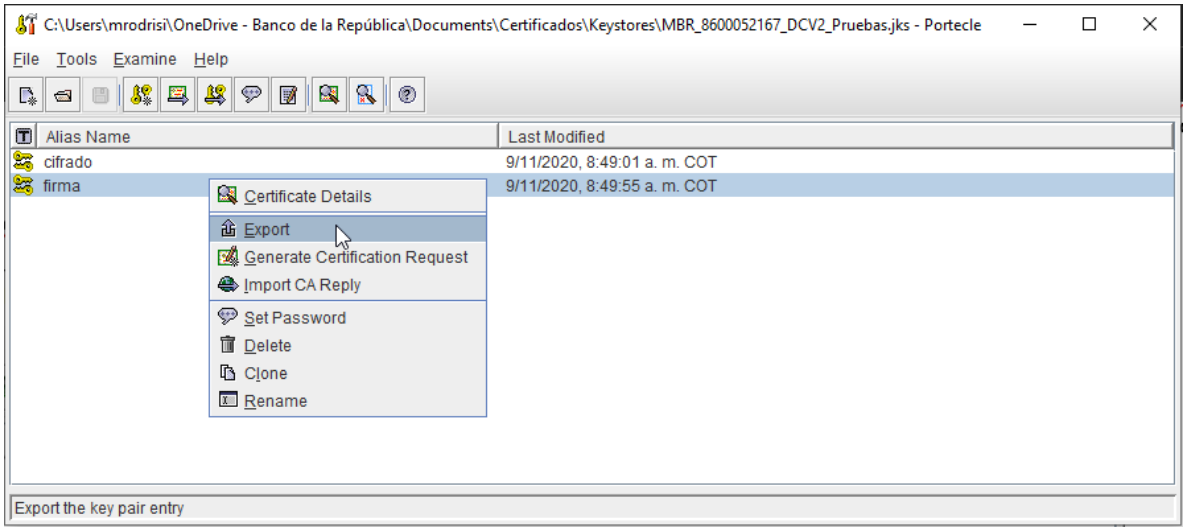
5.1.1 A partir del jks

1. Abrir el llavero (archivo .jks) con portecle. Deben observar algo como la siguiente imagen.

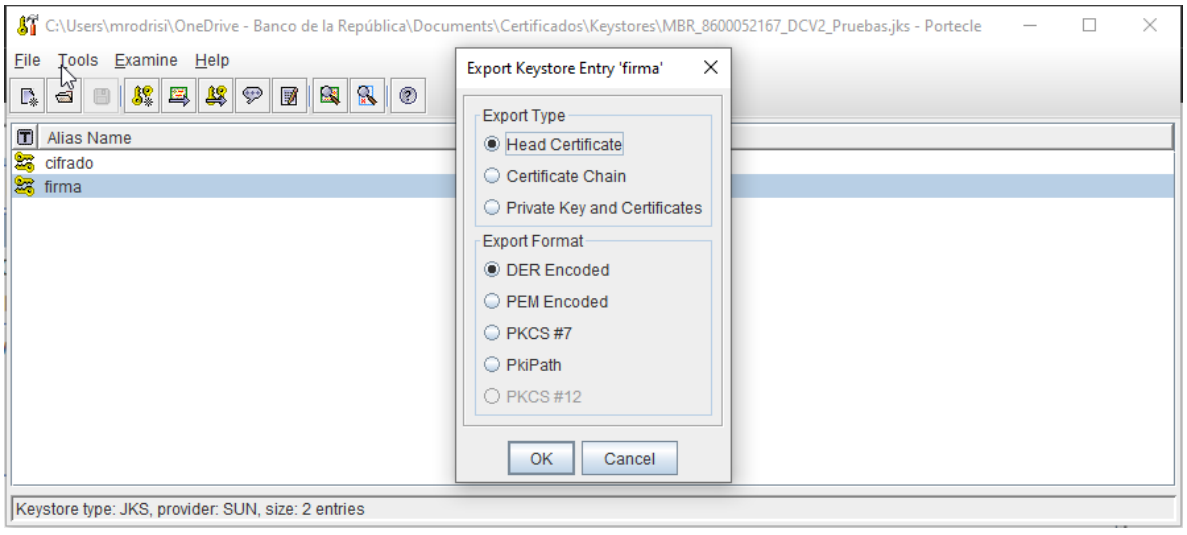


[1] Sistema de Mensajería del Banco de la República. Este sistema se emplea para el envío y recibo de mensajes ISO20022 asociados a sistemas de pago

2. Dar clic derecho sobre el *Alias Name* de “firma” y seleccionar la opción “export”.



3. Exportar el certificado con los valores que vienen por defecto “Head Certificate” y “DER Encoded” y guardarlo dentro de una ruta en el PC.

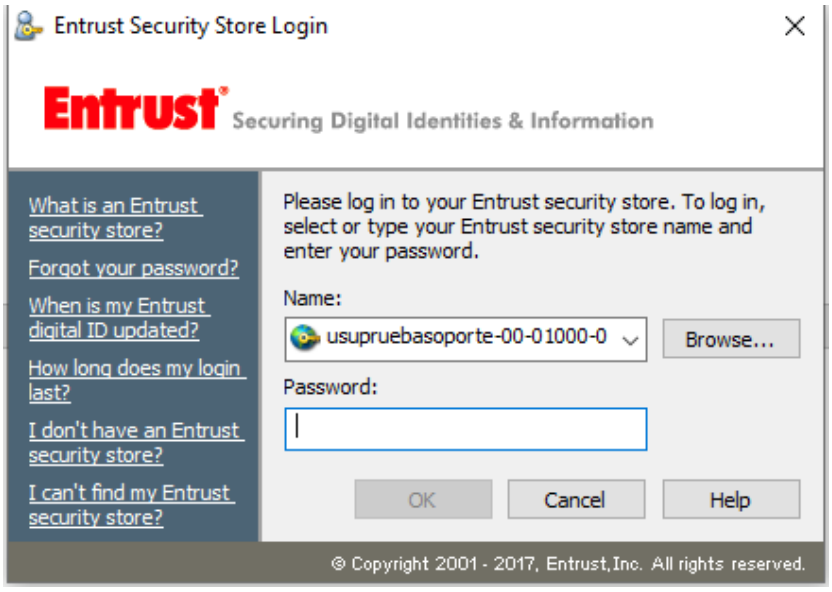


4. Como resultado de este proceso, obtenemos un archivo .cer que contiene la llave pública del certificado de firma de la entidad.

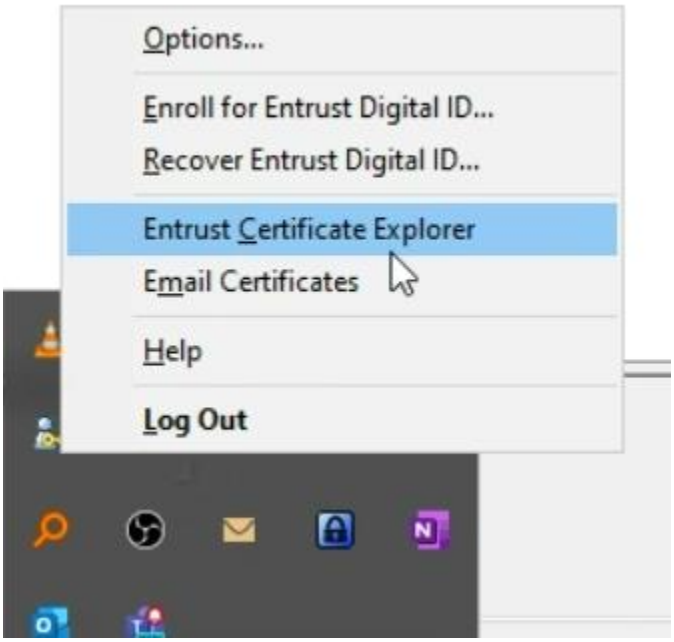
Luego de completar estos pasos, deben enviar el archivo generado (.cer) al correo electrónico soportetecnologico@banrep.gov.co.

5.1.2 Desde el certificado

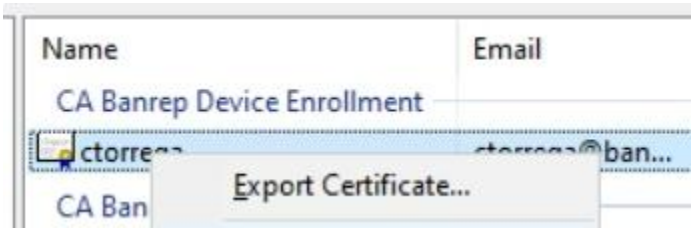
1. Ingresar al entrust login con el usuario asignado



2. Después de ingresar la contraseña del certificado. Dar clic derecho sobre el icono de Entrust y seleccionar Entrust Certificate Explorer

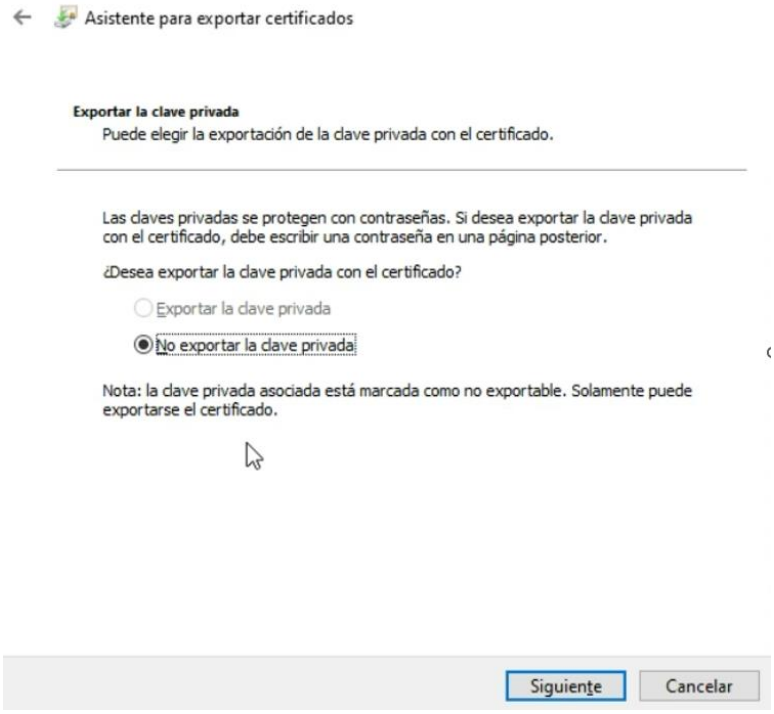


3. Seleccionar el certificado

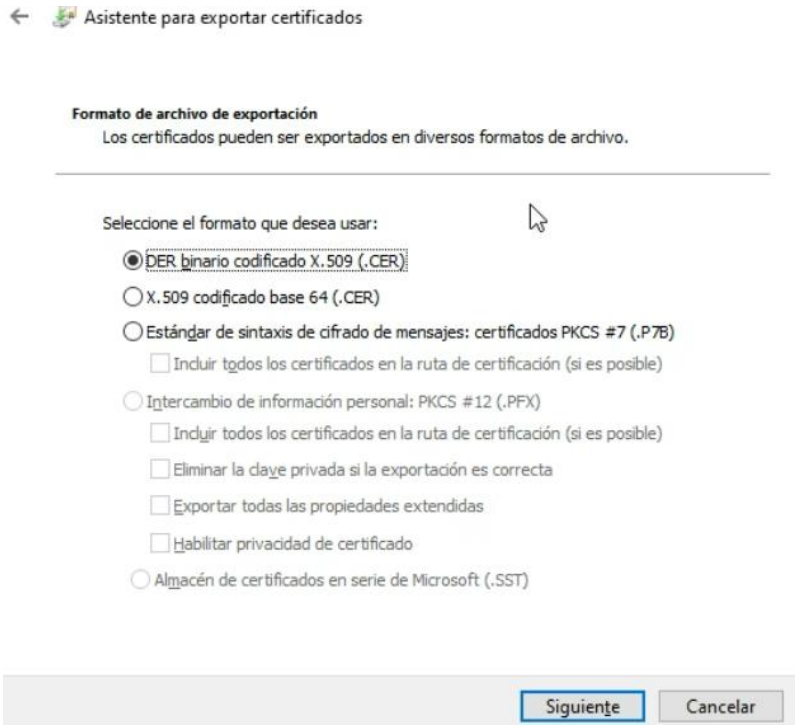


4. Seleccionar el certificado e iniciará el proceso de exportación

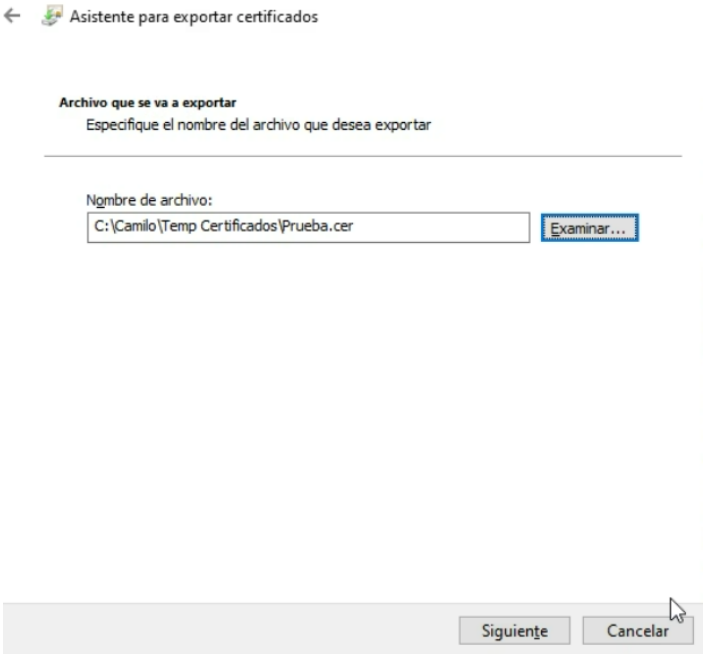
5. Dar clic en Siguiente



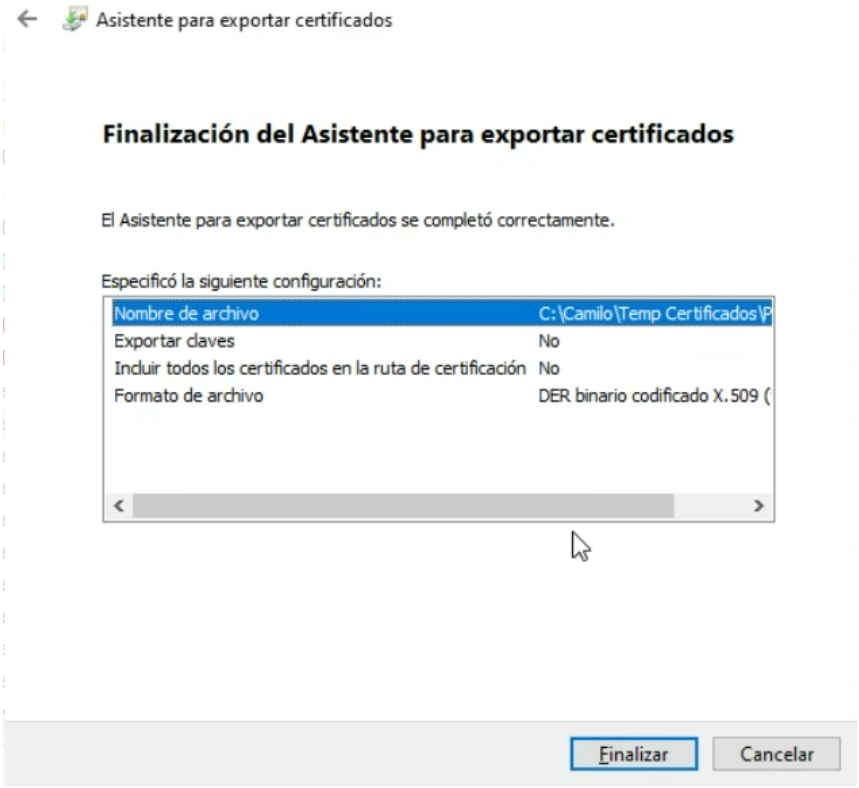
6. Seleccionar **No exportar la clave privada** y dar clic en Siguiente



7. Seleccionar **No exportar la clave privada** y dar clic en Siguiente



8. Indicar la ruta de donde va a dejar el archivo con extensión **.cer** y dar clic en Siguiente



9. Dar clic en Finalizar. Como resultado de este proceso, obtenemos un archivo .cer que contiene la llave pública del certificado de firma de la entidad.

Luego de completar estos pasos, deben enviar el archivo generado (.cer) al correo electrónico soportetecnologico@banrep.gov.co.