Banco de la República
Bogotá D. C., Colombia

Subgerencia de Informática
Unidad de Seguridad Informática

MANUAL DEL USUARIO PKI

USI-PN--18

04 de Julio de 2003

Versión #1.0

CONTENIDO

Pág.

CONTENIDO **3**

1 INTRODUCCIÓN **4**

1.1 OBJETO 4
1.2 ALCANCE 4
1.3 AUDIENCIA 4

2. ABRIR CONEXIÓN CON LA INFRAESTRUCTURA DE LLAVES PÚBLICAS DE LA CA-BANREP **5**

2.1 TRABAJANDO ON-LINE 5
2.2 TRABAJANDO FUERA DE LÍNEA (WORK OFFLINE) 6

3. REGISTRO DE USUARIOS EN LA LIBRETA DE DIRECCIONES **9**

3.1 REGISTRO EN LÍNEA 9
3.2 CREACIÓN DE LISTAS DE CERTIFICADOS 12
3.4 IMPORTAR UNA LISTA COMPARTIDA - REGISTRO FUERA DE LÍNEA 17

4. USO CON ARCHIVOS **19**

4.1 ENCRIPTAR UN ARCHIVO 19
4.2 DESENCRIPTAR UN ARCHIVO 22
4.3 FIRMAR DIGITALMENTE UN ARCHIVO 23
4.4 VERIFICAR LA FIRMA DIGITAL DE UN ARCHIVO 25

5 CERRAR LA CONEXIÓN CON LA INFRAESTRUCTURA DE LLAVES PÚBLICAS DE LA CA-BANREP **28**

6 GLOSARIO **29**

ANEXO 1 ..... **30**

ANEXO 2 ..... **32**

ANEXO 3 ..... **36**

1 INTRODUCCIÓN

1.1 OBJETO

Este documento explica el uso del cliente PKI para la CA BANREP, el software Entrust Entelligence.

1.2 ALCANCE

Explicar detalladamente el uso de la herramienta cliente PKI, para firmar digitalmente y encriptar archivos, con su respectiva desencripción y verificación de firma.

1.3 AUDIENCIA

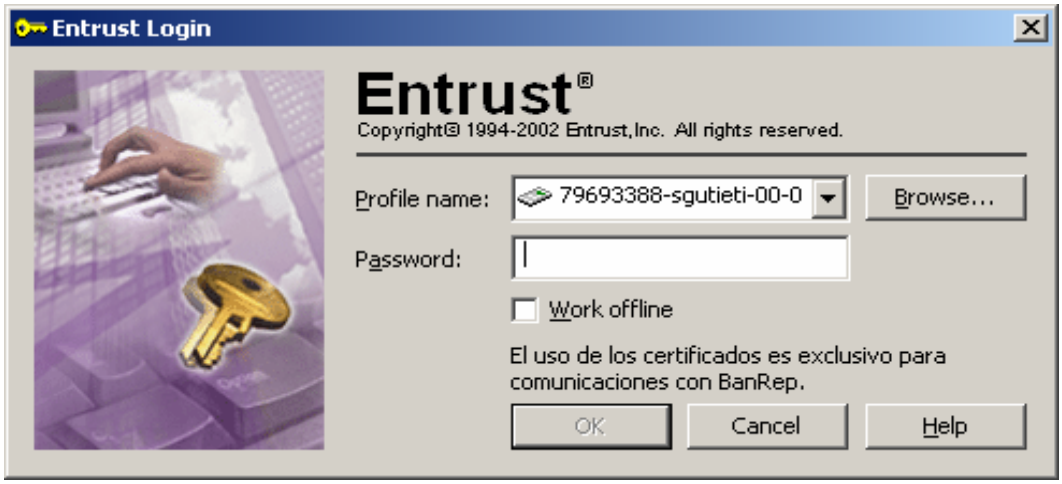
Este documento está dirigido a todos los suscriptores de la CA BANREP.

2. ABRIR CONEXIÓN CON LA INFRAESTRUCTURA DE LLAVES PÚBLICAS DE LA CA-BANREP

2.1 TRABAJANDO ON-LINE

Para poder comunicarse electrónicamente, encriptando y firmando digitalmente con los certificados expedidos por la entidad de certificación CA Banrep del Banco de la República, debe realizar la siguiente conexión:

Dar clic en la llave amarilla, que se encuentra en la parte inferior derecha de la pantalla (con una X de color rojo en la parte superior), previa instalación del software. (Ver manual de instalación) En esta pantalla, dar clic en Log In to Entrust.



El software cliente PKI automáticamente detecta el token que está conectado a la máquina. Ahora debe incluir el password o contraseña. Después de escribirlo, dé un clic en OK.

Si la contraseña ha sido cuidadosamente digitada, el sistema le mostrará en Status una llave amarilla, seguido de "Connected to Entrust", como se muestra en la pantalla siguiente:

Lo anterior, significa que usted ya tiene abierta la conexión y pueda realizar intercambio de información segura con el Banco de la República. El software cliente verifica la validez de sus certificados que están almacenados en el token, descarga la última versión de la lista de certificados revocados CRL y otra información como el certificado de políticas de usuario establecido para Ud. a la máquina (directorio c:\ca-banrep\profiles)

2.2 TRABAJANDO FUERA DE LÍNEA (WORK OFFLINE)

Si no posee conexión directa hacia el Banco de la República (no es estación SEBRA, posee problemas con la comunicación, es un usuario Internet, etc.) y requiere intercambiar información de forma segura con el Banco de la República,

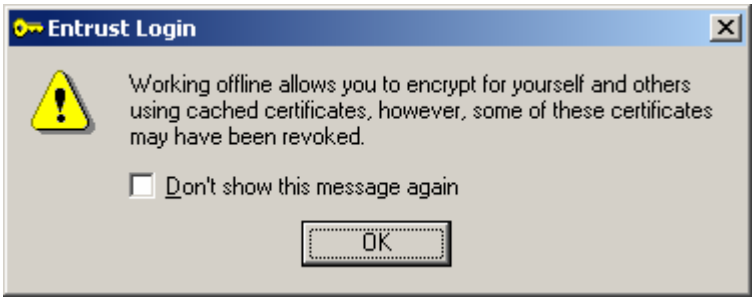
se puede trabajar en modo fuera de línea lo cual significa que usted trabajará con la información que tiene almacenada en su token y su máquina.

Haga clic derecho sobre la llave amarilla que le aparece en la parte inferior derecha de sus pantalla y elija la opción "Log In to Entrust"

Le aparecerá una pantalla como la siguiente:

Digite su password o contraseña y marque la opción "Work Offline"

Dé clic en "OK" y el sistema le mostrará el siguiente mensaje de precaución, en donde se hace explicito el uso de la información local y no en línea de los servidores de la CA Banrep.



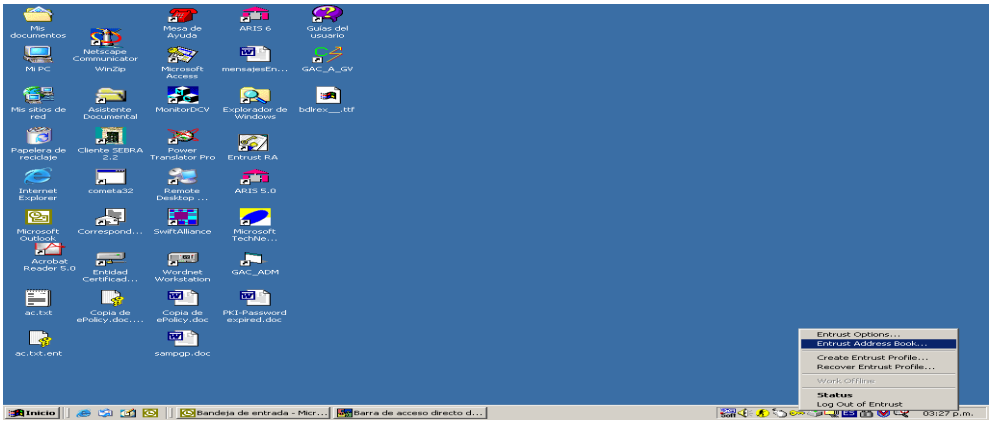
Se pueden realizar todas las operaciones normalmente, Ud. puede tener su lista personal de certificados de los usuarios con los que realiza sus operaciones y no tendrá ningún inconveniente para intercambiar información. El único problema que se puede presentar es el que los certificados que tienen almacenados en la máquina, hayan sido revocados, es aconsejable tener actualizada con cierta frecuencia la lista de los certificados.

3. REGISTRO DE USUARIOS EN LA LIBRETA DE DIRECCIONES

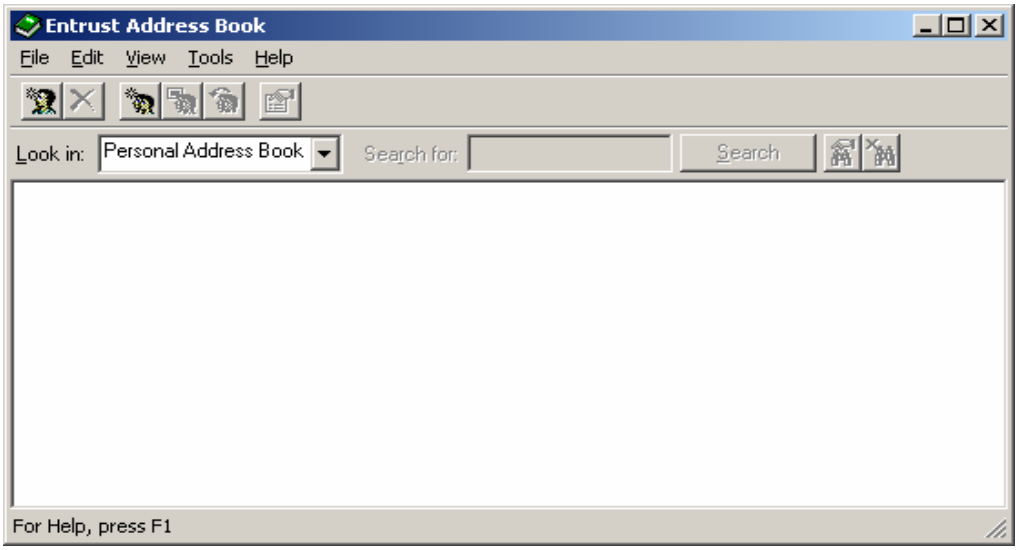
3.1 REGISTRO EN LÍNEA

Antes de encriptar y firmar archivos o mensajes, debe incluir el usuario destinatario en la libreta de direcciones, de la siguiente manera:

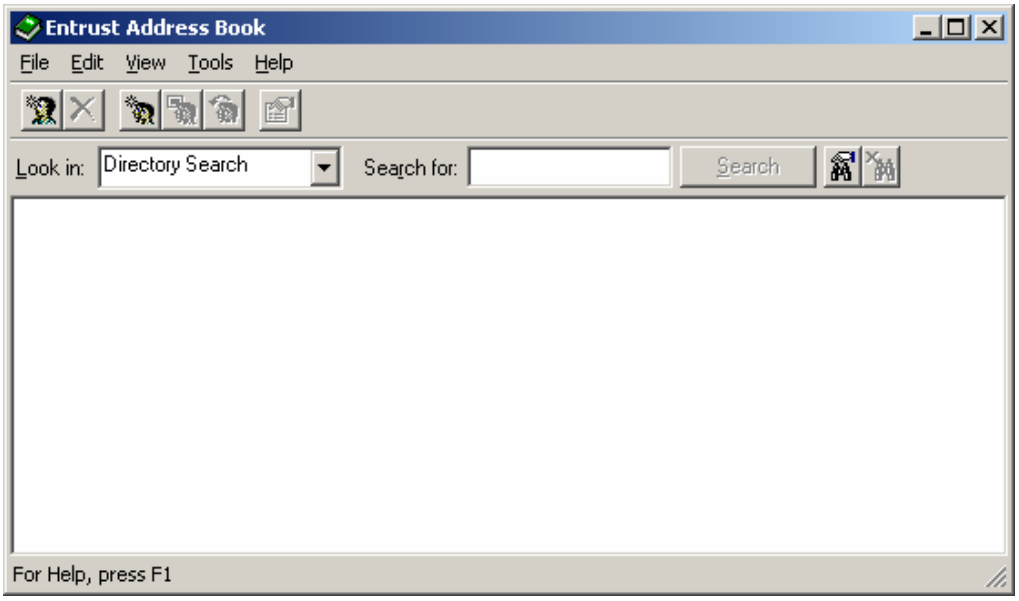
Después de haber hecho conexión con el sistema, dé clic derecho sobre la llave amarilla, localizada en la parte inferior derecha de su pantalla.



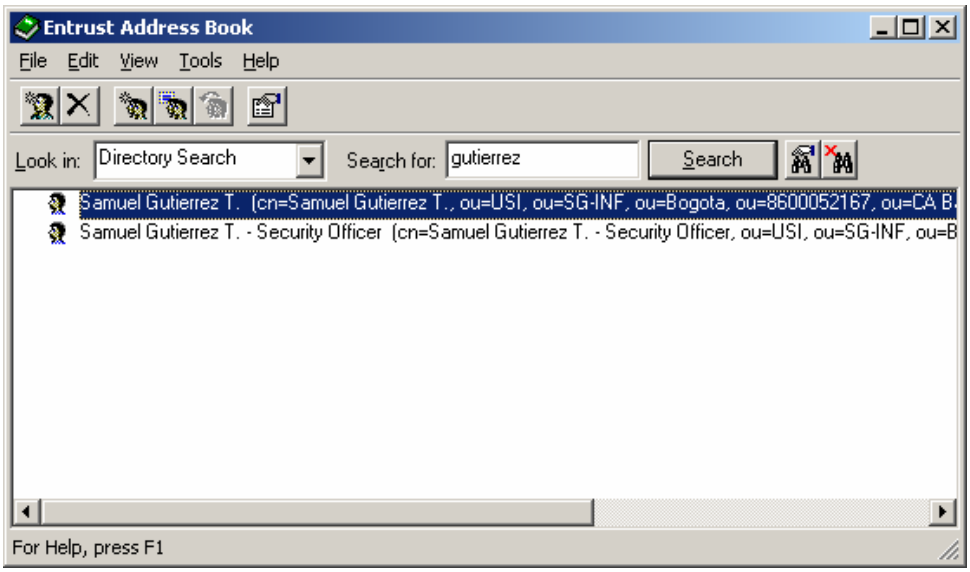
En la pantalla que se muestra a continuación, encontrará la libreta personal de direcciones, que al desplegarla, encontrará el directorio para realizar la búsqueda.



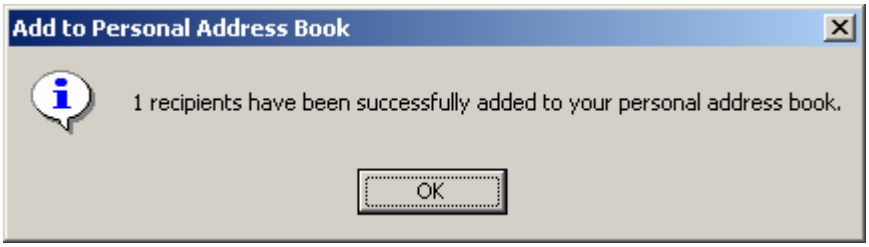
Marque la opción de búsqueda en el directorio y en el espacio siguiente escriba el apellido del usuario que desea incluir en la libreta de direcciones. Para esto, dé clic en Search.

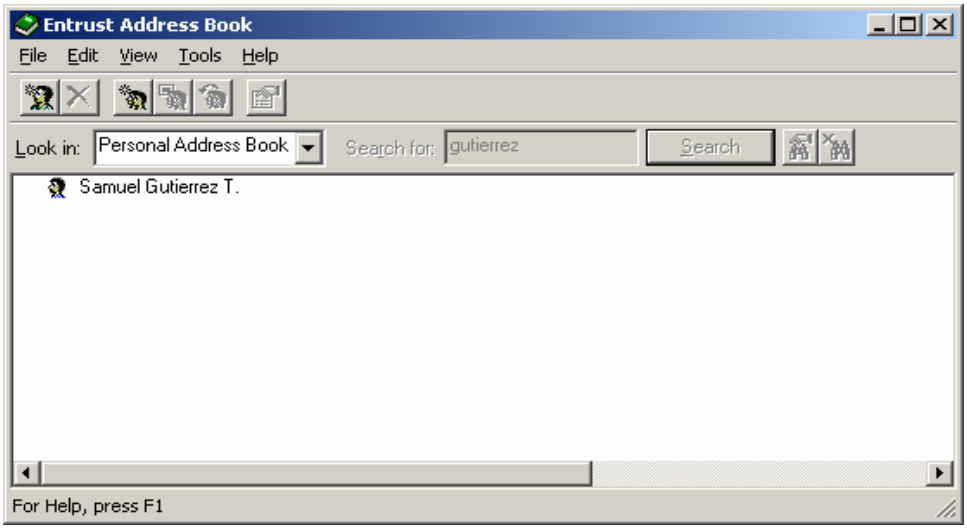


En seguida, le mostrará el resultado de la búsqueda. Por lo tanto, ya puede enviar mensajes seguros al usuario propietario de la llave.



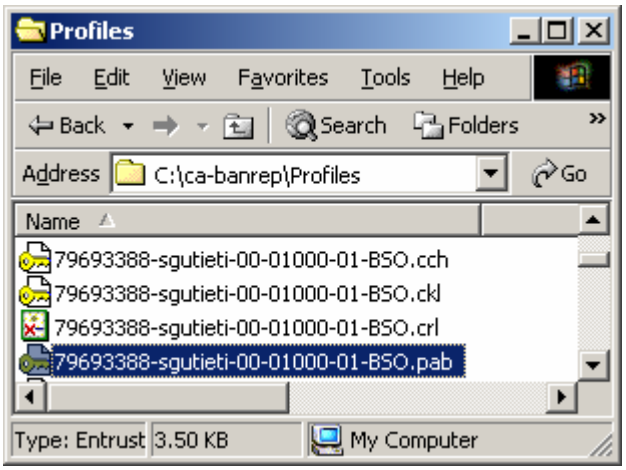
Haga clic derecho y elija "Add to Personal Address Book" y le mostrará una ventana como la siguiente:





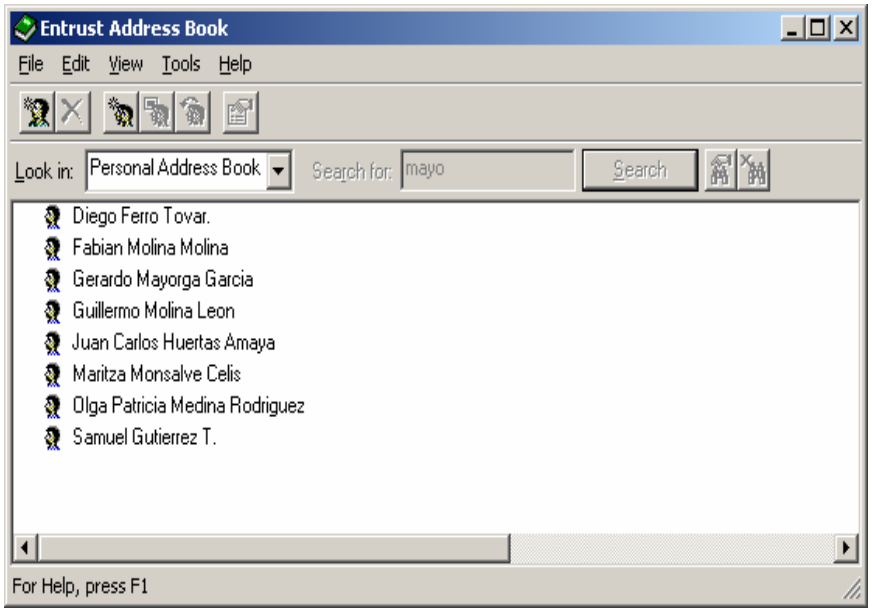
La anterior acción le creará un archivo en el disco de su máquina, en el directorio C:\ca-banrep\profiles\ llamado igual que su Profile y con extensión .pab, en caso

de que requiera moverse de máquina será necesario pasar este archivo (en la misma ruta en la máquina destino) si requiere hacer uso de estos certificados allí almacenados.

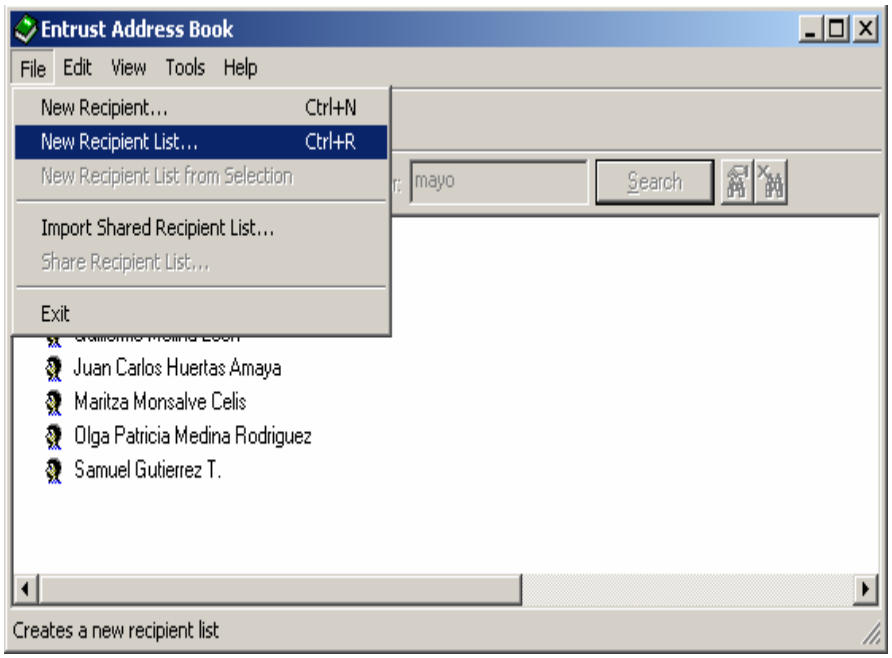


3.2 CREACIÓN DE LISTAS DE CERTIFICADOS

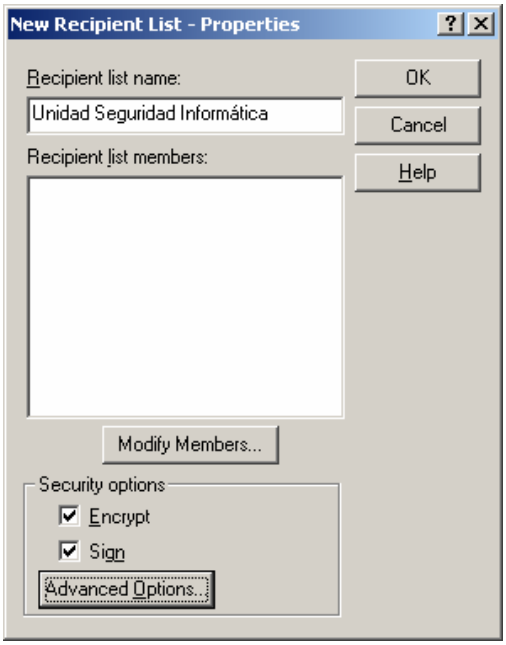
Una vez ya se tenga en su lista de certificados los que regularmente necesita para su intercambio de información se pueden crear listas. Estando en la ventana de "Entrust Address Book"



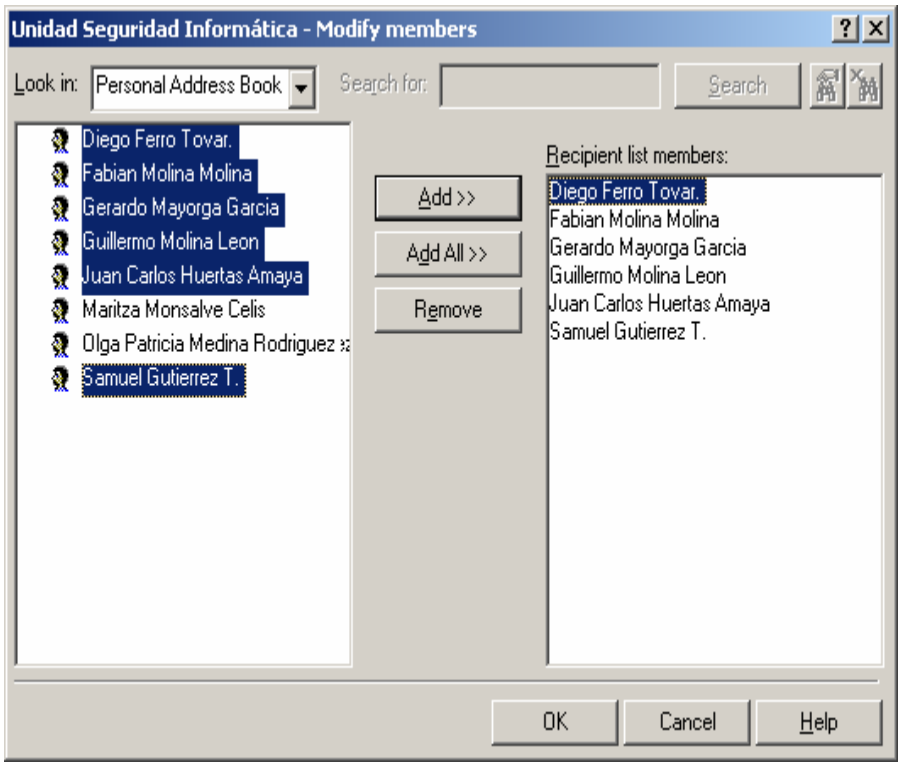
Elija la opción crear una lista, file→ New Recipient List



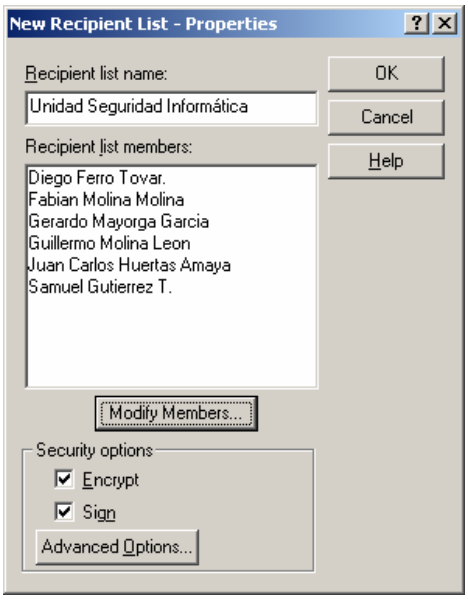
Le aparecerá una ventana como la siguiente en donde se da el nombre de la lista



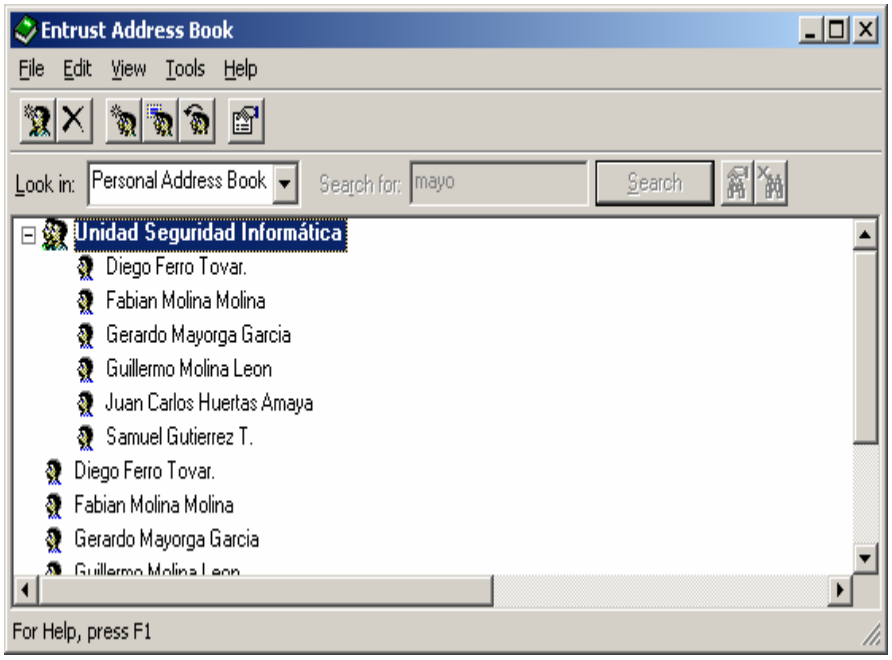
Al hacer clic en “Modif. Members…”, se despliega una ventana como la siguiente, en donde se puede seleccionar usuarios de los que se tienen en el personal address book o del directorio.



Haga clic en OK. y le aparecerán los miembros de la lista seleccionados



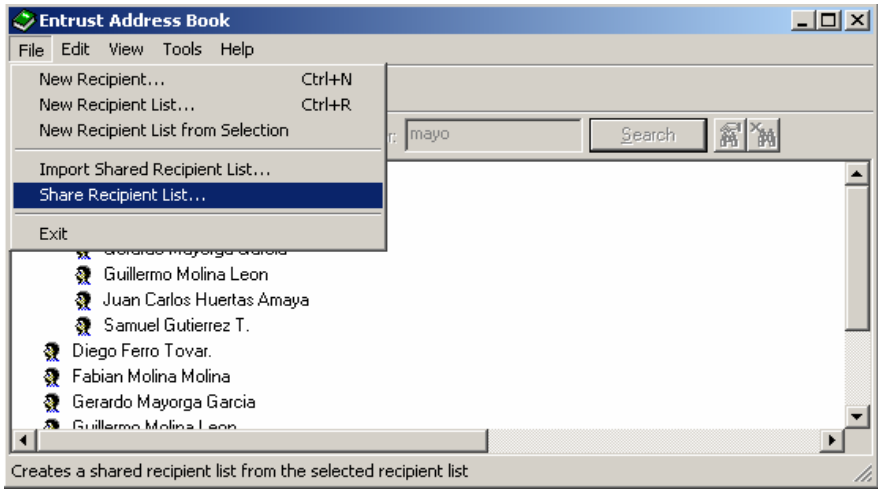
Haga clic en OK y le aparecerá una ventana como la siguiente, en donde le muestra la lista ya creada.



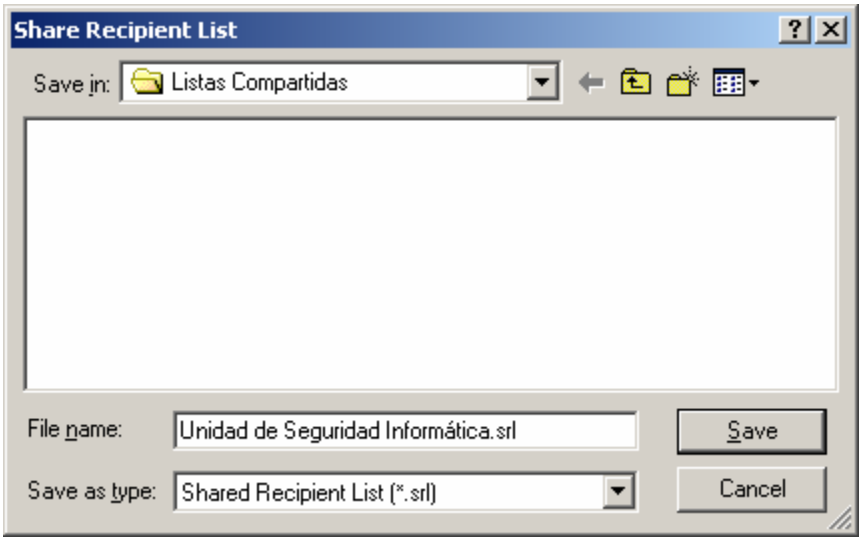
3.3 COMPARTIR (EXPORTAR) UNA LISTA DE CERTIFICADOS

Una vez creada la lista Ud. puede compartirla con otros, esto es bastante útil cuando siempre tenemos que asegurar la información a un grupo fijo de usuarios, se minimiza el riesgo que alguno de los usuarios sea olvidado.

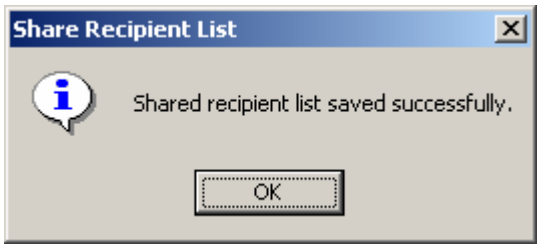
Para compartir la lista haga clic sobre la lista que tiene en su personal address book y elija la opción file → "Share Recipient List…".



Le aparecerá una ventana como la siguiente, en donde será posible ubicar el directorio en donde quedará y asignar el nombre que desee, esta operación crea un archivo con extensión .srl.



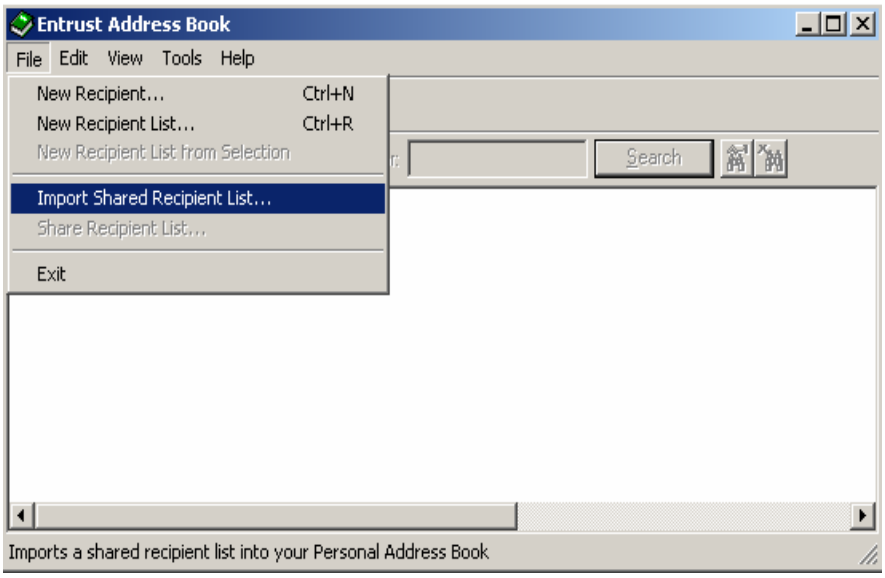
Si la lista se pudo compartir (exportar) de forma exitosa, presentará una ventana como la siguiente:



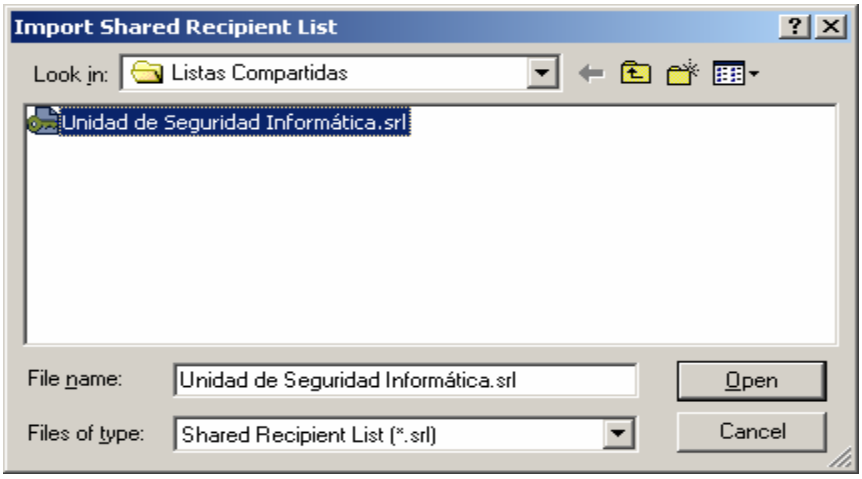
Ese archivo creado puede ser intercambiado con otros usuarios de diferentes formas v.g. Archivo Adjunto a un correo, Disquete, Bajarlo por Internet, etc.

3.4 IMPORTAR UNA LISTA COMPARTIDA - REGISTRO FUERA DE LÍNEA

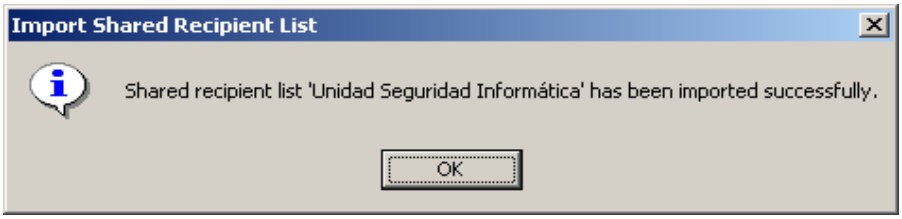
Para importar una lista compartida a su personal address book, se necesita el archivo .srl que quiere importar y abrir su aplicación Entrust Address Book, una vez abierta esta aplicación, elija la opción de importar una lista compartida, file→Import Shared Recipient List. Al hacer clic sobre esta opción le presentará una ventana como la siguiente:



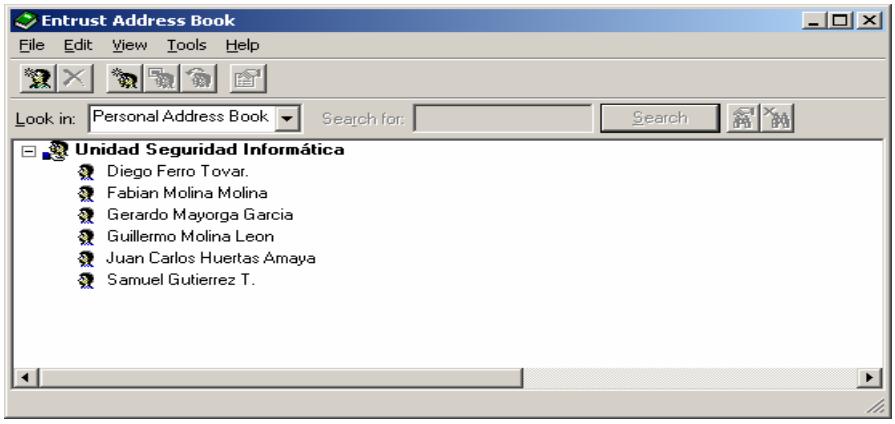
Esta acción le mostrará la siguiente ventana en donde Ud. puede ubicar el archivo que quiere importar, elija el archivo y haga clic en Open.



La aplicación le presentará la confirmación de la operación efectuada:



Ahora Usted puede encriptar información a la lista o a algunos de sus miembros según lo disponga.

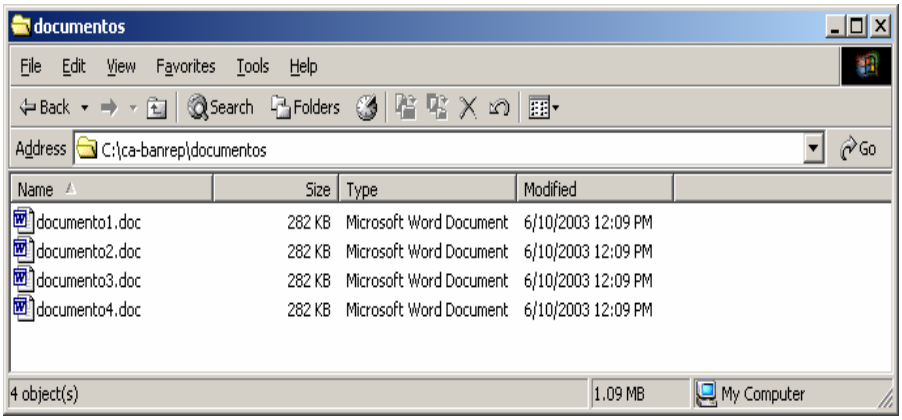


Este mecanismo es el que se debe usar cuando no se tiene conexión con el Banco de la República y no aún no tiene los certificados de las personas con las que se comunica.

4. USO CON ARCHIVOS

4.1 ENCRIPTAR UN ARCHIVO

Entre al explorador



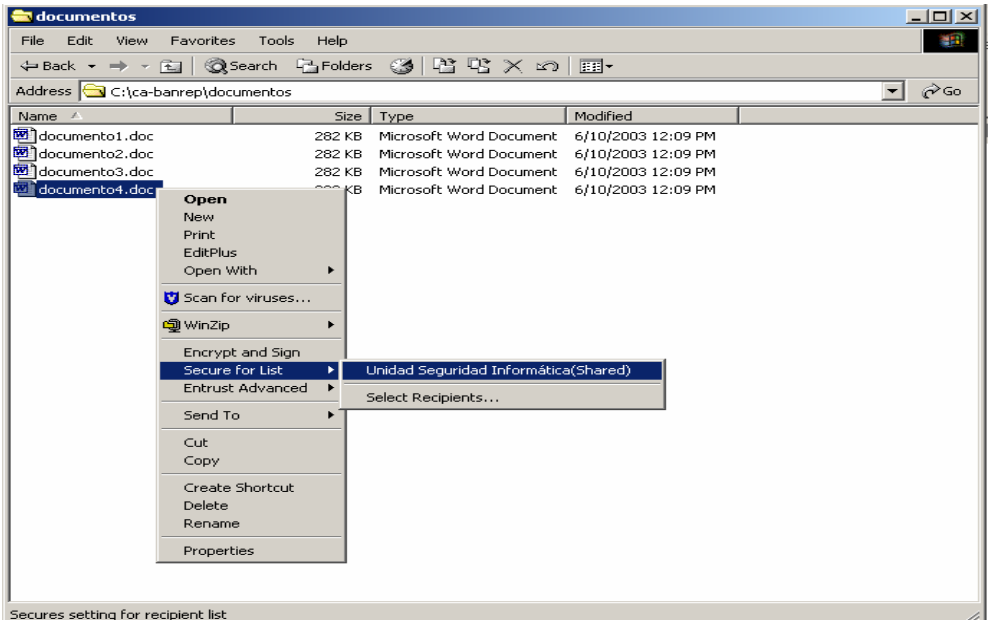
Localice el archivo que desea encriptar. Dé clic derecho sobre este y encontrará tres nuevas opciones en el menú que se despliega, como se muestra en la siguiente gráfica.

Las opciones son:

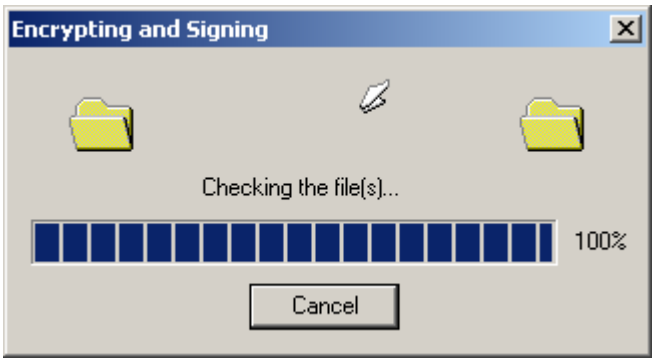
- Encrypt and Sign: Esta opción firma y encripta el archivo para el usuario que esta conectado al Profile.

- Secure for List: Encripta y/o firma digitalmente un archivo para una lista o recipientes elegidos ya sea del personal Address Book ó del directorio directamente.

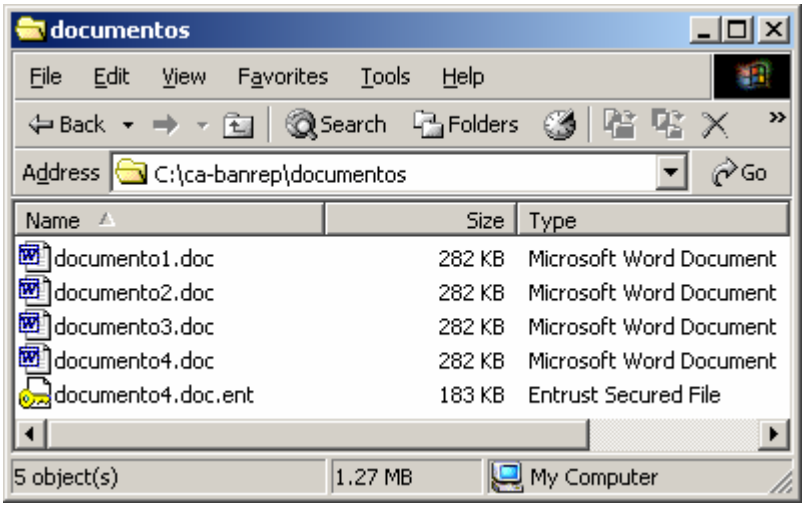
- Entrust Advanced: Esta opción firma y encripta el archivo para el usuario que esta conectado al Profile y le brinda la opción de ir a otras aplicaciones Entrust.



De esta manera para todos los usuarios que se encuentren en la lista será encriptado el archivo.



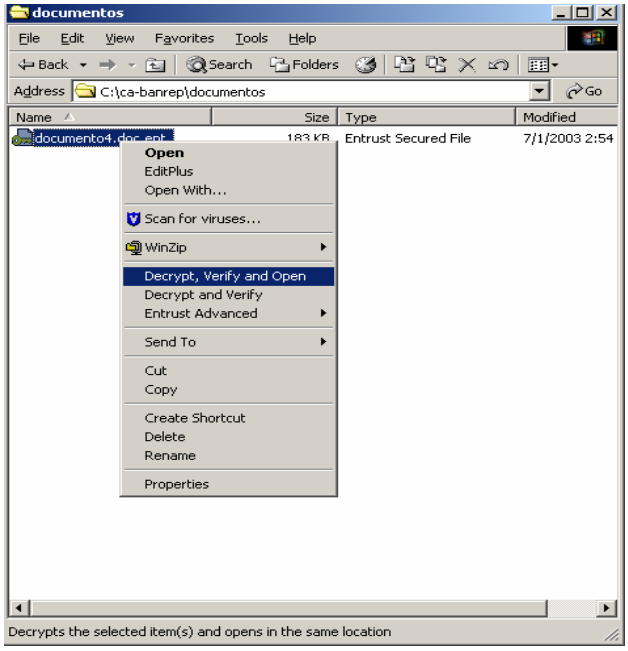
Mientras se realiza la operación de encripción se muestra la anterior ventana, al final le aparecerá un nuevo archivo con extensión .ent. Por defecto el archivo de firma digitalmente y encripta al mismo tiempo.



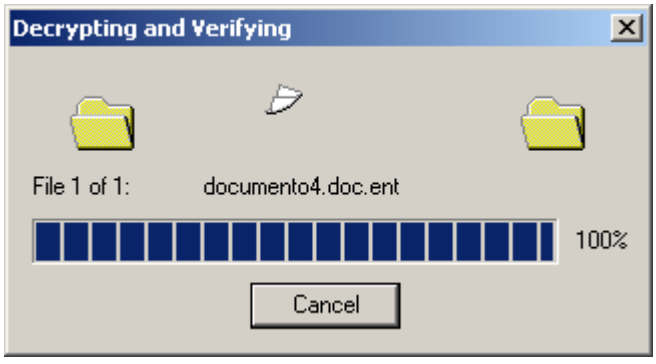
El archivo original permanece en el directorio si se mantiene la configuración estipulada en el anexo 3.

4.2 DESENCRIPTAR UN ARCHIVO

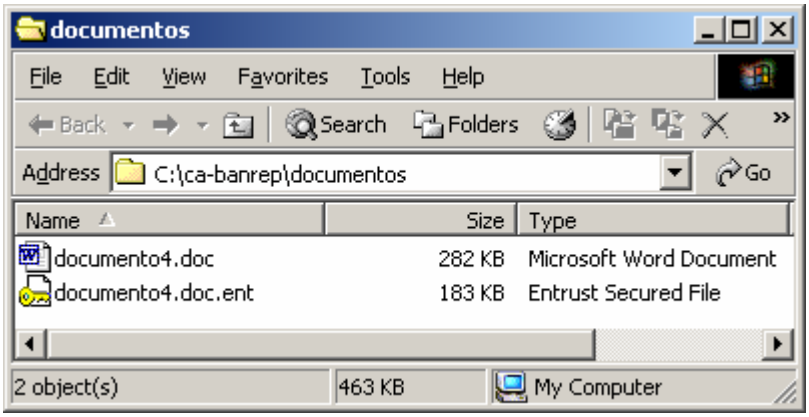
Para conocer el contenido de un archivo que se encuentra encriptado, localícelo por el explorador y dé clic derecho sobre este y encontrará la opción Decrypt, Verify and Open. El archivo desencriptado quedará ubicado en el mismo directorio.



El sistema le mostrará una pantalla en la que sale el proceso de desencripción, y enseguida le muestra el archivo desencriptado.

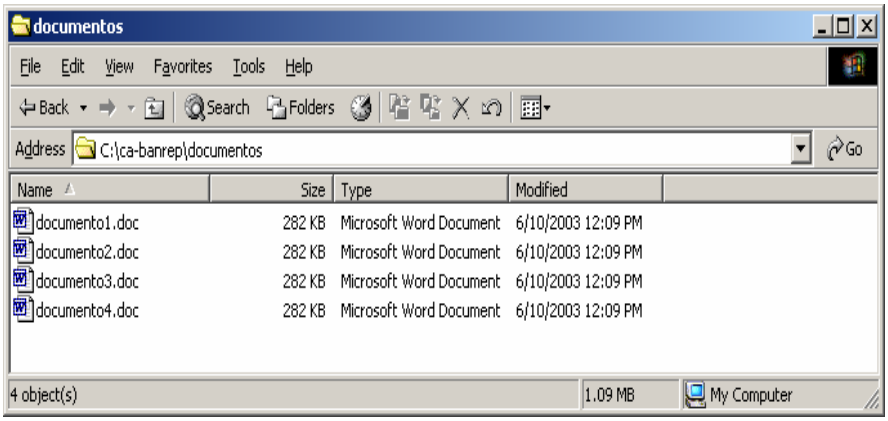


El programa de desencripción le deja el archivo en el mismo directorio en el que se encuentra el archivo seguro.

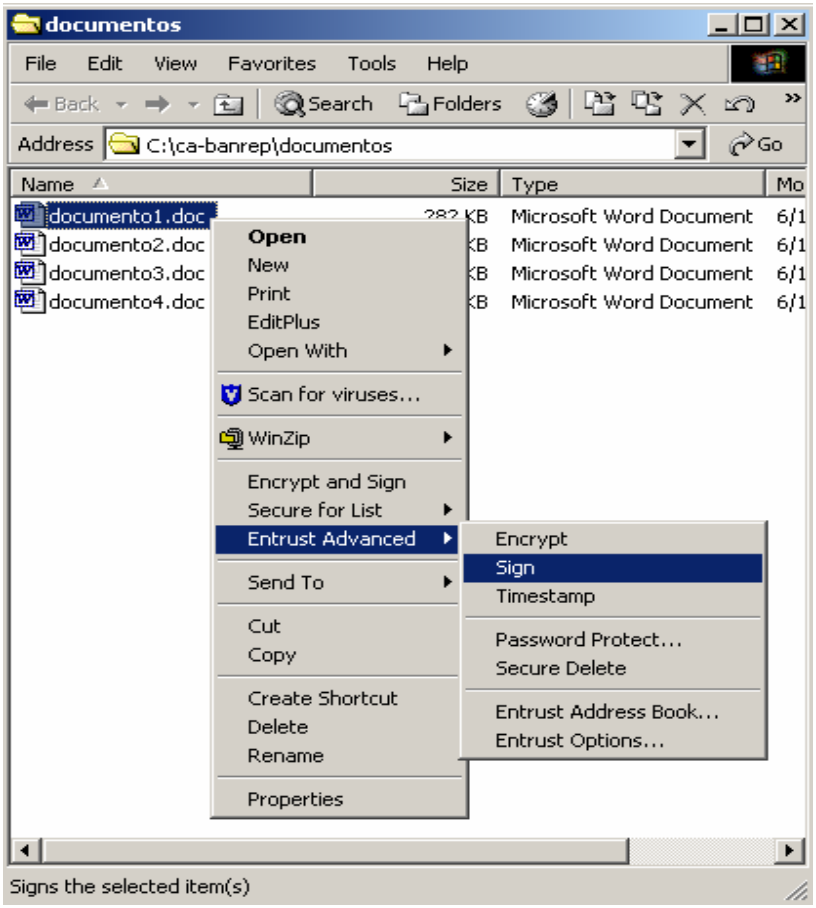


4.3 FIRMAR DIGITALMENTE UN ARCHIVO

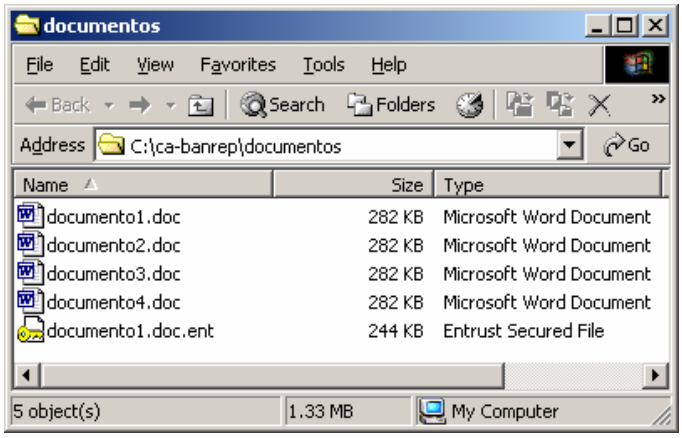
Entre al explorador



Localice el archivo que desea firmar. Dé clic derecho sobre este y encontrará la opción de Entrust Advanced. Dé clic sobre esta opción y encontrará la opción de firmar. Dé clic sobre esta opción y el archivo quedará firmado.

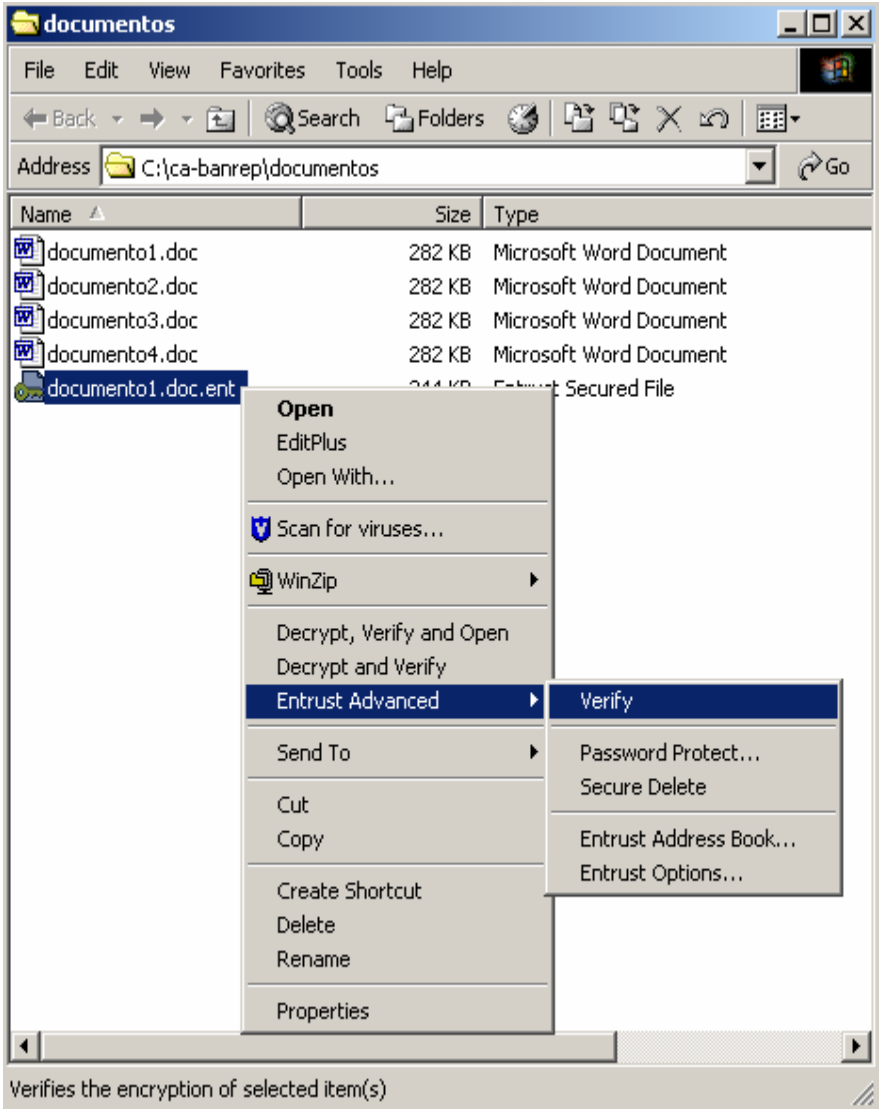


El archivo original permanece. El archivo encriptado y firmado lo antecede una llave de color amarillo y quedará con extensión .ent

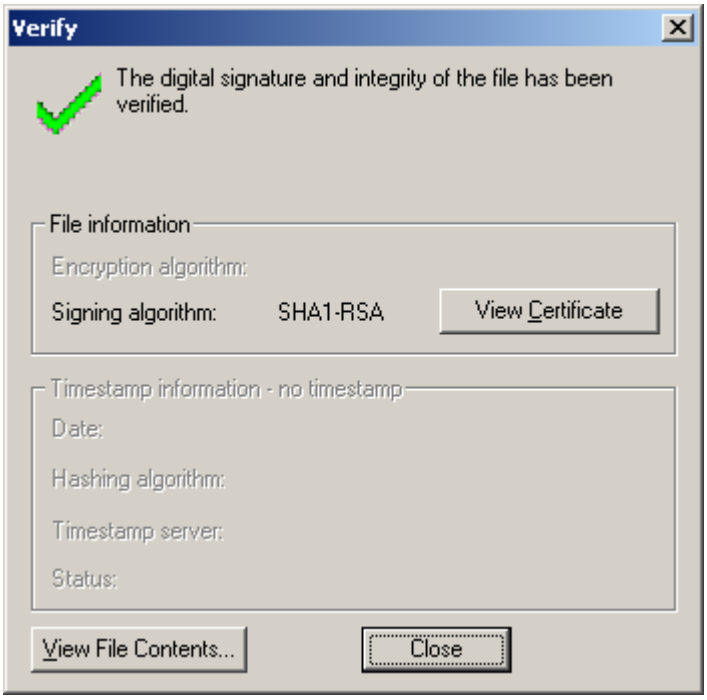


4.4 VERIFICAR LA FIRMA DIGITAL DE UN ARCHIVO

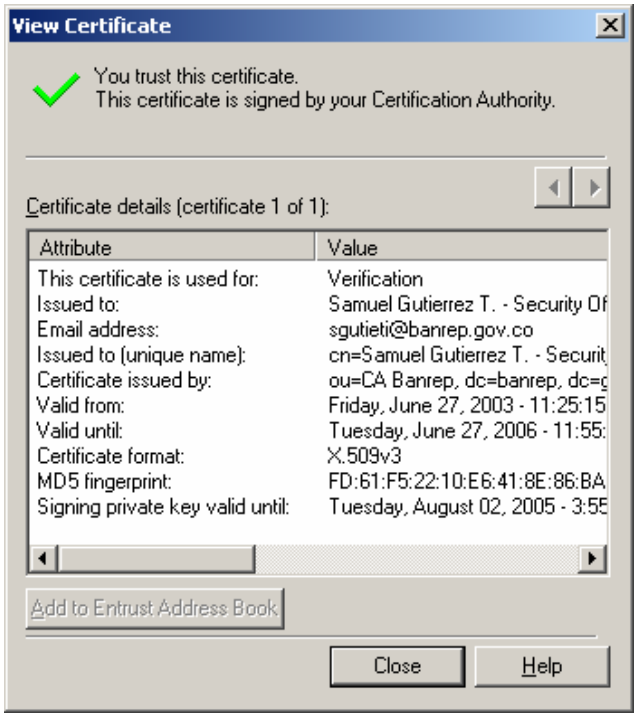
Para verificar la firma de un archivo y conocer el contenido, localícelo por el explorador y dé clic derecho sobre este y encontrará la opción Entrust Advanced. Sobre esta opción de clic sobre verify.



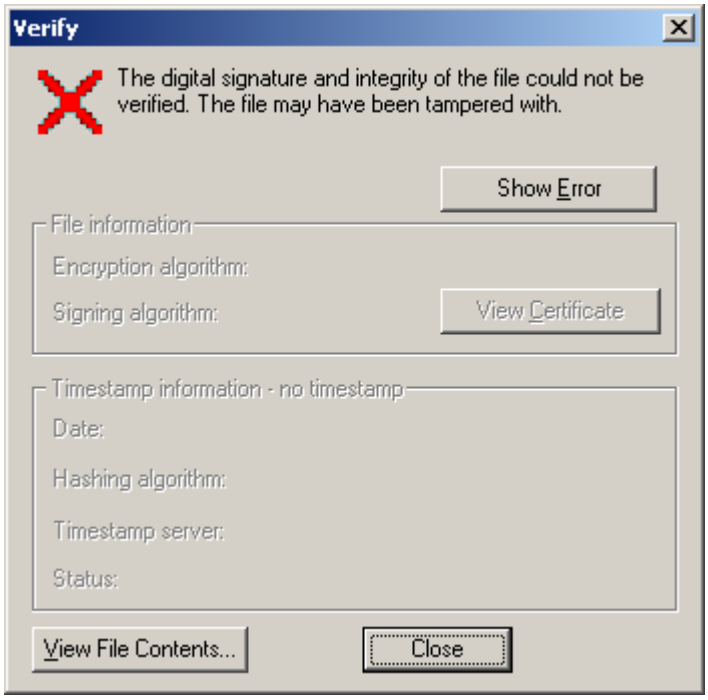
La siguiente pantalla le mostrará las características de seguridad que tiene el archivo.



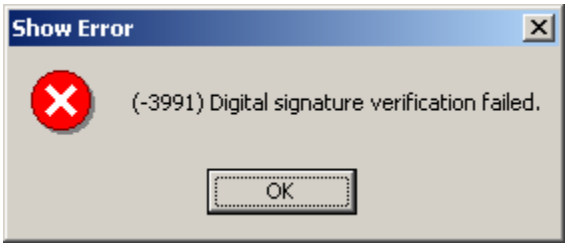
En la parte inferior izquierda de este mensaje, encontrará la opción de View File Contents. Dé clic sobre esta opción, para leer su contenido. También puede ver el certificado con el cual fue firmado el archivo, haga clic en "View Certificate"



En caso que la verificación no sea correcta debe mostrar una ventana como la siguiente:



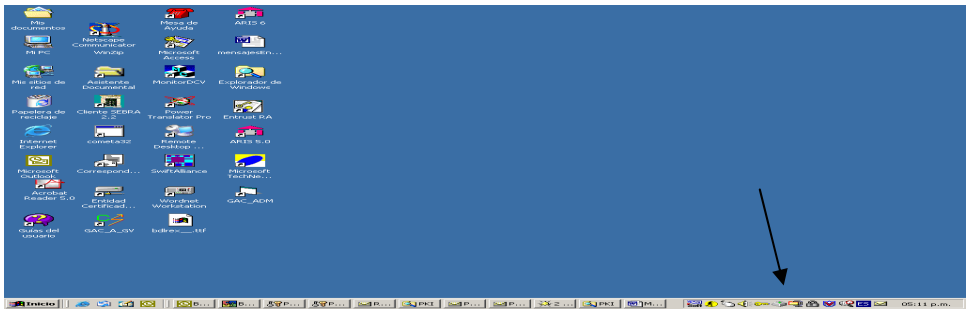
También tiene la opción de mostrar el mensaje de error y puede mostrar algo como lo siguiente:



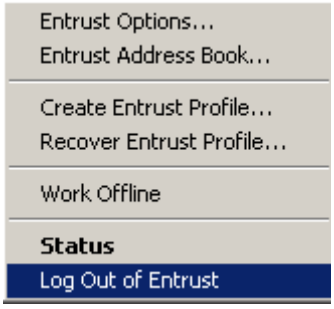
De esta manera no podrá confiar en esta información y la herramienta cliente no le dejará ver el contenido del mensaje.

5 CERRAR LA CONEXIÓN CON LA INFRAESTRUCTURA DE LLAVES PÚBLICAS DE LA CA-BANREP

De clic derecho en la llave amarilla que se encuentra en la parte inferior derecha de la pantalla



Marque la opción Log Out of Entrust para cerrar el sistema.



En la siguiente pantalla, vera en la parte inferior derecha, una llave de color amarillo, la cual tiene una X de color rojo; lo anterior indica que se encuentra desconectado de sistema.

6 GLOSARIO

PKI: Infraestructura de gran alcance que se basa en conceptos de llaves públicas u privadas

Confidencialidad: impide que terceras personas tengan acceso a la información.

Autenticación: Validación del origen de la información.

Integridad: Le ofrece confianza al receptor, en el sentido que la información recibida no ha sido alterada.

No-repudiación: Evita que el originador de la información niegue el envío de los mensajes de datos.

DPC: Declaración de Practicas de Certificación

CA-BANREP: Autoridad de Certificación del Banco de la República

Profile: Estructura de datos en la cual se almacenan las llaves de firma y encripción de los usuarios, los respectivos certificados, el certificado de la entidad de certificación y otra información personal del dueño del profile.

Certificado digital: Archivos digitales que contiene la información básica que le permite a una persona que lo recibe a través de un medio electrónico conocer el remitente del mismo.

Firma digital: método electrónico de firmar un documento constituyéndose en un medio seguro de garantizar al originador y receptor del documento.

Revocación: mecanismo por el que se da por terminado el certificado digital, originando la pérdida de confianza en el mismo.

Servicios: Son los diferentes tipos de operación que realizan las entidades con algunas áreas del Banco de la República. Todos los servicios deben ser relacionados en este formato de "Delegación de usuarios para el manejo de firmas digitales y certificados" para cada uno de los suscriptores.

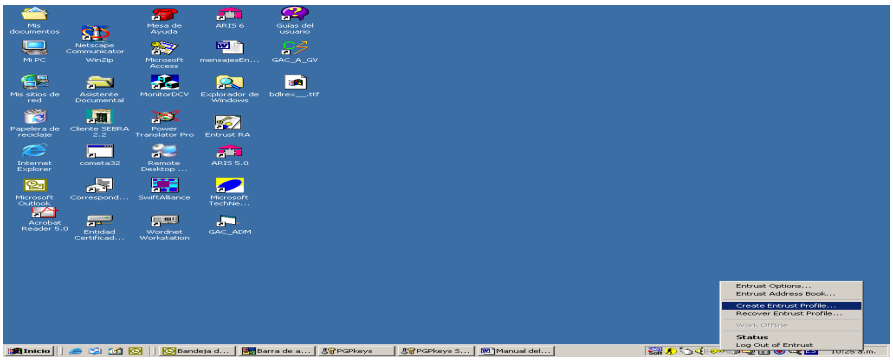
Suscriptor PKI: es el encargado de recibir o transmitir solicitudes o mensajes a las áreas responsables de las operaciones del Banco de la República. Puede ser el mimo delegado con responsabilidad administrativa.

ANEXO 1

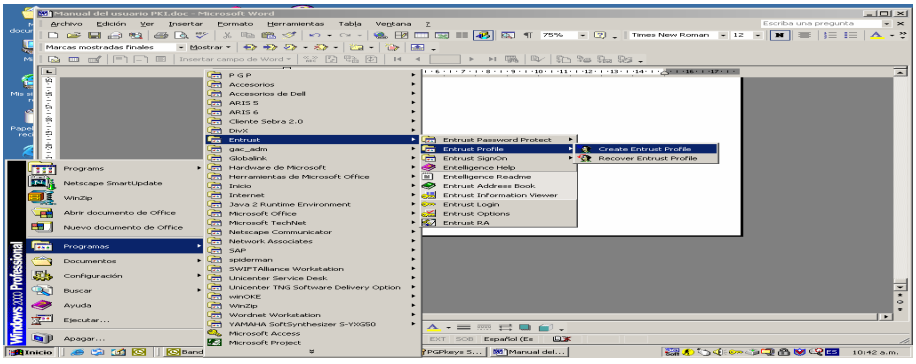
Creación del PROFILE

Se puede realizar de dos formas diferentes:

a. Dé clic derecho sobre la llave amarilla, que se encuentra en la parte inferior derecha de la pantalla y en este menú encontrará la opción Create Entrust Profile.



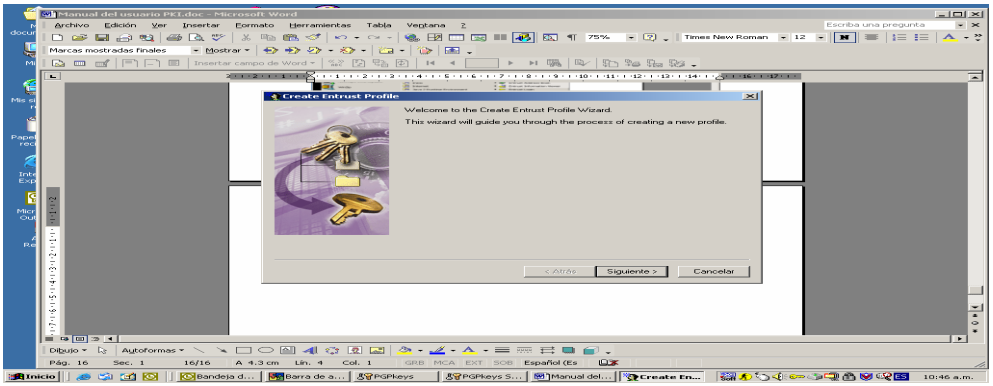
b. Dé clic en **Inicio**, marque la opción **Programas**, seleccione la opción **Entrust** y selecciones **Entrust Profile**. En este menú encontrará la opción Create Entrust Profile.



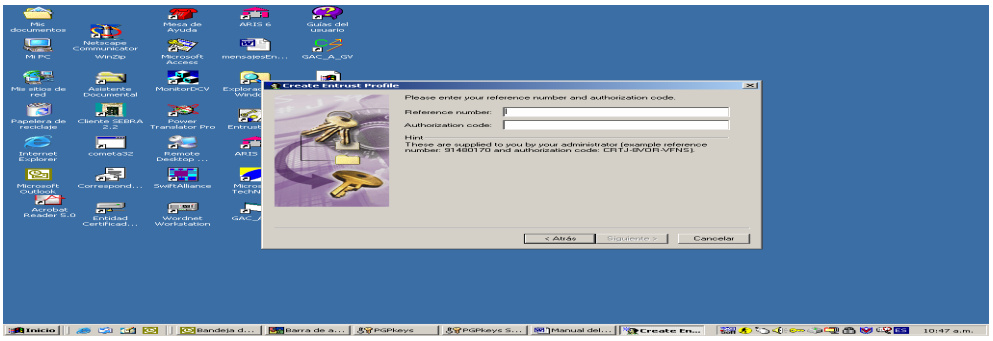
Por cualquiera de los dos pasos anteriores, obtendrá la siguiente pantalla que le permite registrar las claves que previamente le fueron entregadas. (Código de Autorización y Número de Referencia). Este procedimiento debe realizarlo dentro de los primeros 8 días calendario, contados a partir de la fecha de generación de los dos números claves.

En el evento de pasarse esta fecha, deberá solicitar nuevamente el par de claves.

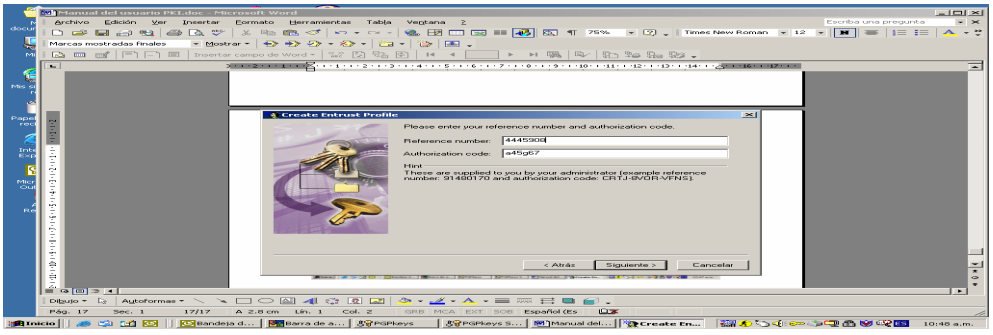
Marque la opción siguiente y encontrará los espacios para incluir el Código de Autorización y el Número de Referencia



Registre los datos requeridos



Después de incluir los datos requeridos, marque la opción siguiente.



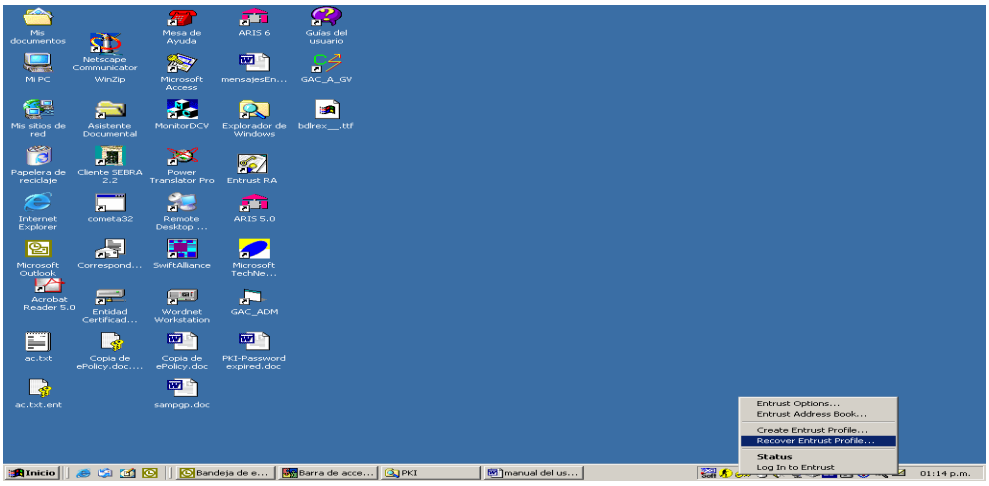
Si usted tiene conección SEBRA con el Banco de la República, este PROFILE viajará en forma automática a la CA BANREP y el usuario quedará registrado.

ANEXO 2

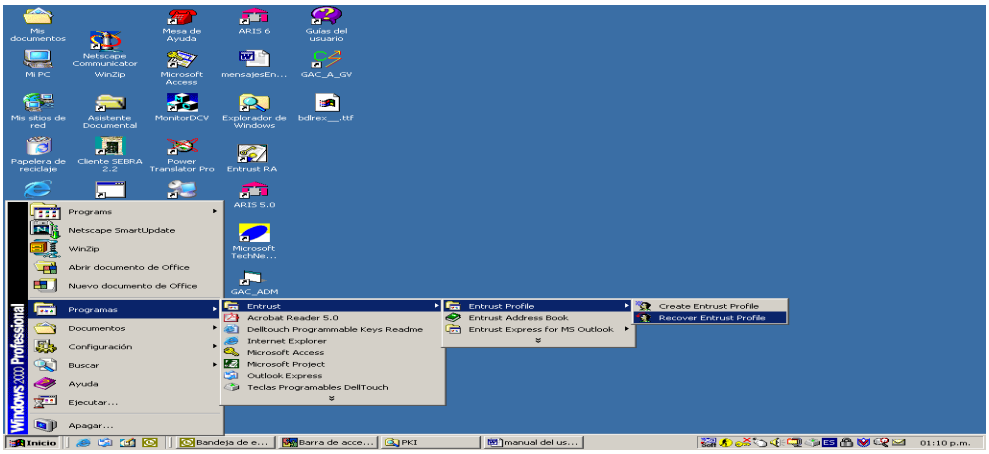
Recuperación del PROFILE

Se puede realizar de dos formas diferentes:

a. Dé clic derecho sobre la llave amarilla, que se encuentra en la parte inferior derecha de la pantalla y en este menú encontrará la opción Recover Entrust Profile.



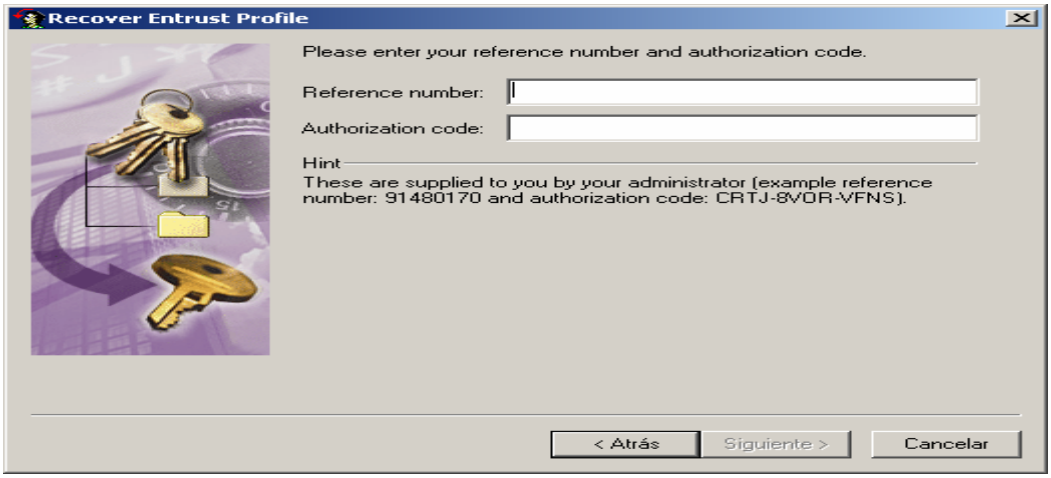
b. De clic en **Inicio**, marque la opción **Programas**, seleccione la opción **Entrust** y selecciones **Entrust Profile**. En este menú encontrará la opción Recover Entrust Profile.



Por cualquiera de los dos pasos anteriores, obtendrá la siguiente pantalla que le permite registrar las claves que previamente le fueron entregadas. (Código de Autorización y Número de Referencia). Este procedimiento debe realizarlo dentro de los primeros 8 días calendario, contados a partir de la fecha de generación de los dos números claves.

En el evento de pasarse esta fecha, deberá solicitar nuevamente el par de claves.

Con los datos que previamente le fueron entregados, diligencie los datos que a continuación se muestran.



Cuando estén los datos incluidos, marque la opción siguiente.

El Nombre del Profile debe seguir el siguiente formato:

12345678-xyyyyyzz-99-99999-99

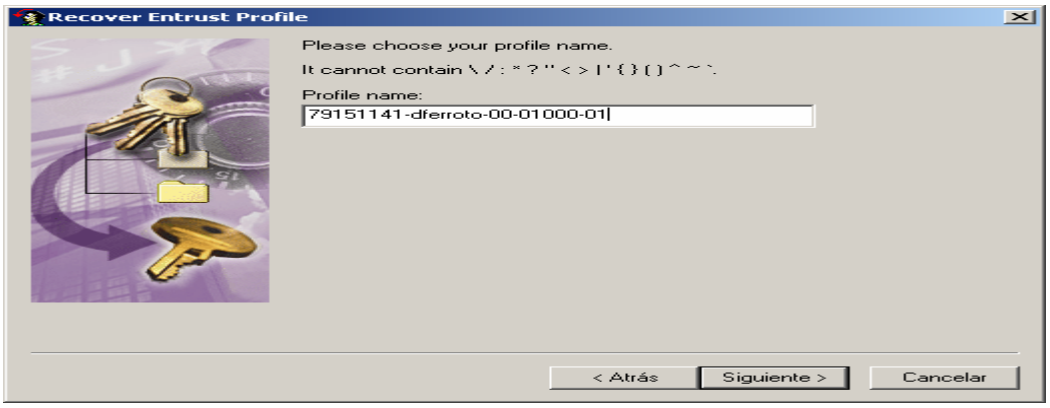
Los primeros dígitos son el número de su cédula, debe teclearlos seguidos, sin puntos ni espacios. Luego incluya un guión y a continuación su carga de usuario. Esta carga, se compone de la primera letra del primer nombre, los cinco primeros dígitos del primer apellido y los dos primeros del segundo apellido.

Ej: diego ramírez gómez - dramirgo

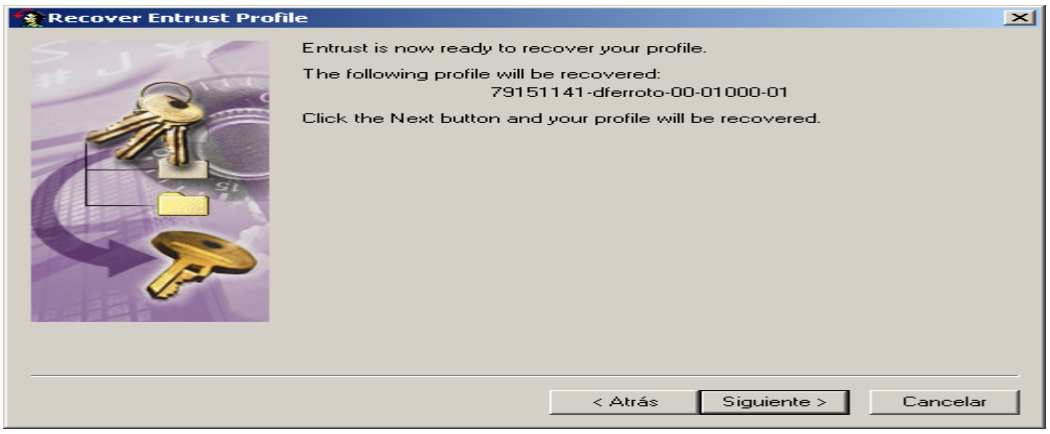
A continuación, nuevamente incluya un guión e inmediatamente después dos dígitos que corresponden al sector que de su entidad. Seguido y con guión, el código SEBRA. Por último, adicione un guión seguido por el código de la ciudad.

> **CódigoCiudad:** Está compuesto por dos dígitos que corresponde a la tabla vigente del Banco de la República.
> **Bogotá 01, Armenia 10, Barranquilla 13, Bucaramanga 16, Buenaventura 18, Cali 20, Cartagena 22, Condoto 26, Cucuta 28, Florencia 35, Girardot 40, Guapi 42, Honda 45, Fca de Moneda 46, Ibague 47, Ipiales 50, Leticia 53, Manizales 56, Medellín 58, Montería 60, Neiva 62, Pasto 65, Pereira 67, Popayán 69, Quibdo 73, Riohacha 75, SantaMarta 78, Sincelejo 80, Tunja 85, Valledupar 86, Villavicencio 87, San Andres 88.**

La carga debe ser en minúscula. Para aquellos que no utilizan el código SEBRA y no están codificados, se les asignará un código definido por el Centro de Soporte del Banco de la República.



Dé clic en siguiente.



Con las condiciones que se describen a continuación debe crear un password. Después de confirmarlo, digite la tecla Siguiente.

En el espacio en blanco no marque nada, y dé clic en finalizar.

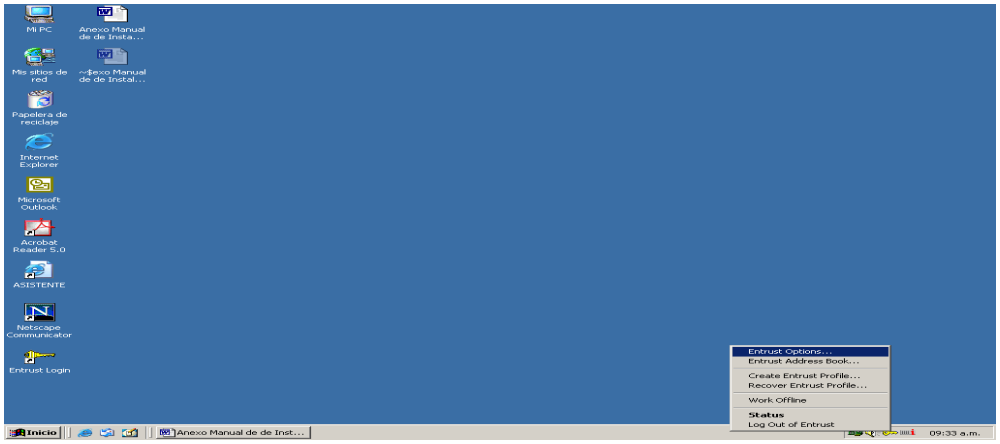
ANEXO 3

CONFIGURACIÓN

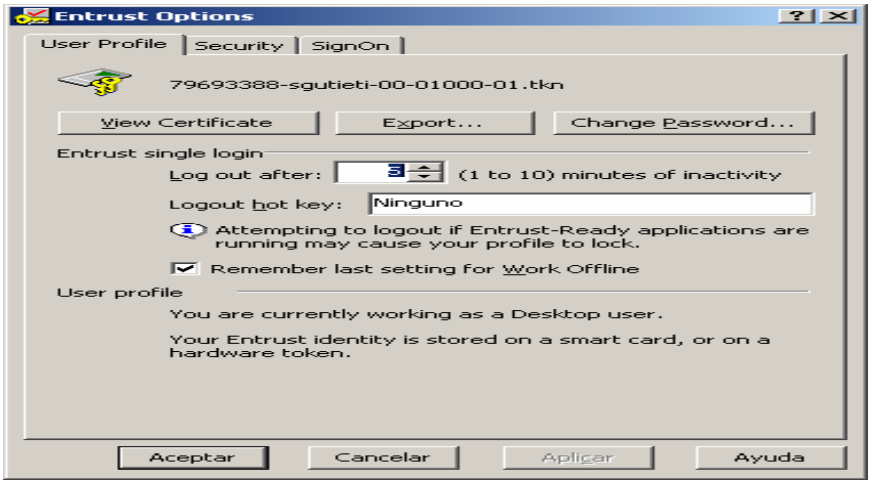
Opciones de Configuración en el Cliente

Una vez instalado el software y conectado al Profile, vamos a configurar las opciones de uso de la aplicación Entelligence.

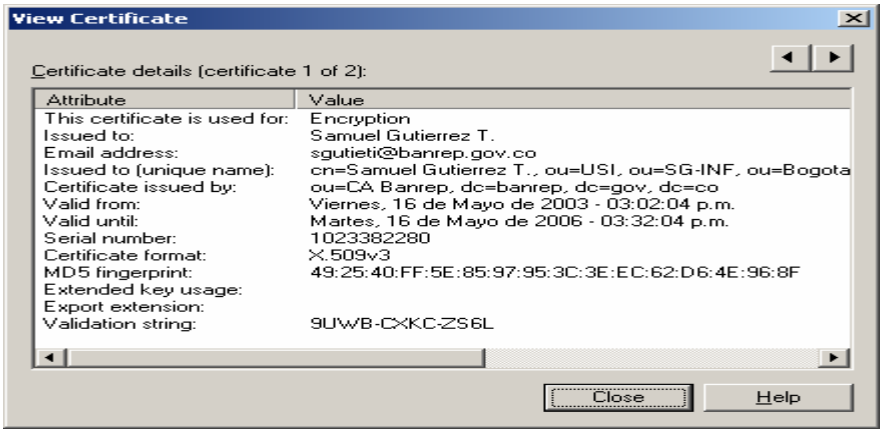
Haga clic en la llave amarilla que aparece en la parte inferior derecha y seleccione la opción “Entrust Options...”

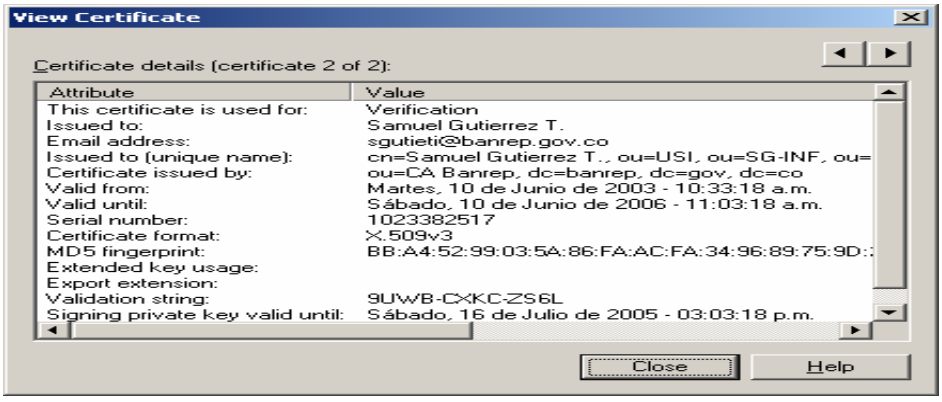


Le aparece una ventana como la siguiente:



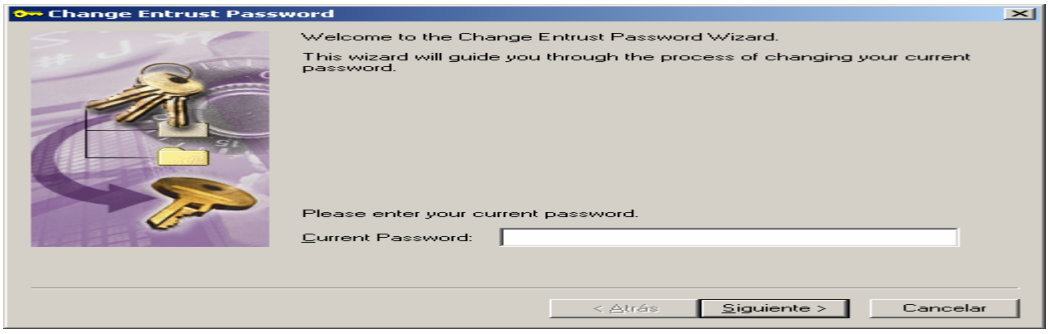
Aquí puede ver los certificados de su Profile.





También se puede cambiar el password, cuando el usuario lo desee, sin embargo existe una política de certificados que obligará a los usuarios ha cambiar el password con una periodicidad establecida.

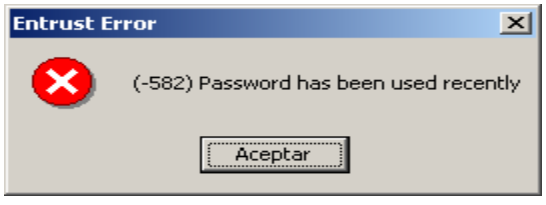
Escriba el password.



Escriba su nuevo password y confírmelo.

Después de confirmarlo, dé clic en finalizar.

Si el password ha sido usado recientemente le aparecerá una ventana como la siguiente



y debe escribir uno diferente.

Si no le reporta lo anterior, la acción ha terminado con éxito

La configuración por cada uno de los tab se recomienda que sea como la siguiente: