



Banco de la República
Bogotá D. C., Colombia

Subgerencia de Informática
Unidad de Seguridad Informática

MANUAL INSTALACIÓN SUSCRIPTORES
EXTERNOS

USI-PN-16

16 de Junio 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 INSTALACIÓN Y CONFIGURACIÓN	5
2.1 INSTALACIÓN DEL CLIENTE ENTELLIGENCE	5
2.2 INSTALACIÓN DEL DISPOSITIVO USB DE ALMACENAMIENTO DE LOS PROFILES ..	7
2.3 CAMBIOS EN EL ARCHIVOS DE HOSTS DE LA MÁQUINA	12
2.4 INICIALIZACIÓN DEL TOKEN	13
2.5 CAMBIO DE PASSWORD	18
2.6 CREACIÓN O RECUPERACIÓN DEL PROFILE	19
2.7 CONFIGURACIÓN	24
3 GLOSARIO.....	29



1 INTRODUCCIÓN

1.1 OBJETO

Este documento explica el proceso de instalación y configuración del cliente PKI para la CA BANREP, el software Entrust Entelligence y los respectivos drivers para el dispositivo de almacenamiento del Profile.

1.2 ALCANCE

Explicar detalladamente los pasos a seguir para la instalación y configuración de las herramientas necesarias para hacer uso de los certificados de los suscriptores.

1.3 AUDIENCIA

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



2 INSTALACIÓN Y CONFIGURACIÓN

2.1 INSTALACIÓN DEL CLIENTE ENTELLIGENCE

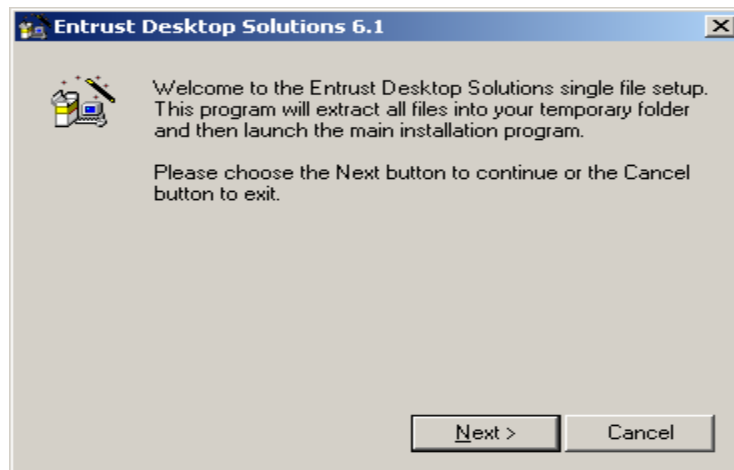
Antes de iniciar la instalación del software, debe tener en cuenta que:

- Debe estar conectado con la carga de un administrador de la máquina.
- Debe tener, por lo menos, 30 MB libres en el disco c:\
- Debe cerrar todas las aplicaciones antes de iniciar la instalación.
- El sistema operativo debe ser Windows 2000 SP2

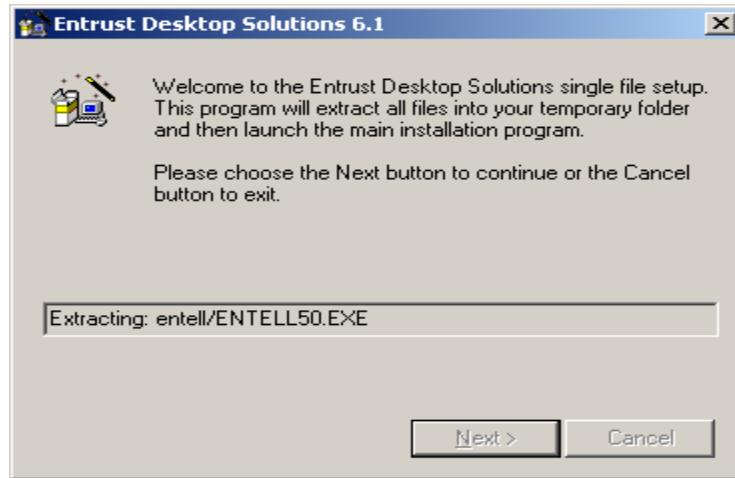
Para realizar la instalación del cliente Entelligence, se debe haber adquirido previamente el software de sitio calima.banrep.gov.co y el archivo instalador es:

CABanrep.exe

Dé doble clic a este archivo y saldrá la siguiente grafica



Dé clic en Next



Dé clic en Next



Durante el proceso de instalación le aparecerán los símbolos de instalación (parte inferior derecha).

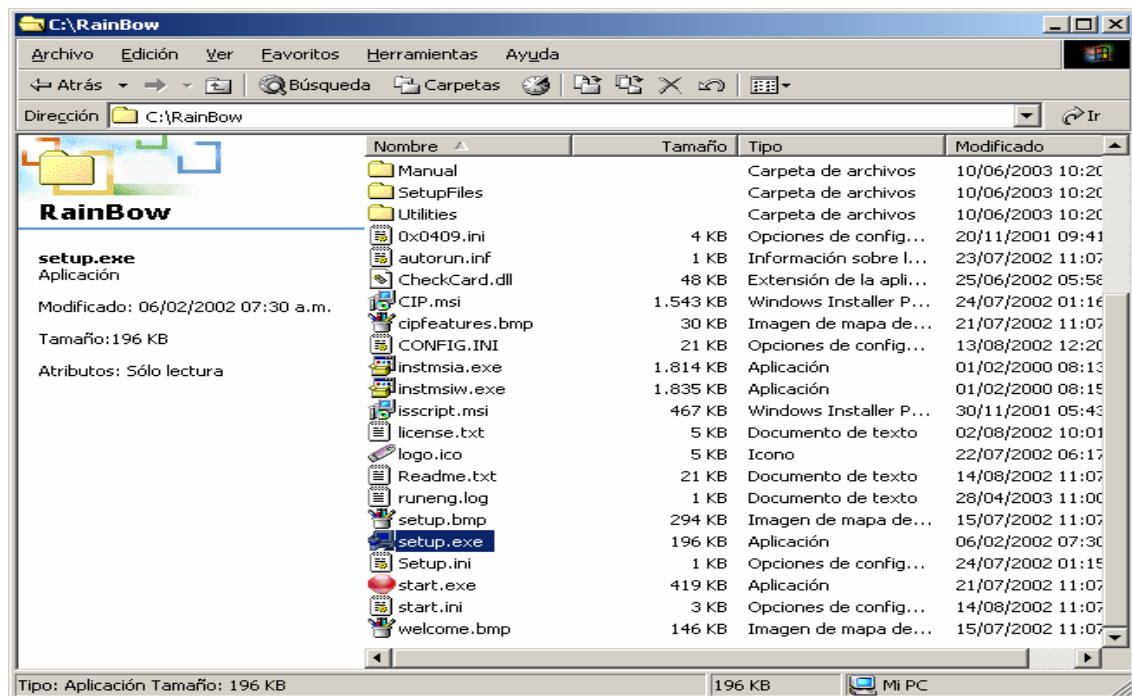
El sistema se reiniciará automáticamente.



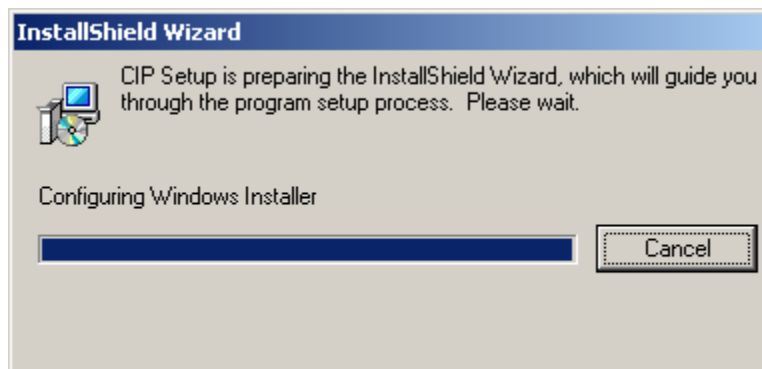
2.2 INSTALACIÓN DEL DISPOSITIVO USB DE ALMACENAMIENTO DE LOS PERFILES

Para realizar la instalación conéctese al sitio calima.banrep.gov.co

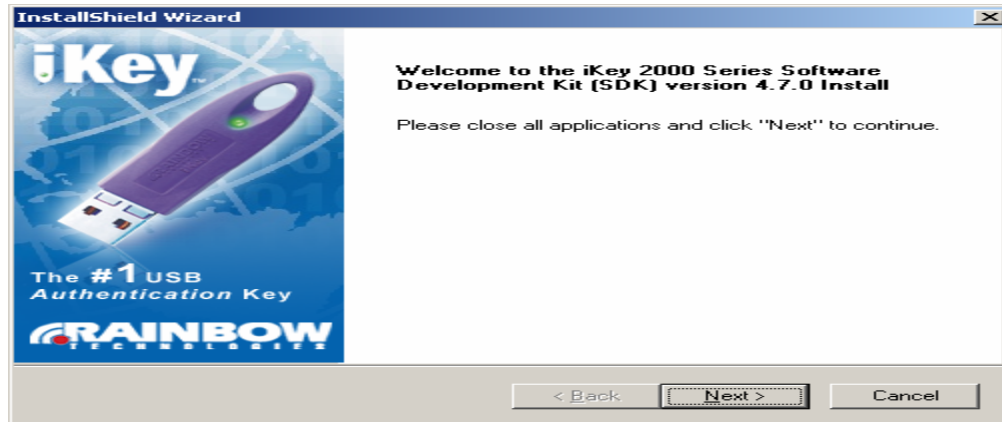
En el archivo Zip **rainbow.zip**, dar doble clic sobre este y buscar el archivo **setup.exe**,



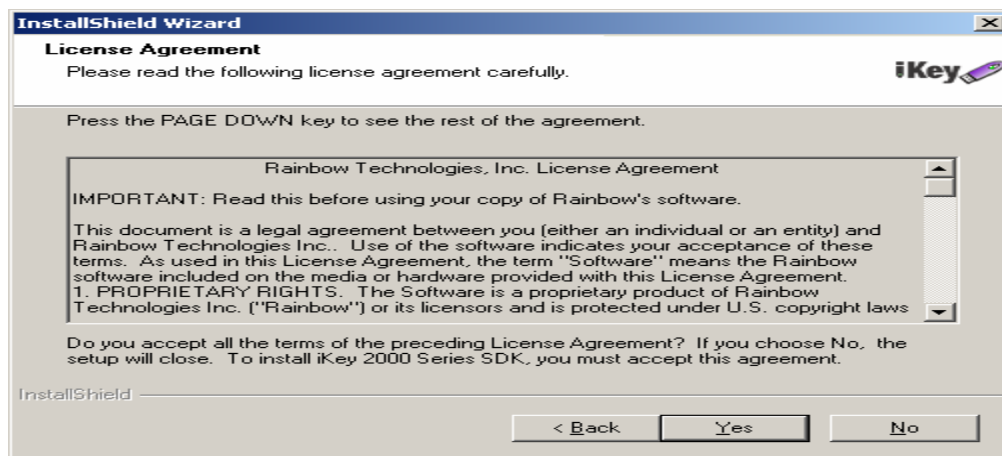
haga clic sobre este archivo.



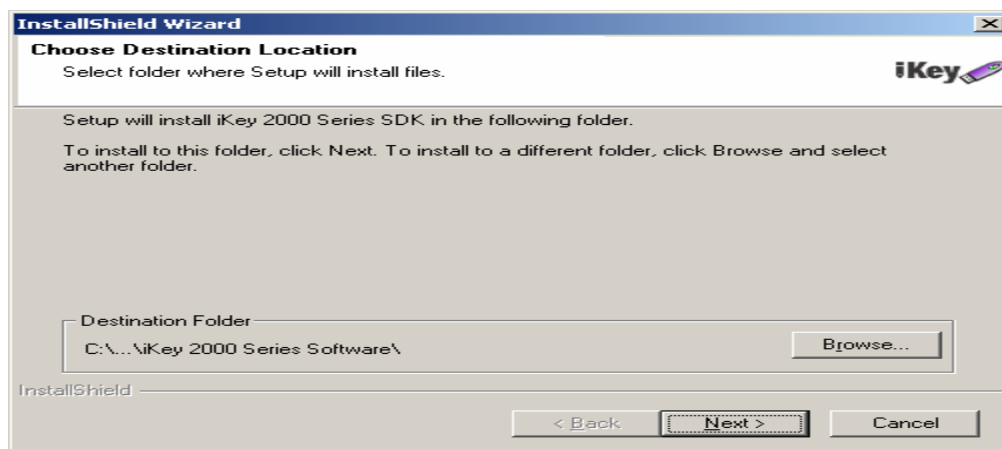
En este gráfico, le muestra que el proceso se está llevando a cabo.



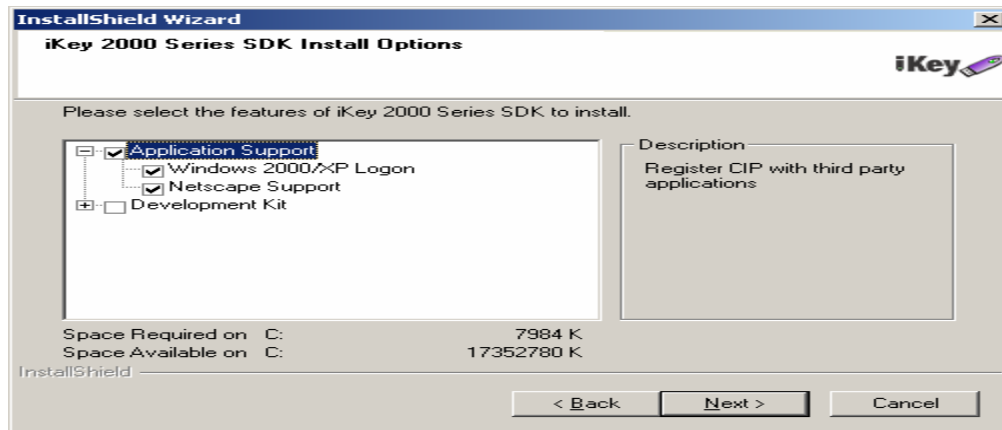
Haga clic en Next



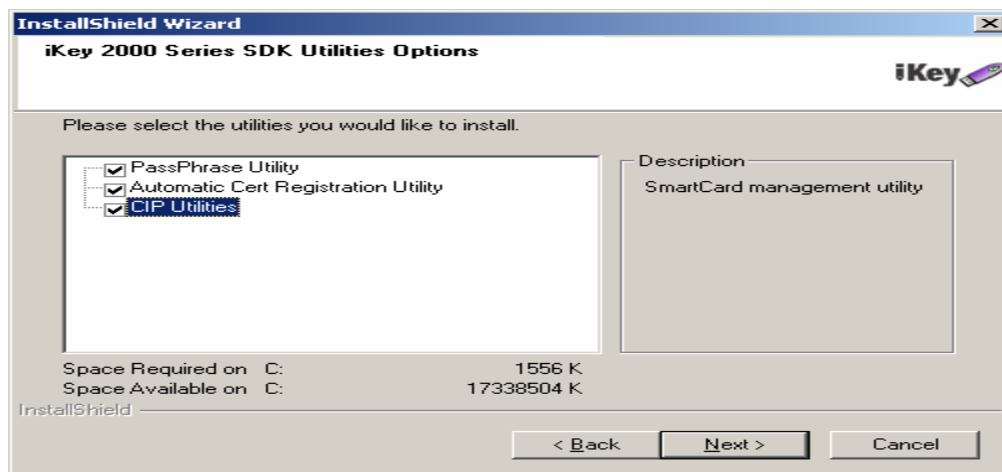
Dé clic en Yes



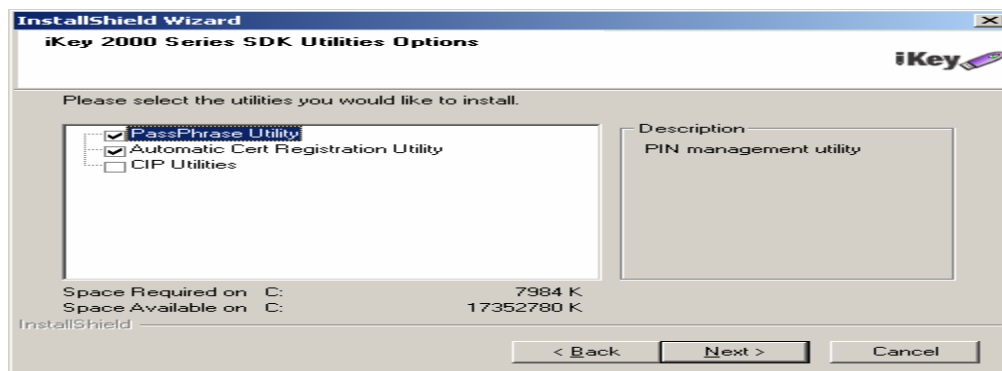
Únicamente seleccione las tres primeras y dé clic en Next



Si usted esta instalando **para el Delegado con responsabilidad administrativa**, se marcan las tres opciones que se muestran en la gráfica y dé clic en Next

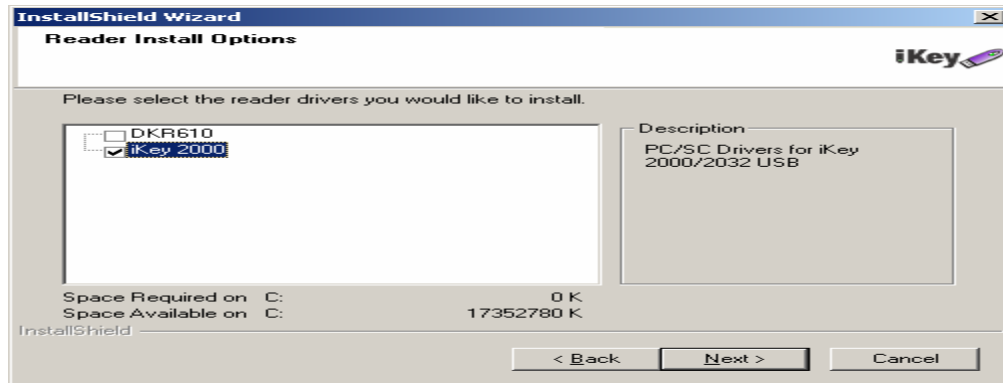


Si usted esta instalando **para el usuario**, se marcan las dos opciones que se muestran en la gráfica y dé clic en Next.

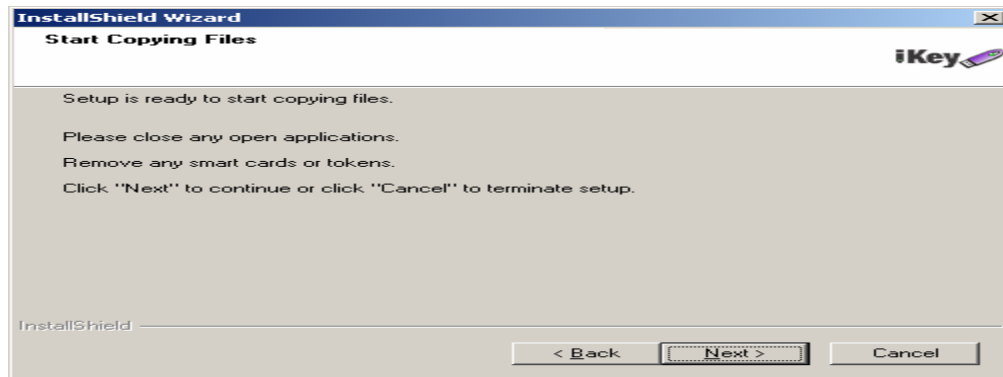




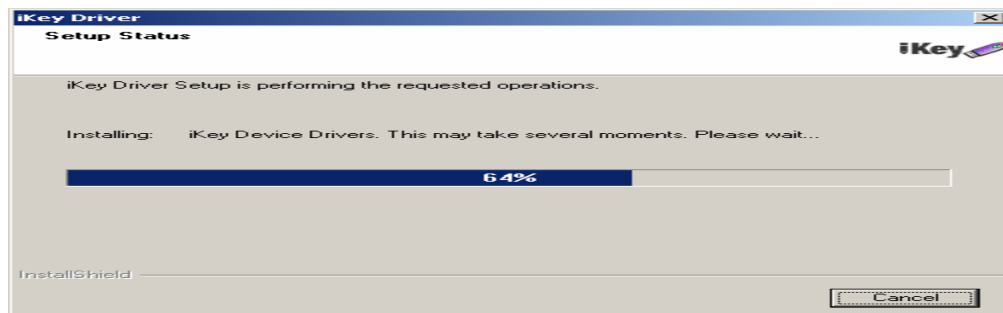
Haga clic en Next

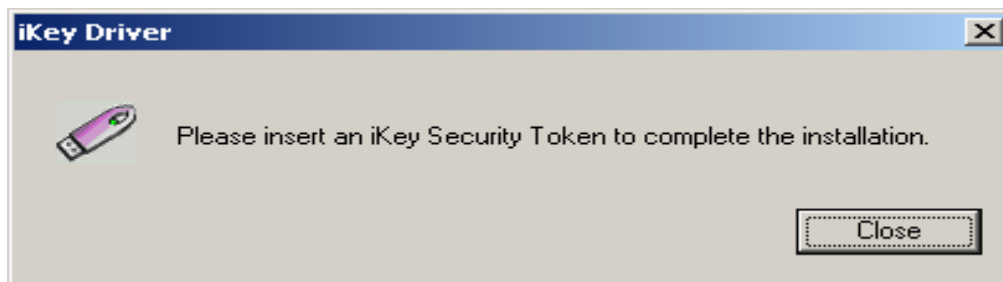
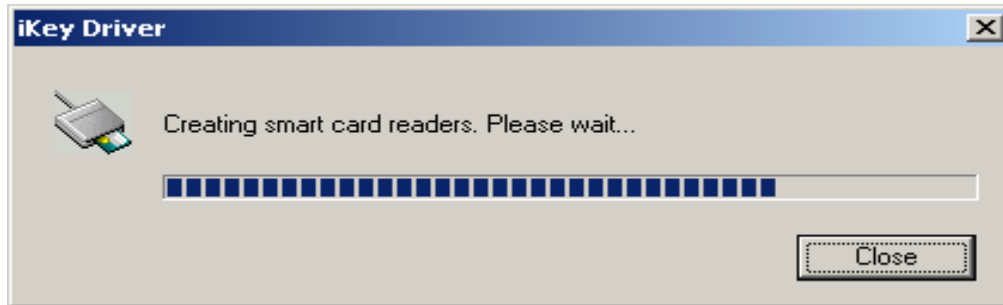


Haga clic en Next

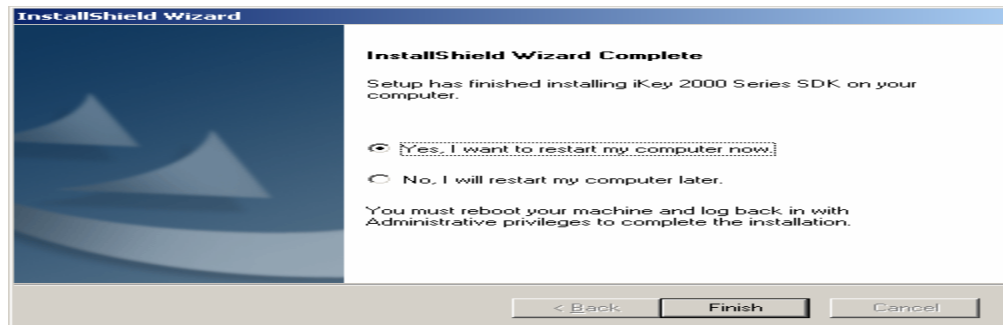


En las gráficas siguientes, se muestra el proceso de instalación.



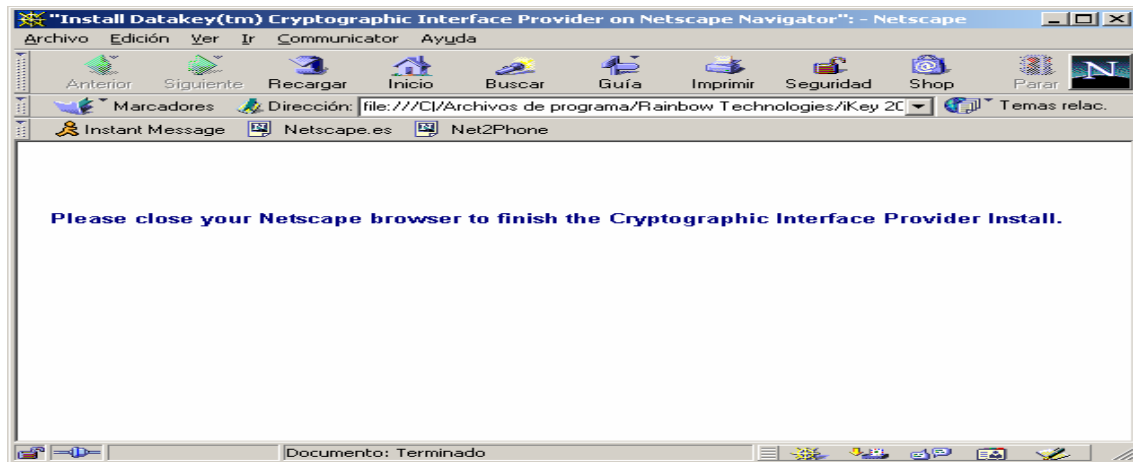


Inserte el token en el puerto de la máquina



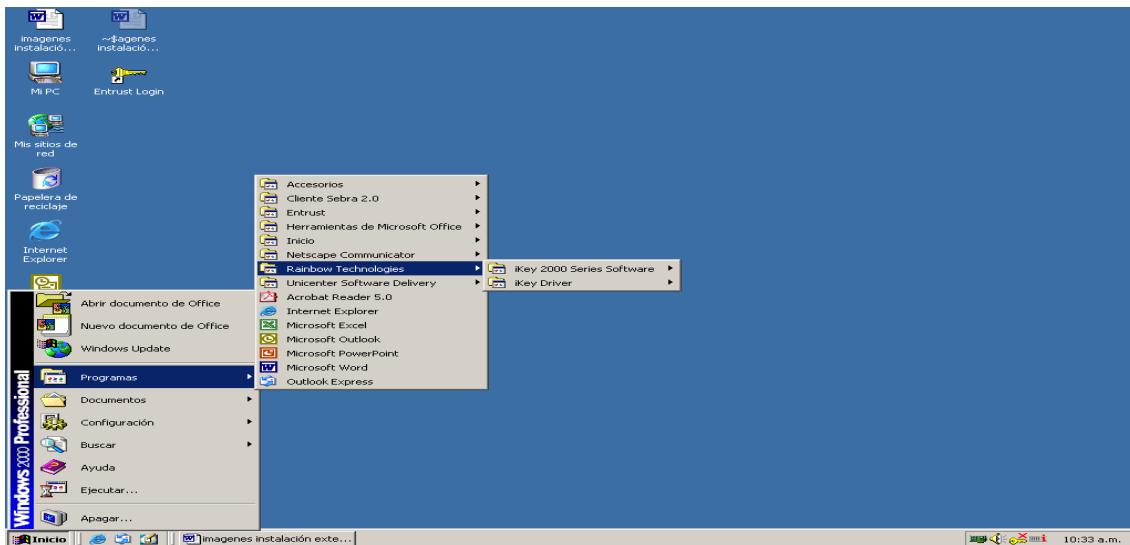
Dé clic en Finish

Debe reiniciar la máquina y cuando esto ocurra marque aceptar en la siguiente ventana y aparecerá esta.



Cierra la ventana anterior

Para verificar que la instalación tuvo éxito, se debió crear el grupo de Programas llamado Rainbow Technologies y este debe tener 2 sub carpetas: iKey 2000 Series Software y iKey Driver



2.3 CAMBIOS EN EL ARCHIVOS DE HOSTS DE LA MÁQUINA

Para realizar los cambios requeridos para la conexión al Banco de la Republica hacia las máquinas PKI, debe bajar del sitio calima.banrep.gov.co el archivo **addhostpki.exe**, dar doble clic sobre este y el cambio será realizado.

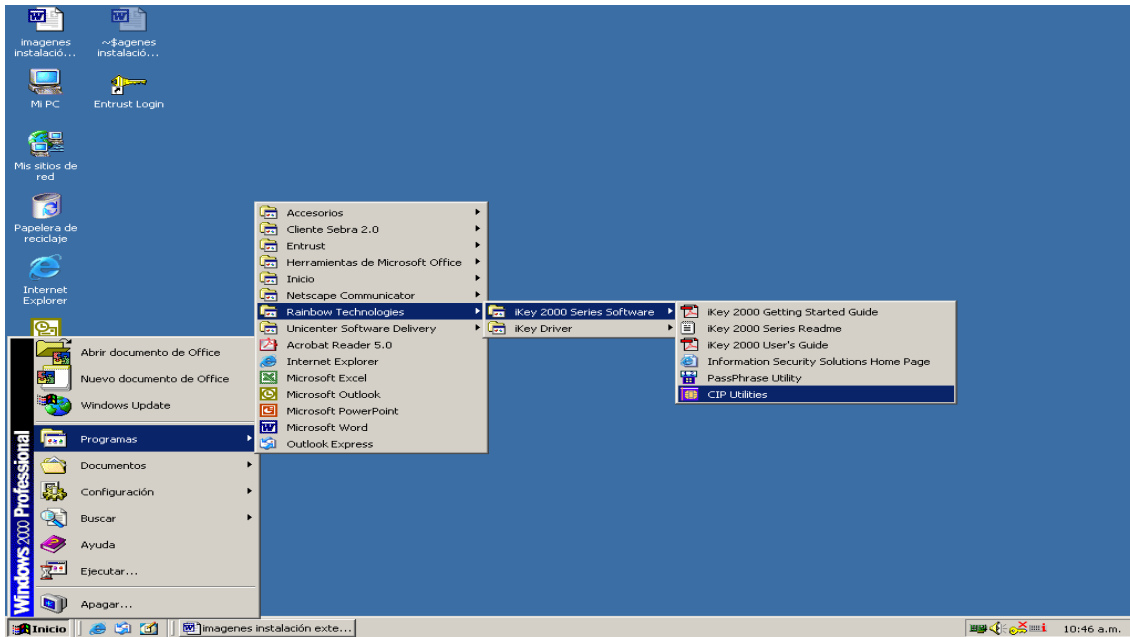


2.4 INICIALIZACIÓN DEL TOKEN

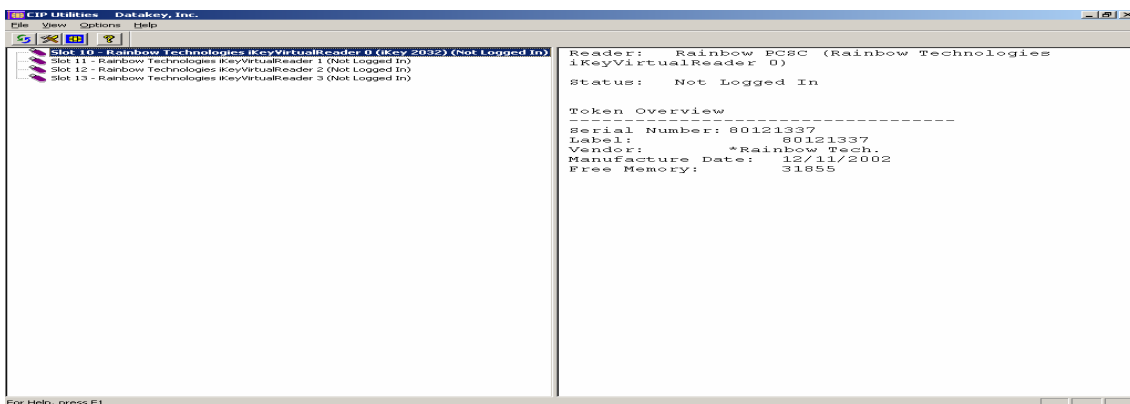
Teniendo en cuenta que el Token es nuevo, es necesario inicializarlo. Para esto se sigue el siguiente procedimiento:

Por inicio, siga la siguiente ruta:

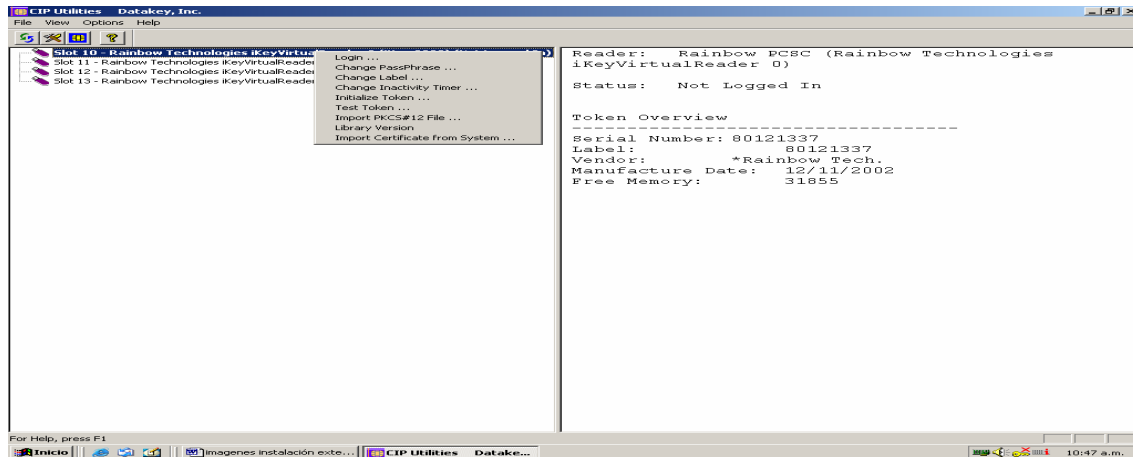
Inicio→Programas→Rainbow Technologies→iKey 2000 Series Software→CIP Utilities



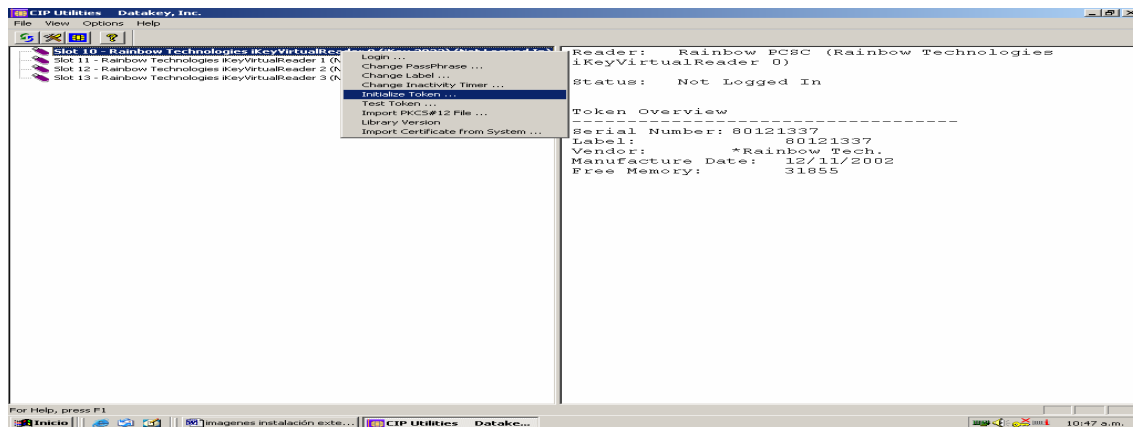
Se reconoce el token



Al realizar clic derecho sobre el token reconocido por las utilidades, aparece esta ventana

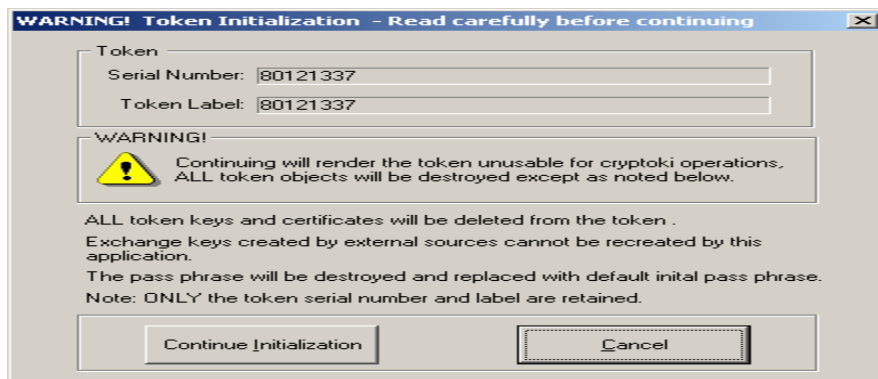


Siempre se debe inicializar (“formatearlo”) el token. Dé clic sobre la opción señalada.



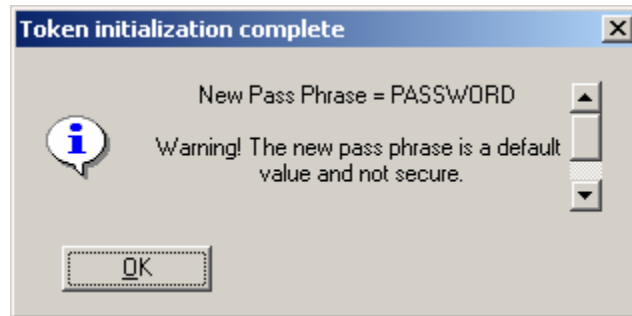
En la siguiente pantalla se muestra el número del serial y del Token

Dé “Continue Initialization”, para continuar

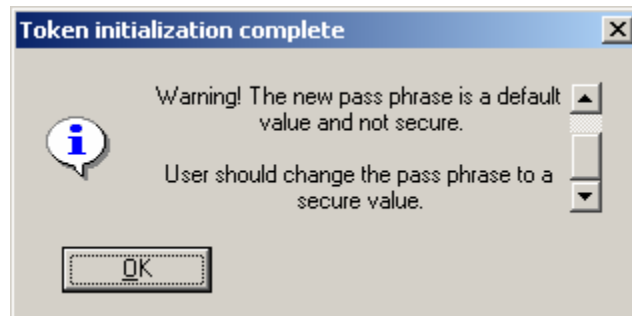




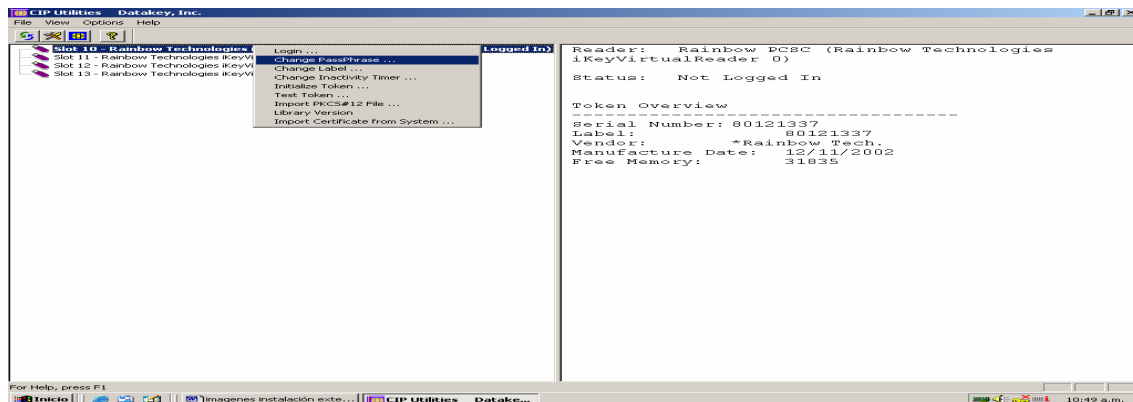
Después de inicializar el Token, el password es la palabra **PASSWORD** y dé clic en OK



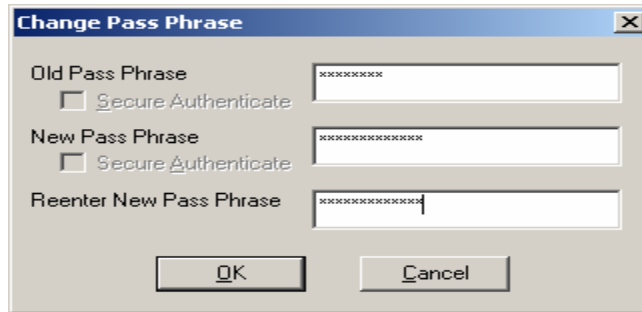
Dé clic en OK



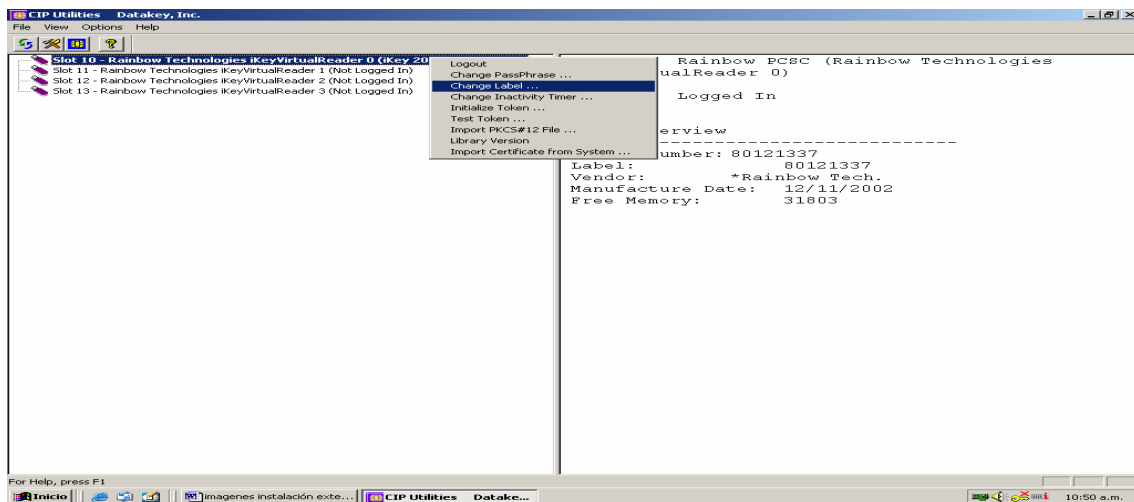
Dé clic derecho sobre la opción señalada para realizar el cambio de password.



En el espacio Old Pass Phrase digite la palabra **PASSWORD** y enseguida el nuevo con su respectiva confirmación.

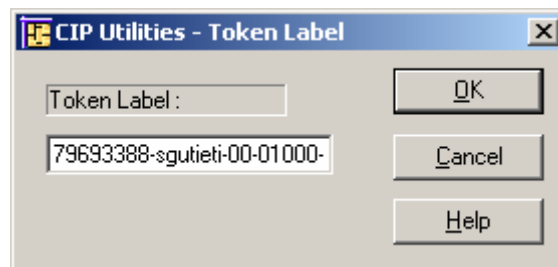


Dé clic derecho sobre la opción señalada para realizar el cambio de label.

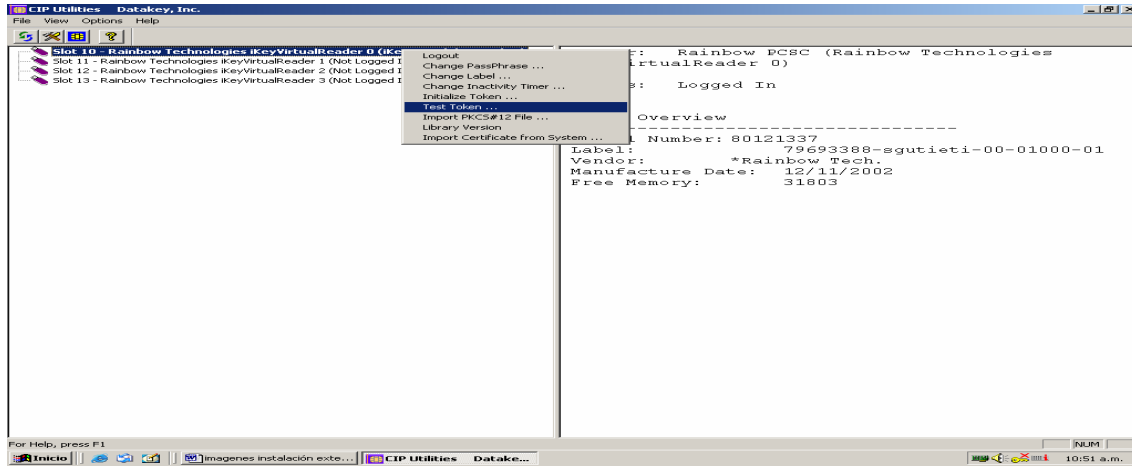


Registre en el siguiente campo, el label que le fue informado en el acta de entrega del código de autorización.

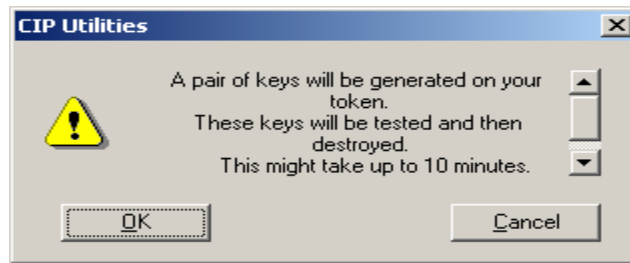
Dé clic en OK



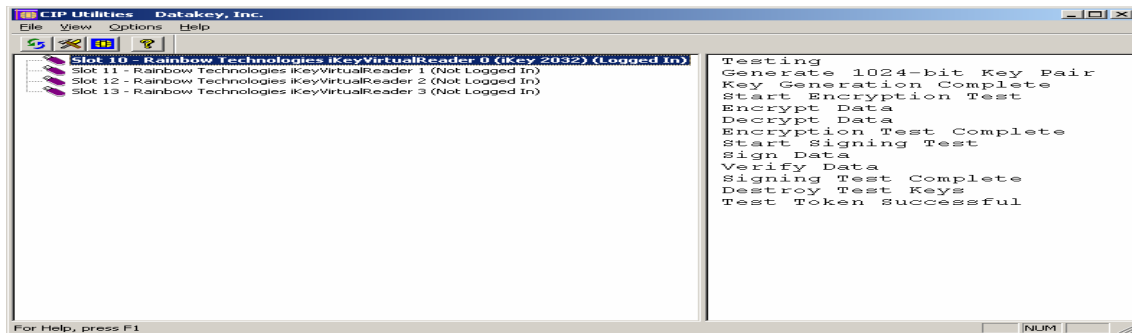
Dé clic derecho sobre la opción señalada para realizar un Test al Token

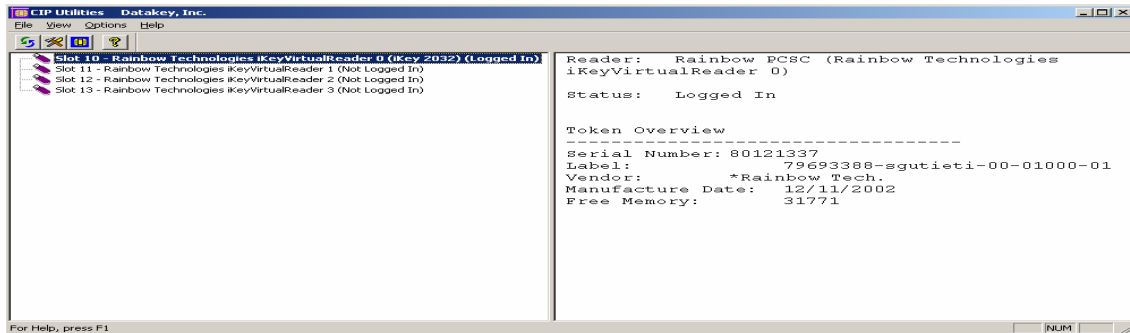


Dé clic en OK. (El proceso puede demorar 10 minutos aprox.)



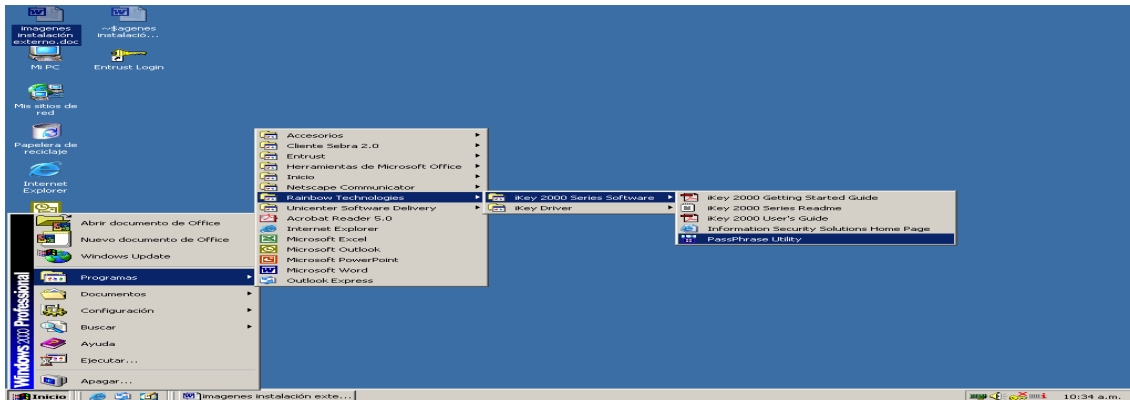
Siempre debe aparecer que el test fue exitoso ver ventana siguiente.



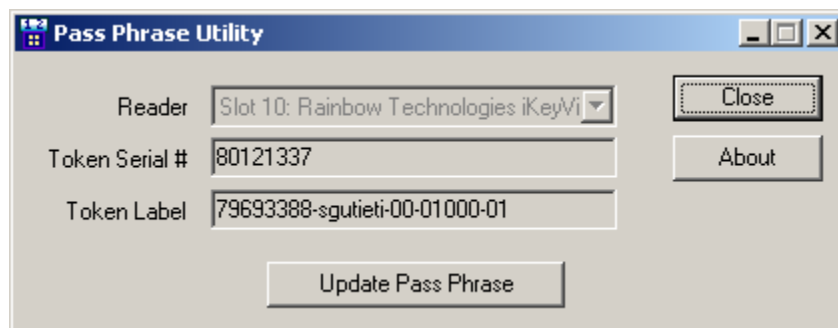


2.5 CAMBIO DE PASSWORD

El suscriptor final de la entidad debe cambiar el password con la utilidad de cambio de password inicio → Programas → Rainbow Technologies → iKey series 2000 Software → Passphrase Utility.

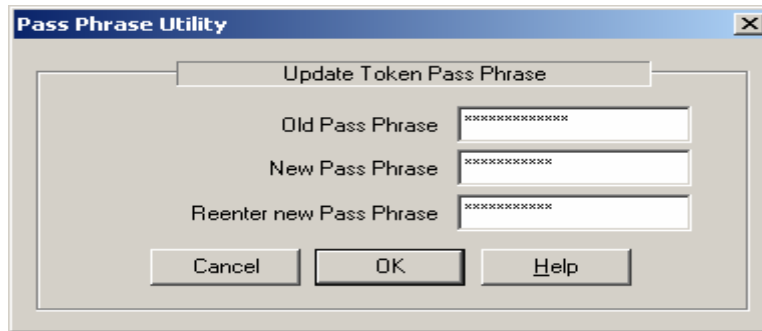


Reconoce el token y muestra su serial y label, haga clic en “Update PassPhrase”

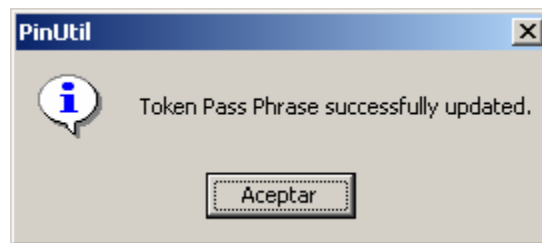




Debe digitar el nuevo password con el cual se inicializó el token.



Muestra la ventana de terminación exitosa.



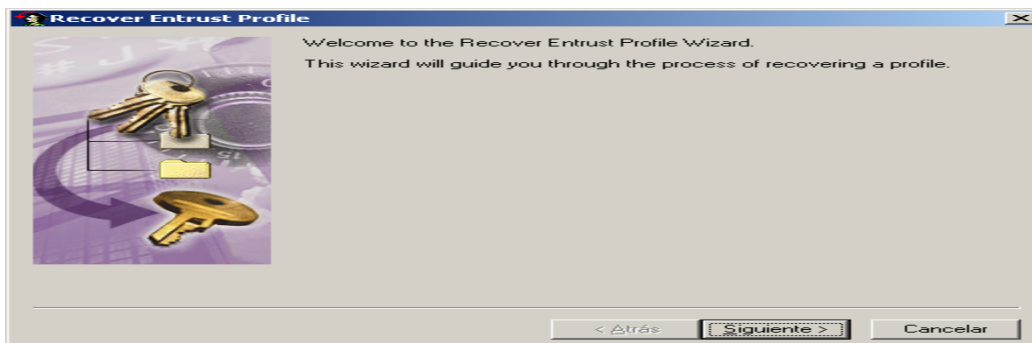
Terminó la instalación y configuración.

2.6 CREACIÓN O RECUPERACIÓN DEL PROFILE

Siguiendo los procedimientos establecidos por la DPC - Declaración de Prácticas de Certificación (<http://www.banrep.gov.co/ca-banrep/documentos/pdc.pdf>), usted obtiene el Número de Referencia y el Código de Autorización

Haga clic derecho en la llave amarilla que aparece en el extremo inferior derecho de su pantalla y seleccione la opción crear o recuperar un Profile, según sea el caso.

Dé clic en siguiente





Ingrese los datos solicitados y dé clic en siguiente.

Recover Entrust Profile

Please enter your reference number and authorization code.

Reference number: 23382516

Authorization code: 3D>K-PPCZ-LWFA

Hint
These are supplied to you by your administrator (example reference number: 91480170 and authorization code: CRTJ-8VDR-VFNS).

< Atrás Siguiete > Cancelar

La siguiente gráfica le mostrará, de forma automática, que reconoce el puerto donde se encuentra el Token

Recover Entrust Profile

Select a folder within which to store your profile:

C:\aca-banrep\Profiles Browse...

Store profile on hardware token (card)

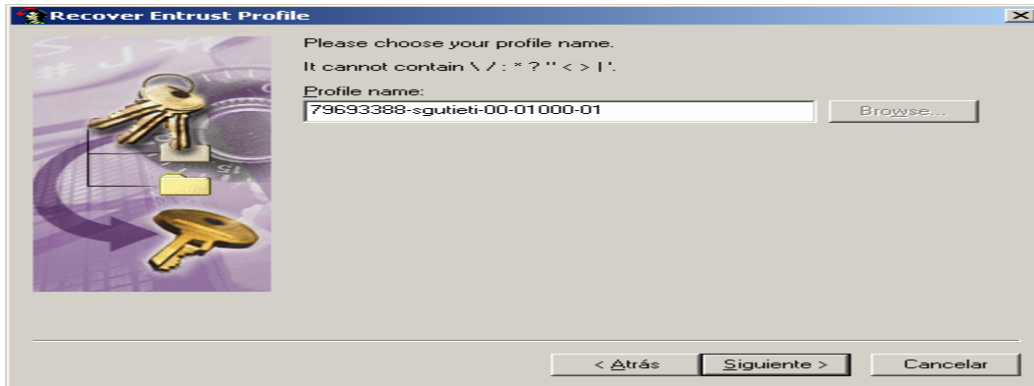
Slot 10

Hint
Your Entrust Profile contains your encryption/decryption keys and your signing/verification keys. The profile can be stored locally on disk or on a hardware token. All supporting files, including your address book, will be stored in the specified folder.

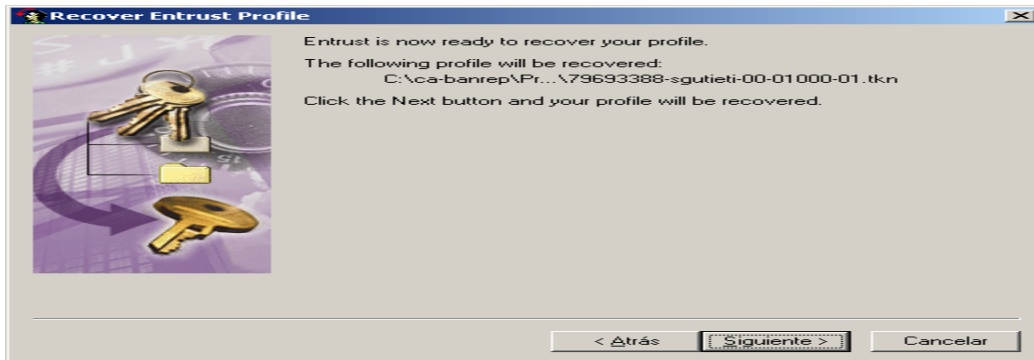
< Atrás Siguiete > Cancelar

Importante no cambiar ninguno de los datos.

Escriba el nombre del Profile, que se encuentra en el acta de entrega del código de autorización. Dé clic en siguiente.



Dé clic en siguiente.



Digite el password que actualmente tiene el token

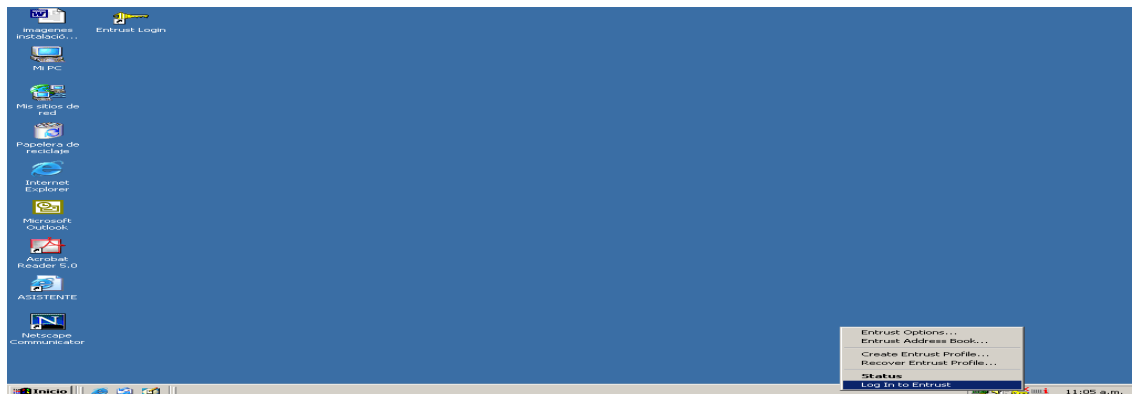


Deje la casilla en blanco y dé clic en Finalizar



Debe abrir el sistema. Dé clic derecho sobre la llave amarilla que se encuentra en la parte inferior derecha de su pantalla.

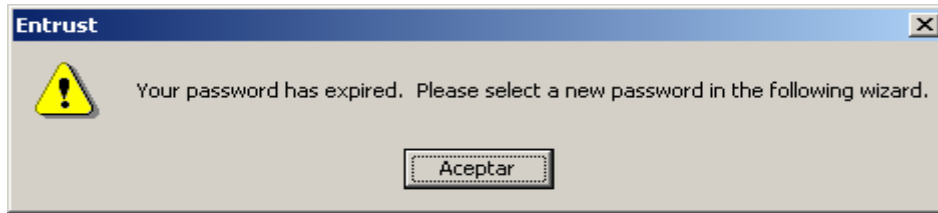
Dé clic sobre la opción señalada.



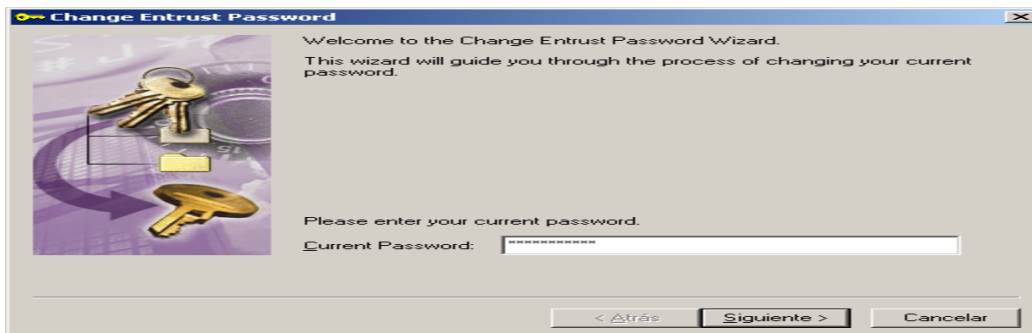
Digite su password y dé clic en OK.



Debe realizar el cambio de password . Dé clic en Aceptar.



Digite el nuevo password que le incluyó al Token.



Registre el nuevo password y confírmelo. Dé clic en Finalizar.



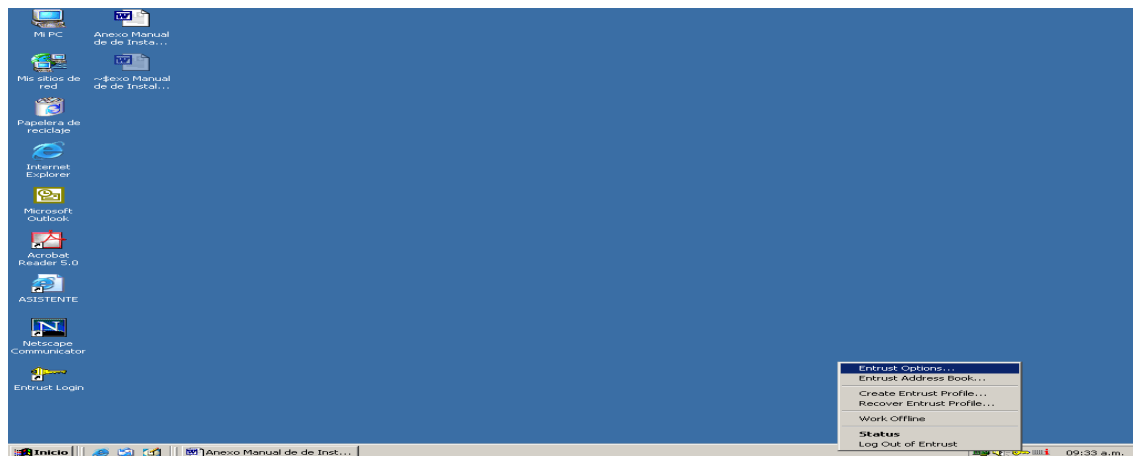
Su password fue cambiado con éxito. Dé clic en aceptar y así termina el proceso.



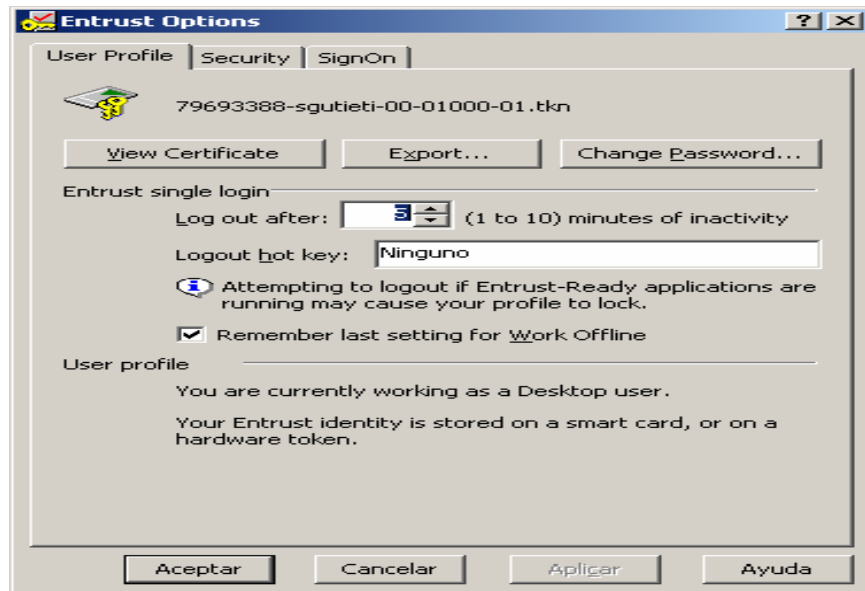
2.7 CONFIGURACIÓN

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

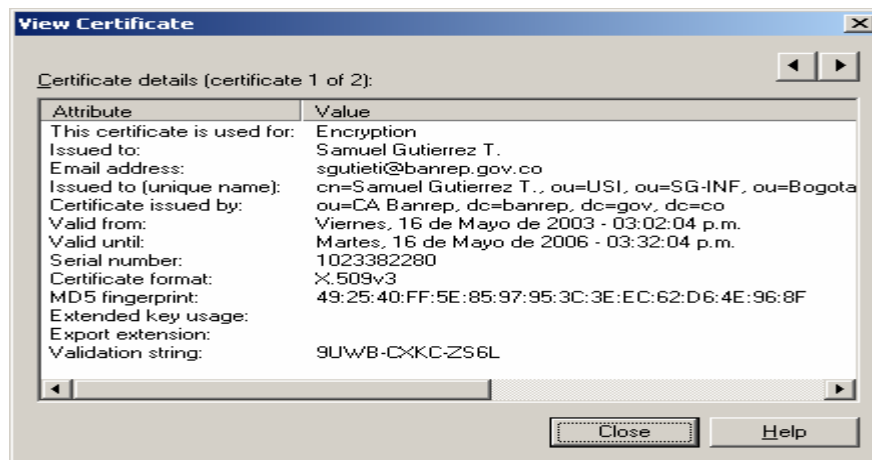
Haga clic en la llave amarilla que aparece en la parte inferior derecha y seleccione la opción “Entrust Options...”

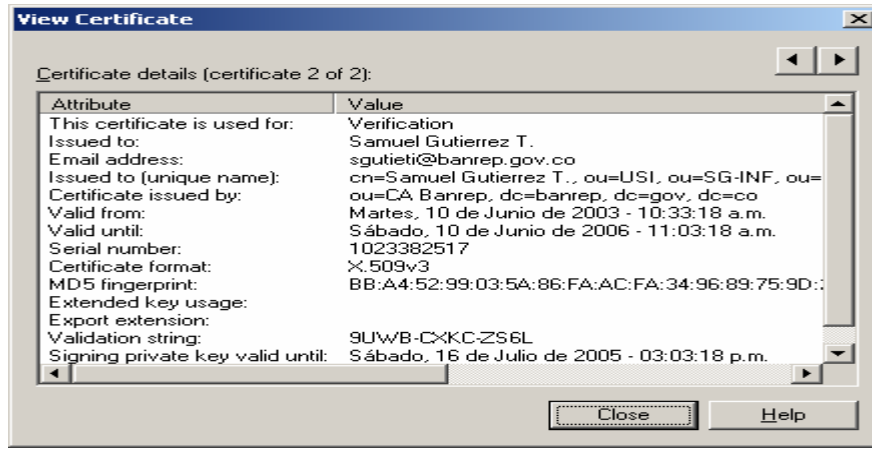


Le aparece una ventana como la siguiente:



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.

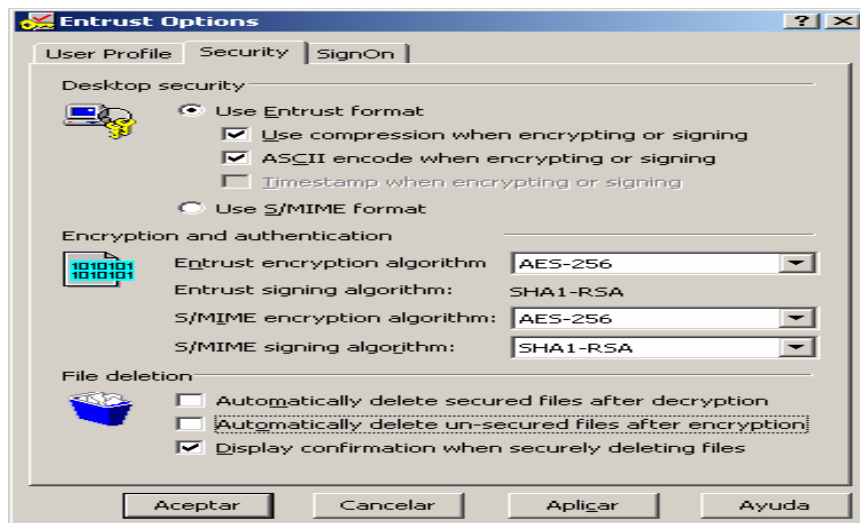
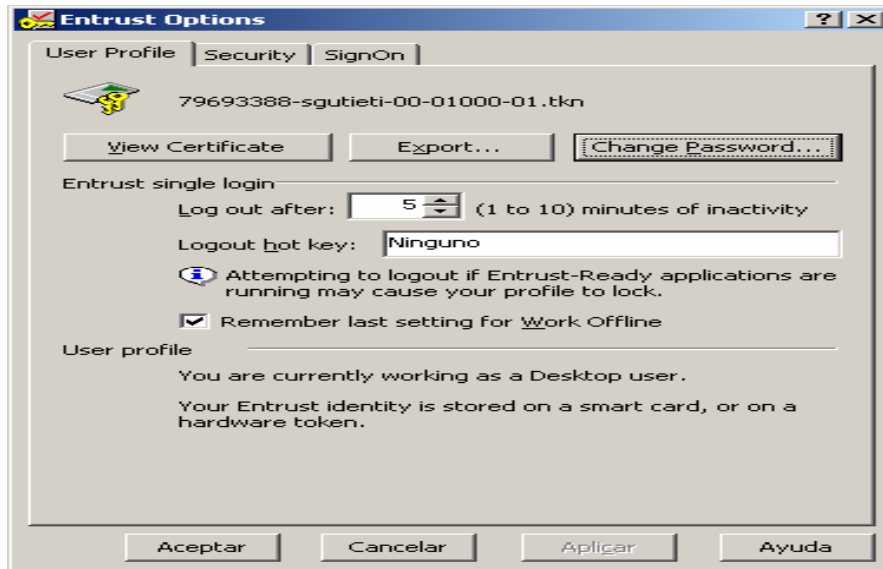
Si el password ha sido usado recientemente le aparecerá una ventana como la siguiente

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:





3 GLOSARIO

PKI: Infraestructura de llaves Públicas basado en conceptos de llaves públicas y privadas.

CA BANREP: Entidad de Certificación cerrada del Banco de la República, autorizada por la SuperIntendencia de Industria y Comercio.

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

Token: dispositivo donde quedará almacenado el Profile

Delegado con responsabilidad administrativa: Delegado de alto nivel en la compañía, el cual cumplirá con la función de administrador de los suscriptores. Es el autorizado para solicitar cualquier cambio en los certificados de los suscriptores de su entidad. Deben existir dos delegados por entidad.

Código de autorización: Una de las partes de la información de activación, utilizada para la generación del certificado, que será entregado por Delegado de la entidad de registro. (ER) en forma personal.

Número de referencia: Una de las partes de la clave, utilizada para la generación del certificado, que será enviado a la cuenta de correo del usuario, por el administrador de la entidad de registro (ER).

Suscriptor: Usuario de la CA BANREP que tiene certificados asignados.