

Banco de la República Bogotá D. C., Colombia

Subgerencia de Informática Departamento de Seguridad Informática

MANUAL INSTALACIÓN SUSCRIPTORES EXTERNOS USI-PN-16

Febrero 2010 Versión #2.0



CONTENIDO

	Pág.
CONTENI	DO3
1	INTRODUCCIÓN4
1.1	Objeto
1.2	ALCANCE
1.3	AUDIENCIA
2	INSTALACIÓN Y CONFIGURACIÓN5
2.1	INSTALACIÓN DEL CLIENTE ENTELLIGENCE
2.2	INSTALACIÓN DEL DISPOSITIVO USB DE ALMACENAMIENTO DE LOS PROFILES7
2.3	CAMBIOS EN EL ARCHIVOS DE HOSTS DE LA MÁQUINA. ; ERROR! MARCADOR NO
DEFINIDO.	
2.4	INICIALIZACIÓN DEL TOKEN
2.5	CAMBIO DE PASSWORD ;ERROR! MARCADOR NO DEFINIDO.
2.6	CREACIÓN O RECUPERACIÓN DEL PROFILE
2.7	CONFIGURACIÓN
3	GLOSARIO



1 INTRODUCCIÓN

1.1 Овјето

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:

• REQUERIMIENTOS BÁSICOS DE HARDWARE

- Hardware mínimo: 2 GB de RAM, procesador de mínimo 2.6Ghz y el espacio en disco que requiera el funcionamiento del sistema operativo más las aplicaciones específicas a instalar.
- Sistema Operativo: Windows XP con SP3. Es necesario que el sistema operativo trabaje con procesamiento a 32 bits.
- Resolución de Monitor: se recomienda trabajar la pantalla a una resolución de 1024 x 768.
- Puertos USB (mínimo dos)

REQUERIMIENTOS BÁSICOS DE SOFTWARE

- Navegador Web Internet Explorer V 7.05, que soporte SSL v.3 y cifrado a 128 bits.
- Plug-in de Java (JRE) instalado versión 1.5
- Antivirus actualizado

•

- Acrobat Reader 5.0 o superior
- Entrust Intelligence 6.1 y Drivers token (software requerido para manejo de PKI que lo proveé El Banco de la República)



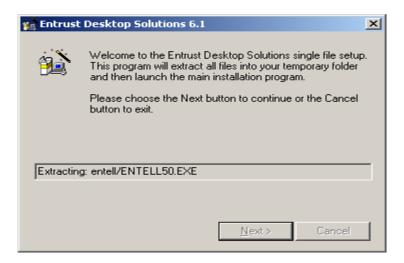
Para realizar la instalación del cliente Entelligence, se debe haber adquirido previamente el software de sitio <u>calima.banrep.gov.co</u> y el archivo instalador es:

CABanrep.exe

Dé doble clic a este archivo y saldrá la siguiente grafica

🙀 Entrust	Desktop Solutions 6.1	×
9	Welcome to the Entrust Desktop Solutions single file setup This program will extract all files into your temporary folder and then launch the main installation program.	,
	Please choose the Next button to continue or the Cancel button to exit.	
	Next > Cancel	

Dé clic en Next



Dé clic en Next



Mis	
ocumentos	Cliente SEBRA 2.2
Mi PC	
62	N
1is sitios de red	Netscape Communicator
1	
Papelera de reciclaje	SIC WEB
\bigotimes	2
Internet Explorer	SOI WEB PRODUCCION
E icrosoft	WinZip
Outlook	winzip
内	6 2 3
Acrobat Reader 5.0	Figuras
	Manual de
@	
ASISTENTE	
2	
Buzón BR	
👧 Inicio 📗	🧔 😒 🛃

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 PROFILES

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

En el archivo Borderless Security BanRep.msi dar doble clic.



😂 D:\Borderless Security BanRep\CompressedInstaller 🗧 🗖 🔀				
<u>A</u> rchivo <u>E</u> dición <u>V</u> er <u>F</u> avoritos	<u>H</u> erra	amientas Ay <u>u</u> da		A.
🔇 Atrás 🔹 🕥 🐇 🏂 Búsqueda 🔊 Carpetas 🛄 🔹				
Dirección 🛅 D:\Borderless Security Bar	nRep\C	CompressedInstaller		🖌 🄁 Ir
Carpetas	×	Nombre	Tamaño	Fecha de modificación
🞯 Escritorio	~	Archivos que están actualmente en e	l CD	
🗉 📋 Mis documentos		Pandadaaa Caasaita Daabaa aasi	7 007 KD	11/02/2010 12:27
🖃 😼 Mi PC		Borderless Security BanRep.msi	7.907 KB	11/02/2010 12:27 a.m.
🗉 🧼 Disco local (C:)				
🖃 💽 BSec7.1 BanRep (D:)				
🖃 🚞 Borderless Security BanRe				
CompressedInstaller	~			
< [>	<		>

Le aparecerá una ventana de instalación

Windows Installer	
Preparing to install	
	Cancel

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





Haga clic en Next

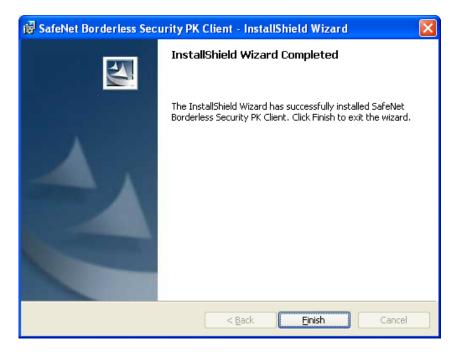
🔀 SafeNet Borderless Security PK Client - InstallShield Wizard	
Ready to Install the Program The wizard is ready to begin installation.	
Click Install to begin the installation.	
InstallShield	Cancel



Dé clic en Install

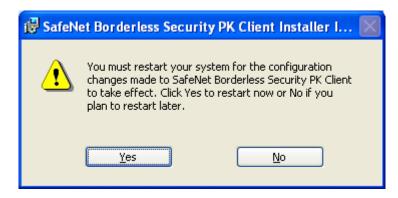
😼 SafeNet	Borderless Security PK Client - InstallShield Wizard 📃 🗖 🔯
-	SafeNet Borderless Security PK Client ram features you selected are being installed.
12	Please wait while the InstallShield Wizard installs SafeNet Borderless Security PK Client. This may take several minutes.
	Status:
InstallShield –	
	< <u>B</u> ack <u>N</u> ext > Cancel

Una vez terminar de copiar los nuevos archivos y driver del token le muestra una ventana como la siguiente:



Haga clic en Finish y le solicitará el reinicio de la máquina para que tome los cambios





Haga clic en Yes

Para verificar que la instalación tuvo éxito, se debió crear el grupo de Programas llamado Safenet y este debe tener una sub carpeta: Borderless Security PK



Adicionalmente, le instala un icono adicional en la barra de estado del sistema operativo:



2.3 INICIALIZACIÓN DEL TOKEN

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

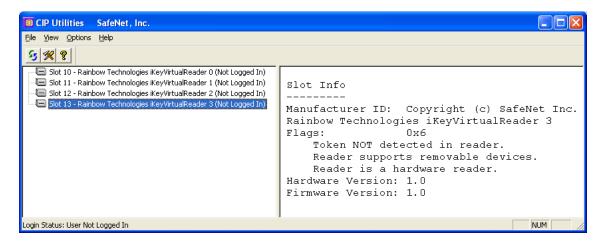
Por inicio, siga la siguiente ruta:

Inicio→Programas

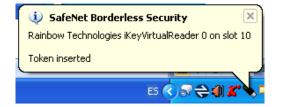


Al hacer clic en SafeNet CIP Utilities, le debe aparecer una ventana como la siguiente:





Al insertar el token en el slot USB, se le muestra la siguiente notificación de reconocimiento del token:

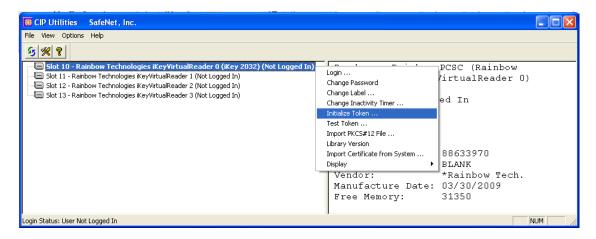


Si vuelve a la ventana del CIP Utilities ya ve que reconoce el token:

EIP Utilities SafeNet, Inc.	
Eile <u>V</u> iew <u>O</u> ptions <u>H</u> elp	
<u>5</u> % ?	
 Slot 10 - Rainbow Technologies iKeyVirtualReader 0 (iKey 2032) (Not Logged In) Slot 11 - Rainbow Technologies iKeyVirtualReader 1 (Not Logged In) Slot 12 - Rainbow Technologies iKeyVirtualReader 2 (Not Logged In) Slot 13 - Rainbow Technologies iKeyVirtualReader 3 (Not Logged In) 	Reader: Rainbow PCSC (Rainbow Technologies iKeyVirtualReader O) Status: Not Logged In Token Overview
	Serial Number: 88633970 Label: BLANK Vendor: *Rainbow Tech. Manufacture Date: 03/30/2009 Free Memory: 31350
Login Status: User Not Logged In	

Al realizar clic derecho sobre el token reconocido por las utilidades. 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

WARNING! Token Initialization - Read carefully before conti ?	×
Token	
Serial Number: 88633970	
Token Label: BLANK	
WARNING!	
Continuing will render the token unusable for cryptoki operations, ALL token objects will be destroyed except as noted below.	
DO NOT remove the token while initialization .	
ALL token keys and certificates will be deleted from the token .	
Exchange keys created by external sources cannot be recreated by this application.	
The Password will be destroyed and replaced with default initial Password	
Note: ONLY the token serial number and label are retained.	
Continue Initialization	

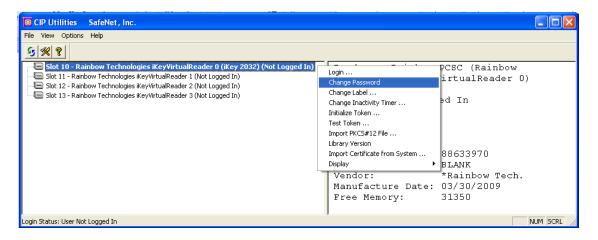
Después de inicializar el Token, el password es la palabra Password#1 y dé clic en OK



Token initialization complete			
٩	New Password = Password#1 Warning! The new Password is a default value and not secure. User should change the Password to a secure value.		
	<u> </u>		

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.

Change Password	X
	BLANK
Old Password	*****
New Password	*********
Reenter New Password	*******
<u>0</u> K	Cancel



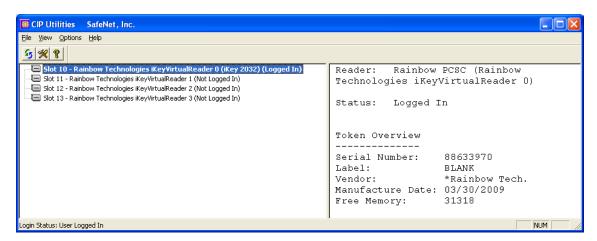
Para probar la nueva clave, realice la operación de Login en el token

EIP Utilities SafeNet, Inc.	
File View Options Help	
<u>5 % 8</u>	
Slot 10 - Rainbow Technologies iKeyVirtualReader 0 (Key 2032) (Not Logged In) Slot 11 - Rainbow Technologies KeyVirtualReader 1 (Not Logged In) Slot 12 - Rainbow Technologies KeyVirtualReader 2 (Not Logged In) Slot 13 - Rainbow Technologies KeyVirtualReader 3 (Not Logged In)	Change Password Change Password Change Label Change Label Initialize Token Test Token Ubrary Version Import Certificate from System Display Vendor: *Rainbow Tech. Manufacture Date: 03/30/2009 Free Memory: 31318
Login Status: User Not Logged In	NUM NUM

Le aparece una ventana como la siguiente:

Token Login		×
Enter Password	*******	
	<u>0</u> K	<u>C</u> ancel

Digite la nueva clave y le debe aparecer una ventana como la siguiente:



Note que en la parte resaltada muestra el estado Logged In.

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



EIP Utilities SafeNet, Inc.		
File View Options Help		
<u>5 % 8</u>		
🔚 🗐 Slot 10 - Rainbow Technologies iKey¥irtualReader 0 (iKey 2032) (Logged In)	Logout	PCSC (Rainbow Technologies
Slot 11 - Rainbow Technologies iKeyVirtualReader 1 (Not Logged In)	Change Password	0)
Slot 12 - Rainbow Technologies iKeyVirtualReader 2 (Not Logged In)	Change Label	
Siot 13 - Kainbow Technologies Keyvirtualkeader 3 (Not Logged In)	Change Inactivity Timer	In
	Initialize Token	
	Test Token	
	Import PKCS#12 File	
	Library Version	
	Import Certificate from System	88633970
	Display 🕨	BLANK
	Vendor:	*Rainbow Tech.
	Manufacture Date:	03/30/2009
	Free Memory:	31318
Login Status: User Logged In		NUM

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

Dé clic en OK

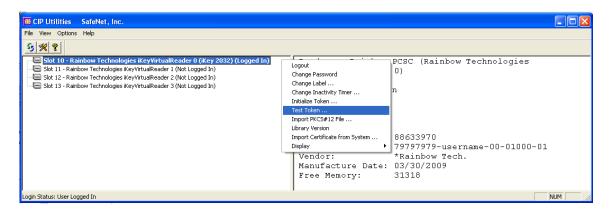
📴 CIP Utilities - Token Label	? 🔀	
Token Label :	<u>0</u> K	
7979-username-00-01000-01	<u>C</u> ancel	

Le aparecerá ya con la información suministrada:

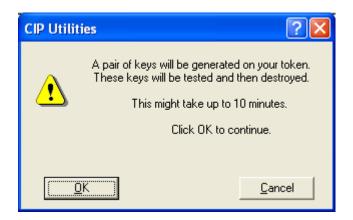
ie ⊻iew Options Help 5 ≪ 😵		
 Slot 10 - Rainbow Technologies iKeyVirtualReader 0 (iKey 2032) (Logged In) Slot 11 - Rainbow Technologies KeyVirtualReader 1 (Not Logged In) Slot 12 - Rainbow Technologies KeyVirtualReader 2 (Not Logged In) Slot 13 - Rainbow Technologies KeyVirtualReader 3 (Not Logged In) 	Reader: Rainbow iKeyVirtualReader Status: Logged : Token Overview Serial Number: Label: Vendor: Manufacture Date: Free Memory:	n 88633970 7979799-username-00-01000-01 *Rainbow Tech.

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

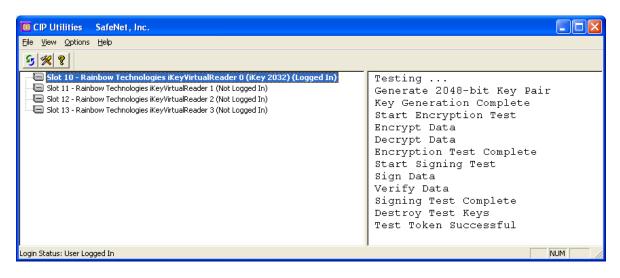




Dé clic en OK. (El proceso puede demorar 10 minutos aprox.)



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





2.4 CREACIÓN O RECUPERACIÓN DEL PROFILE

Siguiendo los procedimientos establecidos por la DPC - Declaración de Prácticas de Certificación (<u>http://www.banrep.gov.co/ca-banrep/documentos/pdc.pdf</u>), 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

👷 Create Entrust Prof	file	×
	Welcome to the Create Entrust Profile Wizard. This wizard will guide you through the process of creating a new profile.	
	< <u>Atrás</u> Siguien <u>te</u> > Cancelar	

Ingrese los datos solicitados y dé clic en siguiente.



🕅 Recover Entrust Profile		×
	Please enter your reference number and authorization code.	
	Beference number: 57727563 Authorization code: D4VT-C7QP-TSTW Hint	
	number: 91480170 and authorization code: CRTJ-8V0R-VFNS).	
	< <u>A</u> trás Siguien <u>t</u> e > Cancela	r

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



🕱 Recover Entrust Pr	ofile	×
	 Where would you like to store your Entrust Profile? On the local computer (work as a Desktop user) Select a folder within which to store your profile: C\ca-banrep\Profiles Browse Store profile on hardware token (card) Slot 10 Slot 10 On the Directory (work as a Roaming user) Hint Your Entrust Profile contains your encryption/decryption keys and your signing/verification keys. The profile can be stored locally on disk, allowing you to work as a Desktop user. It can also be stored in the Directory, secured through the Profile Server. 	
	< <u>A</u> trás Siguien <u>t</u> e > Cancela	r

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.



🕱 Recover Entrust Pr	ofile	×
	Please choose your profile name. It cannot contain \ /: *?'' <> '. Profile name: [79797979-username-00-01000-01] Browse	
	< <u>A</u> trás Siguien <u>t</u> e > Cancela	ar

Dé clic en siguiente.



😭 Recover Entrust Pr	ofile	×
	Entrust is now ready to recover your profile. The following profile will be recovered: C:\ca-banrep\79797979-username-00-01000-01.tkn Click the Next button and your profile will be recovered.	
	< <u>A</u> trás Siguien <u>te</u> > Cancela	ır 🔤

Digite el password que actualmente tiene el token



Empieza el proceso de creación y/o recuperación, esta operación puede tardar varios minutos





Deje la casilla en blanco y dé clic en Finalizar



🕱 Recover Entrust Pr	ofile	×
	Your Entrust profile has been successfully recovered. You may export your Entrust certificates so that non-Entrust users can encrypt for you or so that you can use your Entrust credentials with non-Entrust-Ready applications.	
	< <u>A</u> trás Finalizar Cancel	ar

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.



🖙 Entrust Login			×
	Entru © Copyright 199	IST [®] 4-2004 Entrust. All rights reserved.	_
	<u>P</u> rofile name:		
	P <u>a</u> ssword:	1	
		Work offline	
		El uso de los certificados es exclusivo para comunicaciones con BanRep.	
		OK Cancel <u>H</u> elp	

2.5 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:



😹 Entrust Options 🛛 🤶 🗙
User Profile Security SignOn
79693388-sgutieti-00-01000-01.tkn
View Certificate Export Change Password
Entrust single login
Log out after:
Logout hot key: Ninguno
Attempting to logout if Entrust-Ready applications are running may cause your profile to lock.
Remember last setting for <u>W</u> ork Offline
User profile
You are currently working as a Desktop user.
Your Entrust identity is stored on a smart card, or on a hardware token.
Aceptar Cancelar Aplicar Ayuda

Aquí puede ver los certificados de su Profile.

Attribute	Value
This certificate is used for:	Encryption
Issued to:	Samuel Gutierrez T.
Email address:	sgutieti@banrep.gov.co
Issued to (unique name):	 cn=Samuel Gutierrez T., ou=USI, ou=SG-INF, ou=Bogota
Certificate issued by:	ou=CA Banrep, dc=banrep, dc=gov, dc=co
Valid from:	Viernes, 16 de Mayo de 2003 - 03:02:04 p.m.
Valid until:	Martes, 16 de Mayo de 2006 - 03:32:04 p.m.
Serial number:	1023382280
Certificate format:	X.509v3
MD5 fingerprint:	49:25:40:FF:5E:85:97:95:3C:3E:EC:62:D6:4E:96:8F
Extended key usage:	
Export extension:	
Validation string:	9UWB-CXKC-ZS6L



Vi	ew Certificate	×
1	Certificate details (certificate 2 o	f 2):
	Attribute	Value 🔺
	This certificate is used for:	Verification
	Issued to:	Samuel Gutierrez T.
	Email address:	sgutieti@banrep.gov.co
	Issued to (unique name):	cn=Samuel Gutierrez T., ou=USI, ou=SG-INF, ou=
	Certificate issued by:	ou=CA Banrep, dc=banrep, dc=gov, dc=co
	Valid from:	Martes, 10 de Junio de 2003 - 10:33:18 a.m.
	Valid until:	Sábado, 10 de Junio de 2006 - 11:03:18 a.m.
	Serial number:	1023382517
	Certificate format:	X.509v3
	MD5 fingerprint:	BB:A4:52:99:03:5A:86:FA:AC:FA:34:96:89:75:9D:1
	Extended key usage:	
	Export extension:	
	Validation string:	9UWB-CXKC-ZS6L
	Signing private key valid until:	Sábado, 16 de Julio de 2005 - 03:03:18 p.m. 📃 🗾
	•	
		Close <u>H</u> elp

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.

😎 Change Entrust Pass	vord	×
2000	Welcome to the Change Entrust Password Wizard. This wizard will guide you through the process of changing your current password.	
	Please enter your current password.	
	Current Password:	
	< <u>A</u> trás <u>Siguiente</u> > Cancelar	

Escriba su nuevo password y confírmelo.



🖙 Change Entrust Password 🛛 🛛 💌		
	Please select a new password. New Password: Confirm Password: Your password must satisfy the following rules: must be at least 10 characters long must be less than or equal to 20 characters long must contain an uppercase character must contain a lowercase character must contain a lowercase character must contain a numeric character must not contain a portion of profile name longer than half its length must not repeat a character more than half the length of password must not reuse last 8 passwords	
	< <u>A</u> trás Finalizar Cancelar	

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.

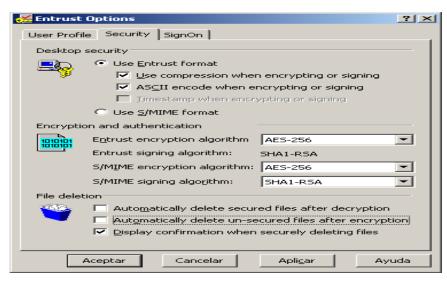
Si no le reporta lo anterior, la acción ha terminado con éxito





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

Entrust Options
User Profile Security SignOn
79693388-sgutieti-00-01000-01.tkn
View Certificate Export
Entrust single login Log out after: 5 🚅 (1 to 10) minutes of inactivity
Logout hot key: Ninguno
Attempting to logout if Entrust-Ready applications are running may cause your profile to lock.
Remember last setting for Work Offline
User profile
You are currently working as a Desktop user.
Your Entrust identity is stored on a smart card, or on a hardware token.
Aceptar Cancelar Apligar Ayuda





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 encripción 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.