

Banco de la República Bogotá D. C., Colombia

Dirección General de Tecnología

Departamento de Seguridad Informática

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

Agosto de 2014

Versión 1

### **CONTENIDO**

1. INTRODUCCIÓN	3
1.1 AUDIENCIA	3
1.2 Alcance	3
2. CONSIDERACIONES ESPECIALES	4
3. GENERACIÓN DE CREDENCIALES PARA EL SUSCRIPTOR	5
3.1 Procedimiento para Inicializar el Token	5
3.1.2 CREACIÓN CERTIFICADO DIGITAL DEL SUSCRIPTOR	
3.1.3 RECUPERACIÓN DE CERTIFICADO DIGITAL PARA SUSCRIPTORES	7
4. GENERACIÓN DE CREDENCIALES PARA PROCESOS AUTOMATICOS Y B2B (BUSINESS TO BUSINESS) 2	4
Certificados Business to Business (B2B):	7
Certificados para Automatización de operaciones criptográficas 2	.8
5. TRANSFORMACIÓN DE CREDENCIALES	1

### 1. INTRODUCCIÓN

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

#### 1.1 Audiencia

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

#### **1.2 Alcance**

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

# 2. CONSIDERACIONES ESPECIALES

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

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

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

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

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

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

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

### 3. GENERACIÓN DE CREDENCIALES PARA EL SUSCRIPTOR

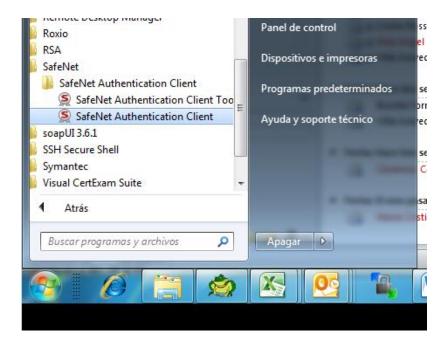
La generación de certificados digitales para el suscriptor contempla dos escenarios, creación (Enroll) y Recuperación (Recovery) del profile, en ambos casos se debe realizar el proceso de inicialización del Token, el cual se describe a continuación:

#### 3.1 Procedimiento para Inicializar el Token

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

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

Se debe ejecutar el cliente "SafeNet Authentication Client" en Inicio  $\rightarrow$  Todos los Programas  $\rightarrow$  Safenet



2. Cuando ingresa, se observa la siguiente pantalla:

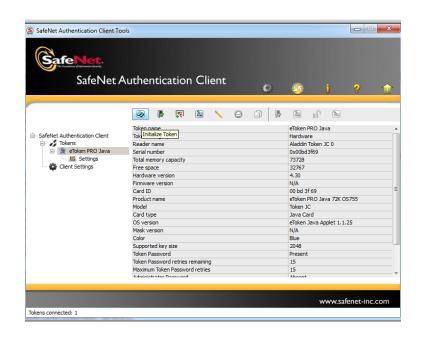
SafeNet Authentication Client Tools				-	• •
SafeNet.					
SafeNet Authenti	cation Client	ö 🐨	;	2	<u></u>
		<u> </u>		8	
	/	Rename Token			
	****	Change Token Password			
	<b>^</b>	Unlock Token			
	$\otimes$	Delete Token Content			
	Q	View Token Information			
	Di:	sconnect SafeNet eToken Vir	tual		
					_
			www.sa	fenet-inc	.com

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

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

SafeNet.	Authentication Client	¢	🔊 i	? 🏦	
	🥺 🖡 🐺 🗎 🔪 🖨 🗄				
	Token name		eToken PRO Java		
∃. SafeNet Authentication Client	Token category		Hardware		
🚊 🧳 Tokens	Reader name		Aladdin Token JC 0		
🗐 🤵 eToken PRO Java	Serial number		0x00bd3f69		
🛄 Settings	Total memory capacity		73728		
🔤 📸 Client Settings	Free space		32767		
	Hardware version		4.30		
	Firmware version		N/A		
	Card ID		00 bd 3f 69		
	Product name		eToken PRO Java 72K OS755		
	Model		Token JC		
	Card type		Java Card		
	OS version		eToken Java Applet 1.1.25		
	Mask version		N/A		
	Color		Blue		
	Supported key size		2048		
	Token Password		Present		

Haga clic en el icono "Inicializar Token"



4. En la siguiente ventana de inicialización del token,

S Token Initialization	×
GafeNet. SafeNet Authentication Client	
Token Name: My Token	
Image: Set Token Password:       Image: Set Token Password:       Logon retries before token is locked:       10         Confirm:       Image: Set Token Password:       Image: Set Token Password:       10	×
Set Administrator Password: Confirm: Logon retries before token is locked: 15 Note: An Administrator Password will be needed to unlock the token.	×
Additional Settings	
<ul> <li>Token Password must be changed on first logon</li> <li>Advanced</li> </ul>	
Current Language: ES	
Start Close	



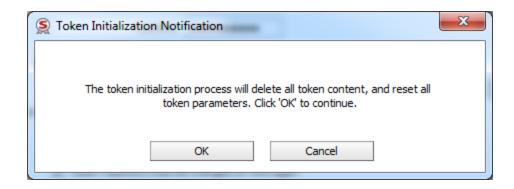
En este paso debemos indicar el Nombre del Token, el cual debe seguir la siguiente estructura: "Cedula de ciudadanía –Login– tipo de sector -codigoEntidad – código de ciudad".

Ejemplo: 1070945805-cramirra-00-01000-01

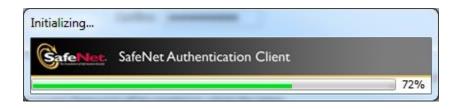
Se debe establecer el password en la Opción "*Establecer Contraseña*" o "*Set Token Password*" y confirmarlo.

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

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



Se inicia la "inicialización del Token".



Al terminar debe presentar un mensaje de inicialización exitosa.

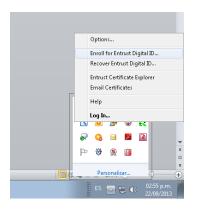


# 3.1.2 Creación Certificado Digital del Suscriptor

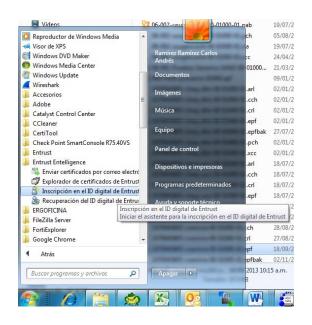
Para realizar este proceso se debe contar con la información de activación (el código de autorización y número de referencia suministrados por el Banco de la República) y con acceso a WSEBRA, y verificar la sección 2 (*Consideraciones Especiales*). El procedimiento de solicitud de certificado se define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

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

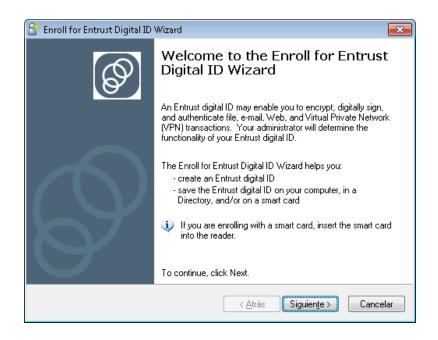
*Opción 1*: En la parte inferior izquierda del escritorio de Windows hacer clic derecho sobre el icono de ESP <sup>38</sup>, procedemos a seleccionar la opción *Enroll for Entrust Digital ID*.



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



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

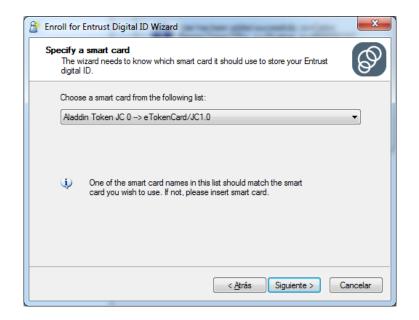


Aparece la siguiente ventana, ingresar el código de autorización y numero de referencia provistos por el Banco de la República y dar clic en "Siguiente"

😤 Enroll for Entrust Digital ID Wizard	<b>-X</b> -
Specify your activation codes The wizard needs to know your activation codes so that it can enroll for an Entrust digital ID that is right for you.	Ø
Enter your reference number and authorization code:	
Reference number:	
Authorization code:	
Your administrator should have provided these values to you (for example, reference number: 91480170 and authorization code: CRTJ-8V0R-VFNS).	
< <u>A</u> trás Siguien <u>t</u> e > Ca	ancelar

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

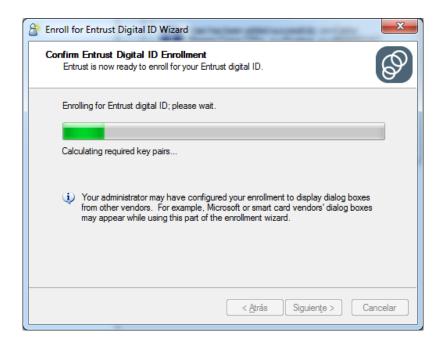
Hacer clic en "Siguiente".



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

C Enroll for Entrust Digital ID Wizard
Confirm Entrust Digital ID Enrollment Entrust is now ready to enroll for your Entrust digital ID.
Click the Next button to enroll for your Entrust digital ID.
Your administrator may have configured your enrollment to display dialog boxes from other vendors. For example, Microsoft or smart card vendors' dialog boxes may appear while using this part of the enrollment wizard.
< <u>A</u> trás Siguiente > Cancelar

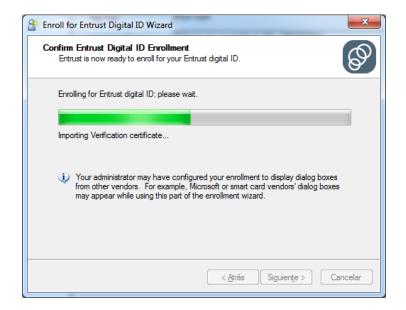
Se iniciará el proceso de Enroll del certificado.



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

S Token Logon	
GafeNet. SafeNet Auth	entication Client
Enter the Token Password.	
Token Name:	1070945805-cramirra-00-01000-01
Token Password:	1
	Current Language: ES
	OK Cancel

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



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



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

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

	hentication Client Tools				×
Safe	SafeNet Authenticatic	on Client	ی چ	i?	
	1070945805-cramii 1070945805-cramira-00-01000-01 (A	Jaddin Token 1C 01	Rename Token		
	10703 1000 Calmina 00 01000 C1 [*	****	Change Token Password		
			Unlock Token		
		$\propto$	Delete Token Content		
		2	View Token Information		
		Dis	connect SafeNet eToken Virtual		
			۷	www.safenet-inc	.com

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

	Authenticatior		¢ 👳	<b>i ?</b> 1
	Issued To	Issued By	Expiration Date	Purposes
🖃 🧳 Tokens	Carlos RamirezTo	CA Banrep	10/22/2016	All application policies
<ul> <li>         1070945805-cramirr      </li> <li>         III User certificates     </li> </ul>		CA Banrep	10/22/2016	All application policies
Lent Settings				

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

<u>de Certificación - CA BANREP'' (BR-3-598-0)</u>. Información que se consulta realizando doble clic sobre el certificado.

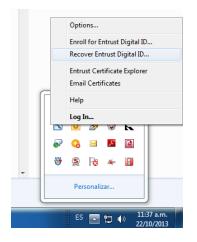
<b>SafeNet</b> SafeNet A	suthenticatior	n Client				
			¢ 👳	i ?		
						Certificado
SafeNet Authentication Client Tools	Issued To	Issued By	Expiration Date	Purposes		General Detalles Ruta de certificación
🗄 🧳 Tokens	🛒 Pruebas Token Su		lunes, 10 de j <mark>u</mark> lio de 2.	All application polici	es	
Token ESP Vigente	Pruebas Token Su		domingo, 17 de mayo			Información del certificado
Pruebas Toke	Pruebas Token Su	CA Banrep	domingo, 30 de julio d.	. All application polici	es 🖉	Este certif. está destinado a los siguientes propósitos:
Gient Settings						• 1.3.6.1.4.1.14256.1.2.1     • Todas las directivas de la aplicación     * Para ver detalles, consulte la declaración de la entidad de ce
						Emitido para: Pruebas Token Suced
					-	
						Emitido por: CA Banrep
						Válido desde 10/ 07/ 2014 hasta 10/ 07/ 2017
				www.safenet	-inc.com	
ser certificates						Instalar certificado Declaración del emisor
INA Almacan da Cantileados	Knowledge Xpart	SUCED Poss	voroi Sale - informe .cc. pr.	. UsuanoAddad PKlixt	Enero2013	Obtener más información acerca de <u>certificados</u>
Cantification						

# 3.1.3 Recuperación de Certificado Digital para Suscriptores

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

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

**Opción 1**: Nos dirigimos a la parte inferior izquierda del escritorio de Windows y de clic derecho sobre el icono de ESP  $\overset{\mbox{\ensuremath{\mathscr{B}}}}{\longrightarrow}$ , procedemos a seleccionar la opción **Recover Entrust Digital ID**.



**Opción 2**: Diríjase a Inicio  $\rightarrow$  Todos los programas  $\rightarrow$  Entrust Entelligence  $\rightarrow$  "**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"

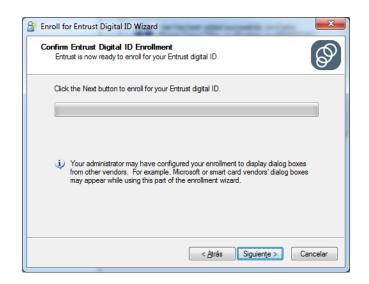
👌 Enroll for Entrust Digital I	D Wizard	×
Specify your activation The wizard needs to kr digital ID that is right for	now your activation codes so that it can enroll for an Entrust	Ø
Enter your reference nu	imber and authorization code:	
<u>R</u> eference number:		
Authorization code:		
	should have provided these values to you (for example, 91480170 and authorization code: CRTJ-8V0R-VFNS).	
	< <u>A</u> trás Siguien <u>t</u> e > Ca	ancelar

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

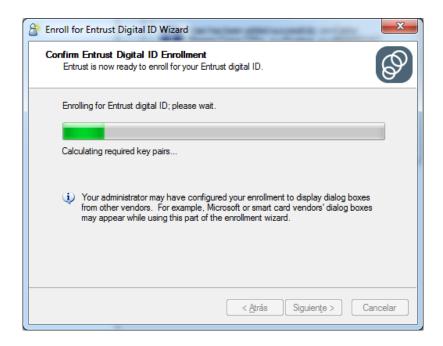
Seleccionar "Siguiente".

\left Enroll for	Entrust Digital ID Wizard
	a smart card izard needs to know which smart card it should use to store your Entrust ID.
Choos	e a smart card from the following list:
Aladd	lin Token JC 0> e TokenCard/JC1.0 🔹
(j)	One of the smart card names in this list should match the smart card you wish to use. If not, please insert smart card.
	< <u>A</u> trás Siguiente > Cancelar

Seleccionar "Siguiente"



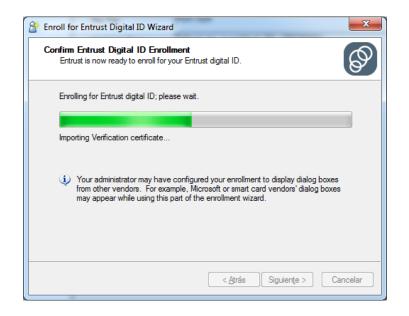
Al seleccionar "Siguiente" comenzara el proceso de Enroll del certificado.



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

S Token Logon	×
SafeNet SafeNet Auth	entication Client
Enter the Token Password.	
Token Name:	1070945805-cramirra-00-01000-01
Token Password:	1
	Current Language: ES
	OK Cancel

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



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

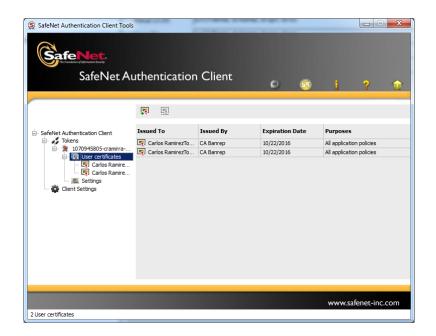


*Nota:* Si la creación del certificado no termino correctamente, debe verificar que se encuentra en línea a través de WSEBRA, si el problema continúa debe contactar a Soporte Informático del Banco de la República.

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

	SafeNet Auth	entication Client	ø	<u>s</u>	i	?	
2	1070945805-crami	ra-00-01000-01 [Aladdin Token JC 0]	Renar	ne Token			
	10/05/0000 0000	****	Change To	ken Password			
			Unloc	k Token			
		$\otimes$	Delete To	ken Content			
		Q	View Toker	Information			
			)isconnect Safe	Net eToken Virti	ual		

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

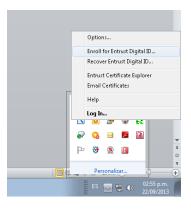


# 4. GENERACIÓN DE CREDENCIALES PARA PROCESOS AUTOMATICOS Y B2B (BUSINESS TO BUSINESS)

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

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

Opción 1: En la parte inferior izquierda del escritorio de Windows hacer clic derecho sobre el icono de entrust <sup>38</sup> y seleccionar la opción Enroll for Entrust Digital ID.



**Opción 2**: Ir a Inicio  $\rightarrow$  Todos los programas  $\rightarrow$  Entrust Entelligence  $\rightarrow$  "Inscripción en el ID Digital de Entrust".

Vídeos		06-002-usur	0-01000-01_pab	19/07/
💟 Reproductor de Windows Medi	ia 🔺		ch	05/08/
< Visor de XPS		States and states and	a	19/07/
Windows DVD Maker		Ramírez Ramírez Ca Andrés	irlos :c	24/04/
😇 Windows Media Center		The local division of	01000	21/03/
Windows Update		Documentos	and the second se	09/01/
Wireshark		Imágenes	.arl	02/01/
Accesorios	=	Imagenes	.cch	02/01/
Adobe		Música	.crl	02/01/
Catalyst Control Center			epf	02/01/
CCleaner		Equipo	.epfbak	27/07/
Certi I ool Check Point SmartConsole R75	101/0		.pch	02/01/
Entrust	.40V5	Panel de control		0.27 0.27
Entrust Entelligence			xcc	02/01/
Entrust Entelligence Enviar certificados por corre	o electri	Dispositivos e impre		18/07/
Explorador de certificados d			.cch	18/07/
Inscripción en el ID digital d		Programas predeter	minados <mark>.crl</mark>	18/07/
Recuperación del ID digital		Avuda v soporte téc	.epf	18/07/
ERGOFICINA FileZilla Server	Inscripción	n en el ID digital de Ent		ntrust
FileZilla Server			tch	28/08/
Google Chrome	-		ri ana	27/08/
	100		pf	18/09/
4 Atrás			epfbak	02/11/
Buscar programas y archivos	٩	Apagar 🕨	2013 10: B	
	8		w w	

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"

👌 Enroll for Entr	rust Digital ID Wizard		<b>-X</b>
The wizar	activation codes d needs to know your activati hat is right for you.	on codes so that it can enroll for an Entrust	Ø
Enter your	reference number and author	rization code:	
<u>R</u> eference	number:		
Authorizati	on code:		
		vided these values to you (for example, authorization code: CRTJ-8V0R-VFNS).	
		< <u>Atrás</u> Siguien <u>t</u> e > Ca	ancelar

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).

Create Entrust Security Store
Entrust Security Store Location The Entrust security store is a protected file that contains your cryptographic data.
This wizard helps you create an Entrust security store for your digital ID.
Select a folder for your Entrust security store:
C.\ca-banrep\Profiles\
< <u>Atrás</u> Siguiente > Cancelar

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

A Create Entrust Security St	ore
Entrust Security Store P Password rules help ens security store.	hassword nure you select a secure password to protect your Entrust
Please enter a password	to protect your Entrust security store.
Password:	•••••
Confirm Password:	•••••
Your password must sati	sfy the following rules:
🛷 must be at least	12 characters long
🛷 must contain a n	on alphanumeric character
🛷 must contain an	uppercase character
🛷 must contain a lo	wercase character
🛷 must contain a n	umeric character
must not contain	a portion of security store name longer than half its length
must not repeat a	a character more than half the length of password
	< Atrás Finalizar Cancelar

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

#### **Certificados Business to Business (B2B):**

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

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

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

Ejemplo: SB-8600052167-CUD-PRU

### Certificados para Automatización de operaciones criptográficas

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

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

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

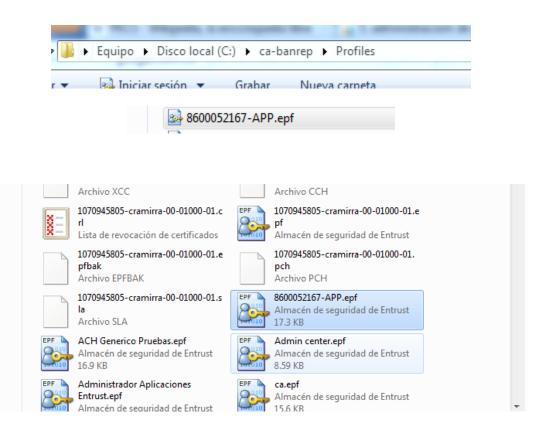
Ejemplo: 8600052167-CUD-PRU

👌 Create Entrust	Security Store
	ity Store Name quely identifies your Entrust security store.
Please ente	r a name for your Entrust security store.
Name:	8600052167-APP
Your Entrus	t security store name must not contain the following characters: ?"<> "
	< Atrás Siguiente > Cancelar

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

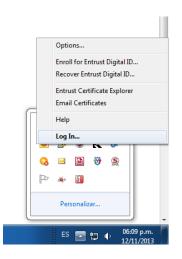


Por defecto ubicación del profile es la ruta *c:\ca-banrep\profiles\* o en la ruta establecida por el usuario en el proceso mencionado anteriormente, el archivo tendrá el nombre que el usuario haya establecido en el proceso de creacion y extension .epf.



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  $\overset{38}{}$  y seleccionar la opción *Log In...* 



En el botón "Browse" seleccionamos el profile correspondiente.



Ingrese la contraseña para hacer el Login.

# 5. TRANSFORMACIÓN DE CREDENCIALES

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

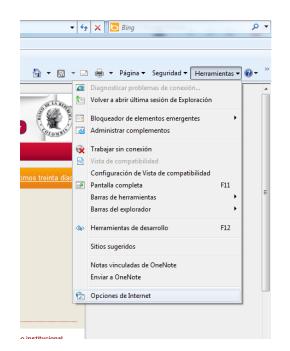
Después de realizar la creación del profile se procede a realizar la transformación de credenciales, a continuación se describe el procedimiento para convertir el profile en formato Entrust Archive (archivo con extensión .epf) en formato PKCS#12 (archivo con extensión .p12 o .pfx) o en formato Java key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

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

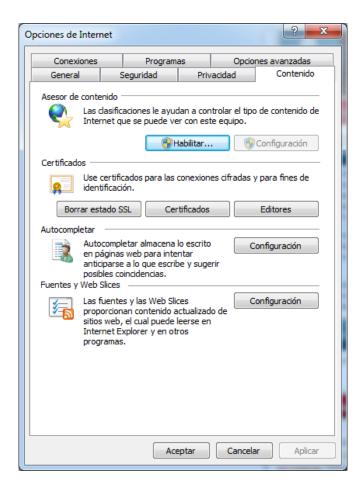
Ingresar al navegador "Internet Explorer".



Ir a la sección Herramientas.



En Herramientas, ir a la sección Contenido  $\rightarrow$  Certificados.



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

tificados		ingeneration of the second	I deserve	and the second sec
ropósito pl	anteado: <too< th=""><th>dos&gt;</th><th></th><th></th></too<>	dos>		
Personal	Otras personas	Entidades de o	certificación intern	nedias Entidades de certificaci
Emitido	para	Emitido por	Fecha de e	Nombre descriptivo
<b>5860</b>	052167 APP	CA Banrep	13/11/2015	860052167 APP's Verificati
860	052167 APP	CA Banrep	13/11/2015	860052167 APP's Encryptio
Alex	ander Prada P	CA Banrep	09/10/2016	Alexander Prada Perez's V
Alex	ander Prada P	CA Banrep	09/10/2016	Alexander Prada Perez's E

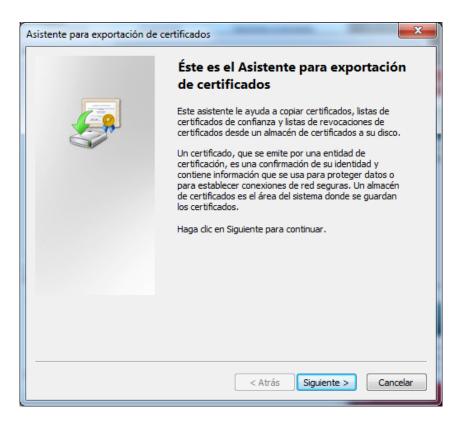
Serán visibles dos certificados, uno utilizado para encriptar y otro para verificación de firma, por cada llave se debe realizar el proceso de exportar las llaves.

Exportar Llave Privada de Verificación de Firma:

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

Emitido para	Emitido por	Fecha de e	Nombre descriptive	0	*
🕞 860052167 APP	CA Banrep	13/11/2015	860052167 APP's	Verification Certi	=
🔄 860052167 APP	CA Banrep	13/11/2015	860052167 APP's B	Encryption Certi	
🔄 Alexander Prada	CA Banrep	09/10/2016	Alexander Prada P	erez's Verificatic	
🔄 Alexander Prada	CA Banrep	09/10/2016	Alexander Prada P	erez's Encryptio	
🔄 Banco de la Repu	AC TEST	13/09/2014	<ninguno></ninguno>		
BR Funcion Public	AC TEST	25/10/2014	<ninguno></ninguno>		
BREntidadPruebas1	AC TEST	23/08/2014	<ninguno></ninguno>		
BREntidadPruebas2	AC TEST	23/08/2014	<ninguno></ninguno>		Ŧ
•				۴.	
Importar Exportar Propósitos planteados del <todos></todos>		litar	Ор	ciones avanzada	as
Obtener más información a	cerca de <u>certi</u>	ficado <u>s</u>		Cerra	ar

Se debe hacer click en siguiente.



En la siguiente sección es indispensable seleccionar la opción "Exportar la llave privada"

Ext	portar la clave privada
	Puede elegir la exportación de la clave privada con el certificado.
	Las daves privadas se protegen con contraseñas. Si desea exportar la dave 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
Má	s información acerca de la <u>exportación de claves privadas</u>

Se debe seleccionar las opciones mostradas a continuación:

Fo	ormato de archivo de exportación Los certificados pueden ser exportados en diversos formatos de archivo.
	Seleccione el formato que desea usar:
	🔘 DER binario codificado X.509 (.CER)
	🔿 X.509 codificado base 64 (.CER)
	Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)
	Incluir todos los certificados en la ruta de acceso de certificación (si es posible)
	<ul> <li>Intercambio de información personal: PKCS #12 (.PFX)</li> </ul>
	📝 Incluir todos los certificados en la ruta de acceso de certificación (si es posible)
	Eliminar la clave privada si la exportación es correcta
	Exportar todas las propiedades extendidas
	O Almacén de certificados en serie de Microsoft (.SST)
Má	ás información acerca de los <u>formatos de archivo de certificado</u>
	< Atrás Siguiente > Cancelar

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.

Contrasei Para conti	a mantener la seguridad, debe proteger la dave privada por medio de una aseña.
Escri	pa y confirme una contraseña.
C	ontraseña:
	••••••
Б	scribir y confirmar contraseña (obligatorio):
	•••••
	< Atrás Siguiente > Can

Proceder a establecer un nombre al archivo.

sister	nte para exportación de certificados	3
An	c <b>hivo que se va a exportar</b> Especifique el nombre del archivo que desea exportar	
		_
	Nombre de archivo:	
	Examinar	
	< Atrás Siguiente > Cancelar	ר
		۲

Especifique el nombre del archivo que desea exportar Nombre de archivo: C:\ca-banrep\Profiles\P12-Banrep\P12-Firma-8600052167.pfx Examinar	Especifique el nombre del archivo que de	sea exportar	
C:\ca-banrep\Profiles\P12-Banrep\P12-Firma-8600052167.pfx Examinar	Nombre de archivo:		
	C:\ca-banrep\Profiles\P12-Banrep\P12-	Firma-8600052167.pfx	Examinar
< Atrás Siguiente > Cance			

Pulsamos Finalizar para terminar el proceso de exportación.

Asistente para exportación de	certificados
	Finalización del Asistente para exportación de certificados
	El Asistente para exportación de certificados finalizó correctamente.
	Especificó la siguiente configuración:
	Nombre de archivo Exportar claves Incluir todos los certificados en la ruta de certificación Formato de archivo
	< Atrás Finalizar Cancelar

Verificamos que la exportación se realizo correctamente.

Asistente para exportación de certifica	×
La exportación se realizó correctamente.	
Aceptar	

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

ersonal	Otras personas	Entidades	de certificación in	termedias Entidades de certificad
	ou do personad	Enddddeb		
Emitida	para	Emitido por	Fecha de e	Nombre descriptivo
<b></b> 860	052167 APP	CA Banrep	13/11/2015	860052167 APP's Verification Cer
<b>160</b> 860	052167 APP	CA Banrep	13/11/2015	860052167 APP's Encryption Cer
🔄 Ale:	xander Prada	CA Banrep	09/10/2016	Alexander Prada Perez's Verificat
🔄 Ale:	xander Prada	CA Banrep	09/10/2016	Alexander Prada Perez's Encrypti
🔄 Ban	co de la Repu	AC TEST	13/09/2014	<ninguno></ninguno>
🔄 BR	Funcion Public	AC TEST	25/10/2014	<ninguno></ninguno>
🔄 BRE	ntidadPruebas1	AC TEST	23/08/2014	<ninguno></ninguno>
🔄 BRE	intidadPruebas2	AC TEST	23/08/2014	<ninguno></ninguno>
•			III	4
nportar	Exportar	Q	uitar	Opciones avanza
	s planteados del	contificando		
· ·		ceruncado		
<todos></todos>				
				Ver

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

🏉 Guardar como				×
OO • D • Eq	uipo + Disco local (C:) + ca-banrep + Profiles + P	12-Banrep 👻	€ Buscar P12-Bar	nrep 🔎
Organizar 🔻 N	ueva carpeta			:≕ ▼ 🕡
🔆 Favoritos	^ Nombre	Fecha de modifica	Тіро	Tamaño
<ul> <li>Descargas</li> <li>Escritorio</li> <li>Sitios reciente</li> <li>config</li> <li>Vídeos</li> </ul>	P12-Firma-8600052167.pfx E	12/11/2013 06:16	Personal Informati	7 KB
➢ Bibliotecas ➢ Documentos ➢ Imágenes ∂ Música ☑ Vídeos				
Nombre:	P12-Cifrado-8600052167.pfx			•
Tipo:	Intercambio de información personal (*.pfx)			•
Ocultar carpetas			Guardar	Cancelar

chivo que se va a exportar Especifique el nombre del archivo qu	e deces exportar	
Especinque el nombre del archivo qu	le desea exportar	
Nombre de archivo:		
C:\ca-banrep\Profiles\P12-Banrep\	P12-Cifrado-8600052167.pfx	Examinar

Asistente para exportación de	e certificados
	Finalización del Asistente para exportación de certificados
	El Asistente para exportación de certificados finalizó correctamente.
	Especificó la siguiente configuración:
	Nombre de archivo
	Exportar daves Incluir todos los certificados en la ruta de certificación Formato de archivo
	• Þ
	< Atrás Finalizar Cancelar

Asistente para exportación de certifica	
La exportación se realizó correctamente.	
Aceptar	

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

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

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

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

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

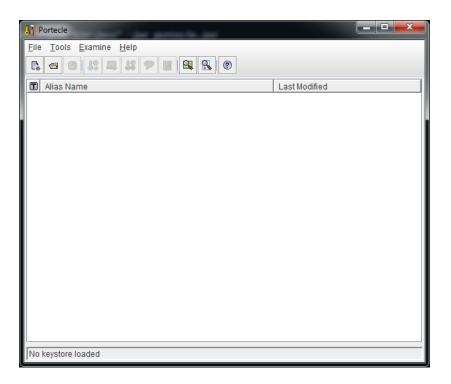
🖉 📿 🗢 📔 🕨 Equipo 🕨 Disco local	(C:) → ca-banrep → Profiles → P12-Banrep	-	-		
Organizar 👻 Incluir en biblioteca 🔻	<ul> <li>Compartir con</li></ul>	rpeta			
🖌 🚖 Favoritos	Nombre	Fecha de modifica	Тіро	Tamaño	
📕 Descargas	😼 P12-Cifrado-8600052167.pfx	12/11/2013 06:17	Personal Informati	7 KB	
Escritorio	澷 P12-Firma-8600052167.pfx	12/11/2013 06:16	Personal Informati	7 KB	
Sitios recientes					
🎍 config 🔣 Vídeos					
4 🚔 Bibliotecas					

Procedemos a usar el Software "Portecle":

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

Para abrir el sofware hacemos doble click en "portecle.jar", según se muestra a continuación:

		Terrings in others.	-
:) > portecle-1.7			
r Nueva carpeta			
Nombre	Fecha de modifica	Тіро	Tama
📓 bcprov.jar	11/01/2010 06:22 a	Executable Jar File	1
LICENSE.bcprov.txt	17/01/2011 08:02	Archivo TXT	
LICENSE.txt	24/03/2010 01:34 a	Archivo TXT	
NEWS.txt	23/01/2011 12:47	Archivo TXT	
portecle.desktop	27/04/2010 12:07 a	Archivo DESKTOP	
🔊 portecle.ico	01/06/2009 11:26	Icono	
📓 portecle.jar	23/01/2011 01:04	Executable Jar File	
portecle.p Tipo: Executable Jar File	01.000.11:26	Imagen PNG	
README.t Fecha de modificación: 23/01/2		Archivo TXT	



Se selecciona "New Keystore"

👫 Portecle				
<u>File Tools Examine H</u> elp		_		
🕞 <u>N</u> ew Keystore	Ctrl-N	8 🕵 😨		
Open Keystore File	Ctrl-O		Last Modified	1
Open CA Certs Keystore	Ctrl-Y		Edot modified	1
Save Keystore	Ctrl-S			
Bave Keystore As		_		
➡ <u>1</u> 8600052167.p12				
2 Vigente-Certicamara.p12 3 GenericoPruebas.jks				
GenericoPruebas.jks <u>4</u> SB_EntidadPruebas1.jks				
		-		
Create a new keystore				-
jorodio a non nojotoro	_			

De las alternativas presentadas debe escoger tipo JKS.

New Keystore Type				
Select the type of the new Keystore:				
<u>UKS</u> <u>PKCS</u> #12				
⊖ J <u>C</u> EKS				
<ul> <li>JK<u>S</u> (case sensitive)</li> <li>BKS</li> </ul>				
O <u>g</u> kr				
OK Cancel				

👫 [Untitled] - Portecle			
<u>File Tools Examine H</u>	elp		
C: < C 👫 📮	<b>1</b> 9 <b>1 1 1 1</b>		
Alias Name	Import Key Pair (Ctrl-K)	Last Modified	
Import a key pair into the lo	aded keystore		

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

👫 Choose Key Pair File	for Import	×
Buscar en: 📑 P12	-Banrep	
P12-Cifrado-860		
😫 P12-Firma-8600	052167.pfx	
Nombre de archivo:	P12-Firma-8600052167.pfx	
Archivos de <u>t</u> ipo:	Key Pair Files (*.p12;*.pfx;*.pem)	▼
		Choose Cancelar

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

PKCS #12 Keystore Password				
Enter Password:				
OK Cancel				

Import Key Pair	X
Select a key pair for import:	
4 18 18 0 T+hDS22sSgafRY0BCIAFHw==	
Algorithm: RSA (1.024 bits) Certificate Details	
OK Cancel	

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

Key Pair Entry Alias
Enter Alias: 4 18 18 0 t+hds22ssgafry0bcia
OK Cancel
Key Pair Entry Alias
Enter Alias: firma

El sistema solicitará una contraseña para este alias.

Key Pair Entry Password				
Enter New Password:	•••••			
Confirm New Password:	•••••			
ОК	Cancel			



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

Choose Key Pair File	for Import	×	
Buscar en: 📑 P12	-Banrep	A C C B C	
P12-Cifrado-860			
f P12-Firma-8600	P12-Firma-8600052167.pfx		
Nombre de archivo:	P12-Cifrado-8600052167.pfx		
Archivos de <u>t</u> ipo:	Key Pair Files (*.p12;*.pfx;*.pem)	-	
		Choose Cancelar	

PKCS #12 Keystore Password				
Enter Password:				
OK Cancel				

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

Key Pair Entry Alias		
Enter Alias: cifrado		
OK Cancel		

Key Pair Entry Password				
Enter New Password:	•••••			
Confirm New Password:	•••••			
ОК	Cancel			

Im	port Ke	ey Pair	x
(	i	Key Pair Import Successful.	
		Aceptar	

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

37 [Untitled] - Portecle	
<u>File Tools Examine H</u> elp	
📑 New Keystore Ctrl-N	
Open Keystore File Ctrl-O	
Open CA Certs Keystore Ctrl-Y	Last Modified 12/11/2013 06:26:39 PM COT
🖺 Save Keystore Ctrl-S	12/11/2013 06:25:38 PM COT
B Save Keystore As	
🚭 <u>1</u> 8600052167 APP.jks	
🚭 <u>2</u> 8600052167 APP	
🗟 <u>4</u> Vigente-Certicamara.p12	
Exit	
Save the loaded keystore to disk	

Set Keystore Password					
Enter New Password:	•••••				
Confirm New Password:	•••••				
ОК	Cancel				

Save Keystore As		×
Guardar en: Guardar en:	S-Banrep	
Nombre de archivo:	8600052167-APP.jks	
Archivos de <u>t</u> ipo:	Java Keystore Files (*.jks;cacerts)	•
		Guardar Cancelar

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

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

Organizar ▼ Incluir en biblioteca ▼ Compartir con ▼ Grabar Nueva carpeta					
🙀 Favoritos	Nombre	Fecha de modifica	Тіро	Tamaño	
📜 Descargas	8600052167-APP.jks	12/11/2013 06:29	Archivo JKS	7 KB	
🧮 Escritorio					
🗐 Sitios recientes					
🌗 config					
📕 Vídeos					

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