



*Banco de la República
Colombia*

Guía de creación o recuperación de Identidades Electrónicas virtuales– Noviembre de 2021

A continuación, se presentan dos alternativas de uso de Firma Electrónica emitidas por el Banco de la República, para aquellas entidades que tengan problemas al usarlas dadas las restricciones técnicas en el escenario de trabajo remoto por la contingencia del COVID-19.

Solicitamos realizar las configuraciones aquí descritas y si tiene alguna dificultad, por favor escriba un correo a la cuenta MesadeAyuda@banrep.gov.co indicando el error que presenta, nombre y número de contacto para que uno de nuestros ingenieros de soporte se comunique con usted y le ayude a superar el inconveniente.

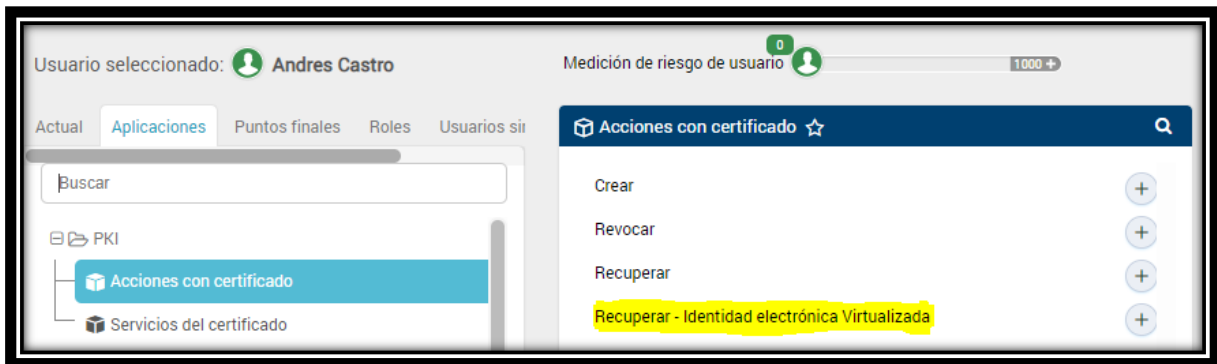
La primera alternativa aplica solo para el caso de servicios como Master-Antares cuyo acceso es directamente a través de Internet. El usuario puede utilizar la firma electrónica en el token criptográfico y lo único que requiere es instalar el driver del token en el computador de su casa. El instalador lo puede encontrar en el portal <https://caribe.banrep.gov.co/emisor> en la ruta Descargas SUCED, PKI, SAC, Instalador SAC 10.6.

Para los usuarios de los sistemas ofrecidos en el portal SEBRA del Banco de la República, se ofrece una segunda alternativa; cabe anotar que la solución planteada no se concibe como una solución masiva. Esta alternativa deberá ser adoptada por cada entidad de forma controlada y el Banco de la República la atenderá por demanda. Dicha medida es de tipo transitorio, de manera que una vez se supere esta situación de contingencia, los usuarios que se acogieron a este esquema deberán retornar al esquema tradicional, lo que implica una nueva recuperación y configuración de sus certificados en los dispositivos criptográficos.

Esta estrategia consiste en habilitar la Firma Electrónica en “tokens de tipo virtual”, apalancados en la infraestructura del Banco de la República, de modo tal que no se dependa del acceso físico al token para realizar las operaciones de aseguramiento de archivos requeridas (firmar, cifrar, verificar, descifrar). Para poder cambiar al nuevo esquema

ofrecido, se requiere solicitar la recuperación en formato Virtual de la Firma Electrónica digital que hoy día se almacena en un token criptográfico, para que una vez efectuado este proceso pueda trabajarlo en forma remota sin tener que conectar un dispositivo criptográfico al PC.

Para obtener la Firma Electrónica en formato virtual se debe realizar una solicitud formal de recuperación mediante el portal de Gestión de identidades seleccionando la opción “Recuperar – Identidad electrónica Virtualizada”, de acuerdo con el procedimiento actual.



Para hacer uso de este nuevo tipo de Firma Electrónica se deben cumplir las siguientes condiciones técnicas requeridas para el correcto funcionamiento de la alternativa propuesta. Estos prerrequisitos son de carácter obligatorio.

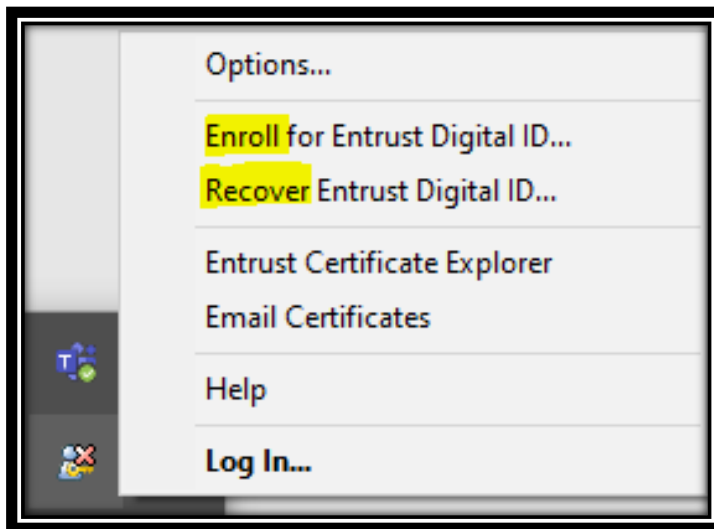
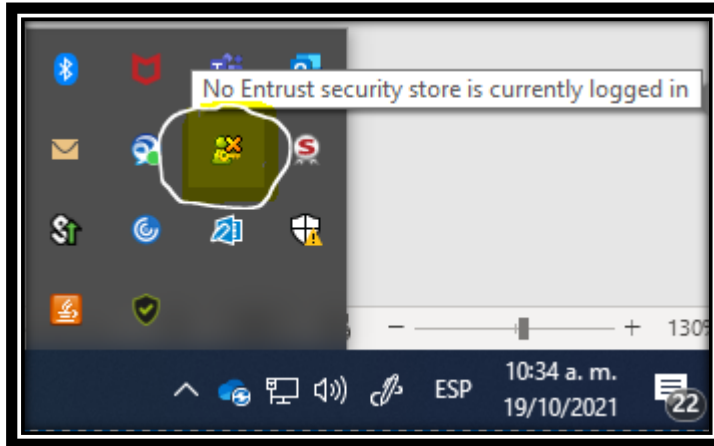
- El usuario debe establecer conexión remota a una máquina de su Entidad que cuente con acceso al canal dedicado con el Banco de la República.
- El usuario debe abrir sesión en el portal WSebra¹.
- En la máquina que tiene comunicación con el Banco de la República se debe tener instalado el software “Entrust Entelligence Security Provider”, que se encuentra

¹ Para usuarios de la Aplicación Antares el ingreso se deberá dar por el portal <https://wsebra.banrep.gov.co/internet>, adicionalmente no requerirán un canal dedicado con el Banco de la República.

dispuesto en el portal <https://caribe.banrep.gov.co/emisor> en la ruta Descargas SUCED, PKI, ESP, 2. ESP 10.0 W10 – banrep.gov.co



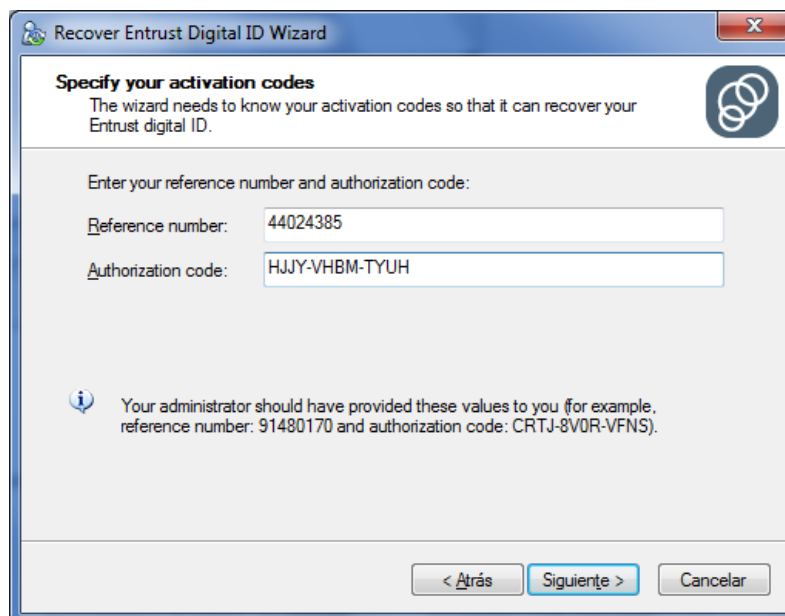
- Para la activación de la Identidad Electrónica, una vez instalado el software descrito en el ítem anterior, se debe realizar el siguiente procedimiento:
 - o Ingresar por **Entrust Security Provider**, seleccionando con el botón derecho del mouse la opción deseada para Crear (**Enroll**) o Recuperar (**Recover**) la identidad Electrónica del usuario.

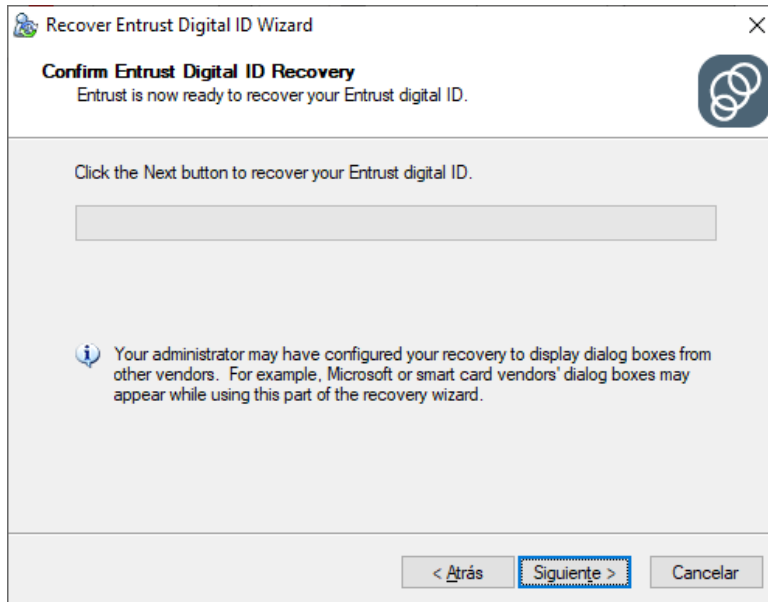


La primera ventana del asistente es esta. Aquí hacemos clic en **Siguiente**.

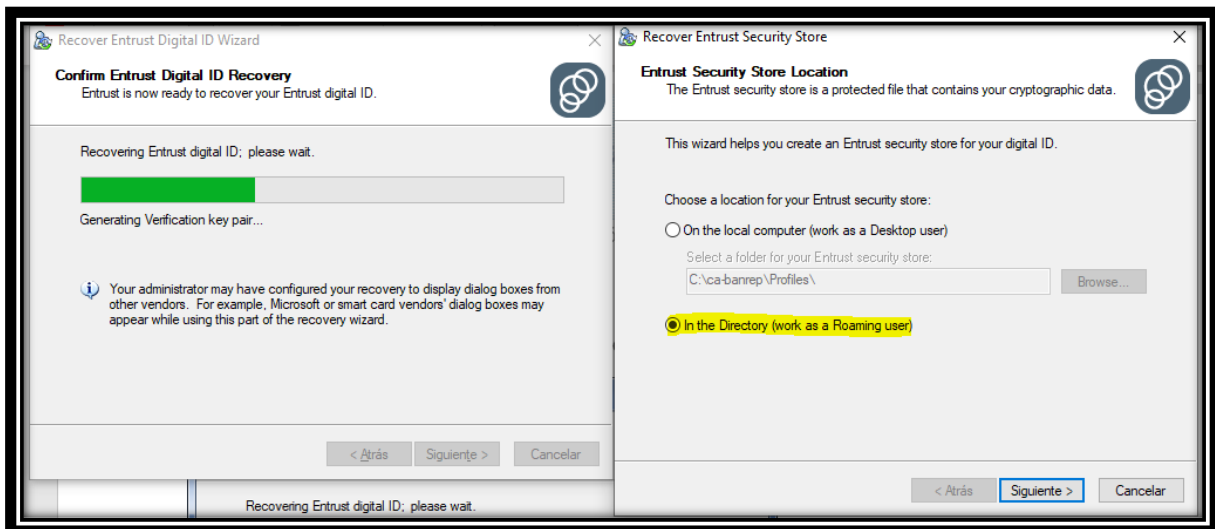


- En la pantalla siguiente, ingresar el código de autorización enviado en el acta PDF y el número de referencia remitido por el Banco de la República, luego dar clic en el botón con la opción **Siguiete** en las dos pantallas.

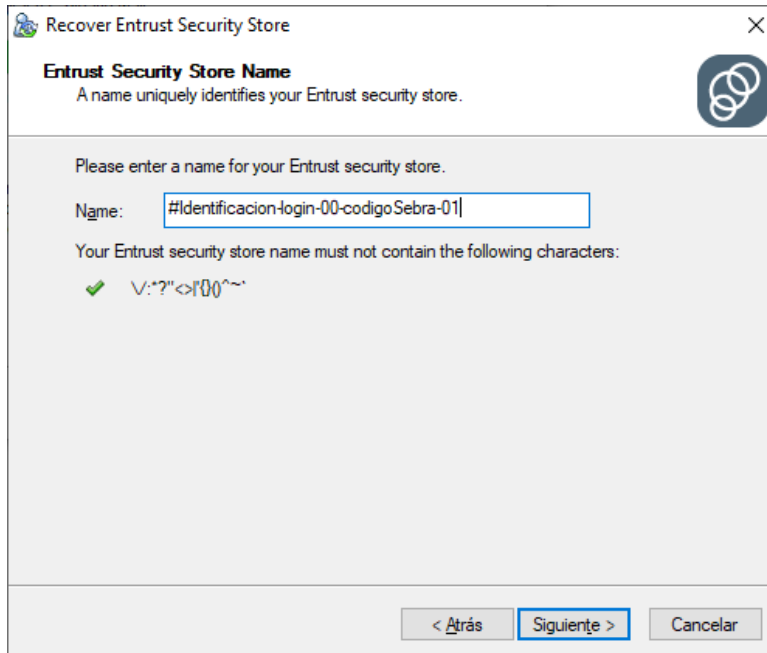




- En la ventana de **Entrust Security Store Location**, se debe seleccionar la opción **“In the Directory (work as a Roaming user)”**, y clic en **Siguiete**



- A continuación, el usuario deberá crear el nombre de su perfil *Roaming* de acuerdo al estándar **#Identificacion-login-00-codigoSebra-01**



Recover Entrust Security Store

Entrust Security Store Name
A name uniquely identifies your Entrust security store.

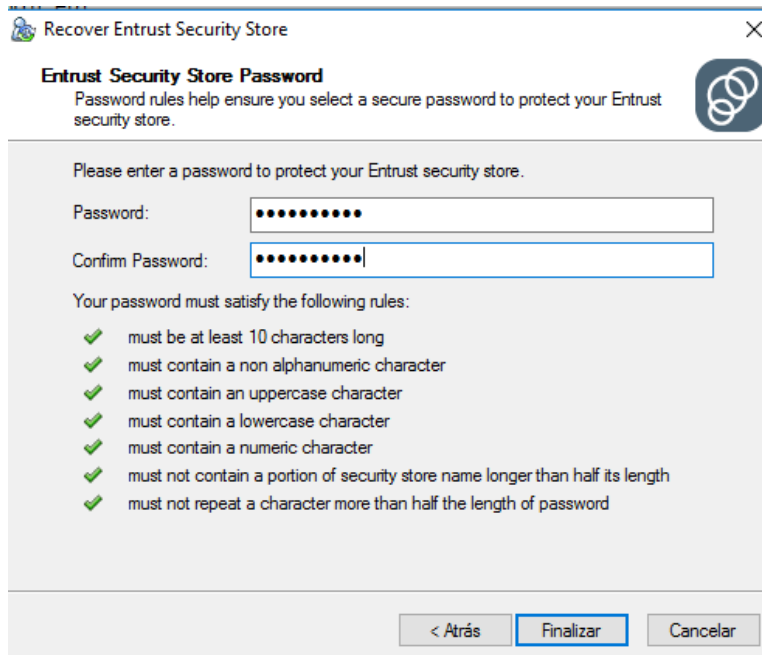
Please enter a name for your Entrust security store.

Name: #Identificacion+login-00-codigoSebra-01

Your Entrust security store name must not contain the following characters:
✓ \ : * ? " < > { } ^ _ ~

< Atrás Siguiente > Cancelar

- El procedimiento finaliza asignado una contraseña segura



Recover Entrust Security Store

Entrust Security Store Password
Password rules help ensure you select a secure password to protect your Entrust security store.

Please enter a password to protect your Entrust security store.

Password: ●●●●●●●●

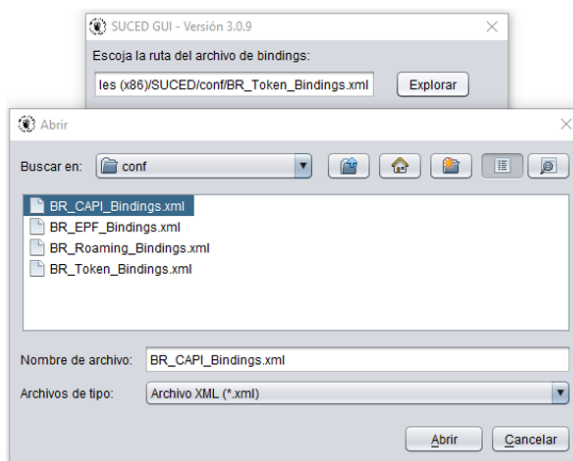
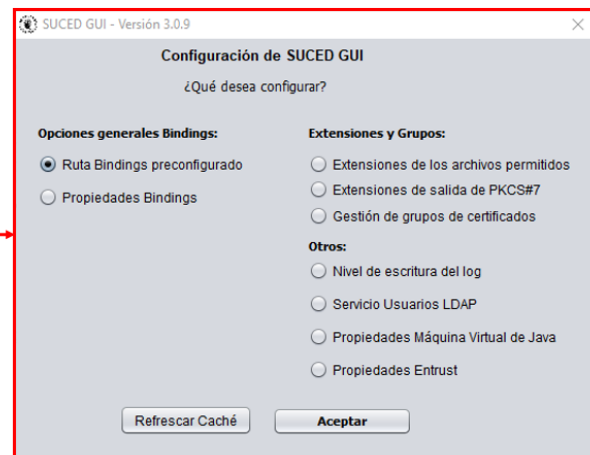
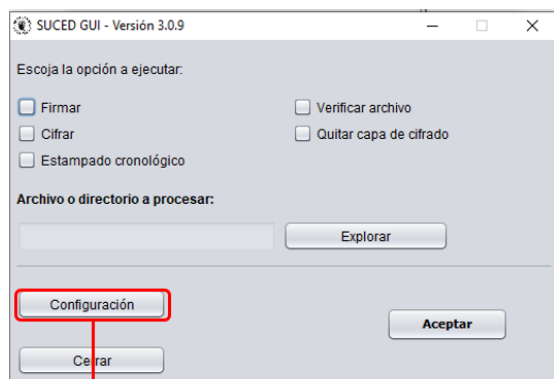
Confirm Password: ●●●●●●●●

Your password must satisfy the following rules:

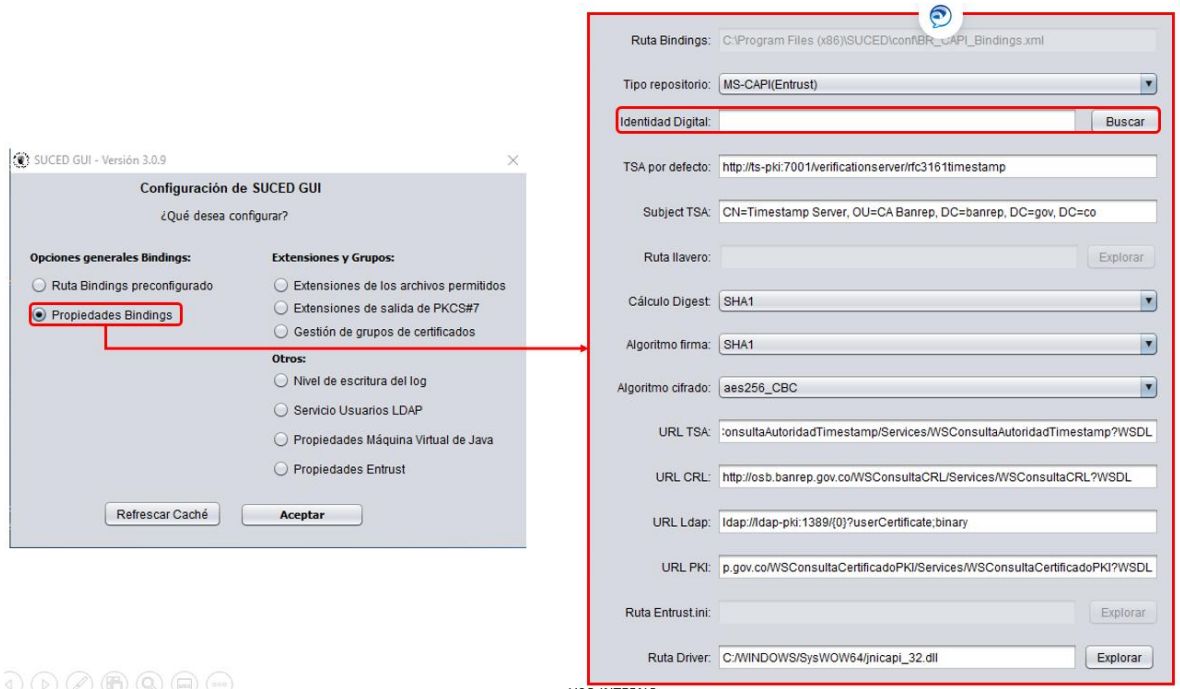
- ✓ must be at least 10 characters long
- ✓ must contain a non alphanumeric character
- ✓ must contain an uppercase character
- ✓ must contain a lowercase character
- ✓ must contain a numeric character
- ✓ must not contain a portion of security store name longer than half its length
- ✓ must not repeat a character more than half the length of password

< Atrás Finalizar Cancelar

- En el aplicativo SUCED GUI se debe realizar una configuración adicional, que se explica a continuación.
 - o Ingresar al aplicativo e ir al menú de configuración, una vez allí se debe seleccionar la opción “Ruta Bindings Preconfigurado” y seleccionar el archivo “BR_CAPI_BINDINGS.xml”



- Luego de configurar el archivo se debe ingresar nuevamente al menú de configuración, pero esta vez seleccionar la opción propiedades Bindings, lugar en donde se deberá cargar la identidad digital que fue previamente recuperada, dando clic en el botón buscar.



Este mismo procedimiento se describe a continuación para los usuarios que tenga otra versión de SUCED GUI

