Banco de la República
Bogotá D. C., Colombia

Dirección General de Tecnología
Departamento de Gestión Informática

DOCUMENTO TÉCNICO DE SERVICIOS NO INTERACTIVOS DEL BANCO DE LA REPÚBLICA

Julio de 2021

Versión 1.3

CONTENIDO

1 INTRODUCCIÓN

1.1 OBJETO

El presente documento tiene como fin establecer el procedimiento para el uso de la automatización de procesos criptográficos de archivos y comunicaciones B2B (***modelo no interactivo***) entre servidores de las entidades financieras y el Banco de la República a través de los canales dedicados, utilizando las herramientas SUCED CommandLine, Gestión de Transferencia de Archivos (GTA) y a través de Servicios Web.

1.2 ALCANCE DEL DOCUMENTO

Este documento define el procedimiento, políticas y demás reglas para el uso de los servicios automáticos del Banco de la República.

1.3 AUDIENCIA

Este documento está dirigido a las áreas tecnológicas de las entidades financieras que desean automatizar los procesos criptográficos de archivos y comunicaciones B2B.

2 PRERREQUISITOS

Para la implementación de la automatización procesos criptográficos se deben tener en cuenta los siguientes prerrequisitos:

2.1 ACCESOS REQUERIDOS

Para la correcta operación del cliente de automatización de procesos, se hace necesario que las máquinas de la entidad tengan los siguientes accesos:

Para Ambiente de Producción:

Sistema	IP	Nombre	servicio	Descripción
SUCED[1]	192.168.61.15	tunebo.banrep.gov.co (Bus de producción)	TCP/443	Acceso a Bus de Servicios (OSB) del ambiente de producción
	192.168.61.15	awa.banrep.gov.co (TSA de Producción)	TCP/443	Acceso al servicio de timestamping del ambiente de Producción
Web Services de Negocio	192.168.58.13	totoro.banrep.gov.co (Bus de producción)	TCP/443	Acceso a Bus de Servicios (OSB) del ambiente de Producción

[1] La resolución de los WSDL para SUCED CommandLine debe realizarse de forma local. Se recomienda consultar el manual: "**Manual y puesta en marcha de SUCED Command Line**" publicado en https://caribe.banrep.gov.co/emisor

GTA	192.168.61.26	GTAGW-Financiero.banrep.gov.co	TCP/22	Producción

Para Ambiente de Pruebas:

Sistema	IP	Nombre	servicio	Descripción
SUCED[3]	192.168.61.21	nukak.banrep.gov.co (Bus de pruebas)	TCP/443	Acceso a Bus de Servicios (OSB) del ambiente de pruebas
Web Services de Negocio	192.168.58.14	nasa.banrep.gov.co (Bus de pruebas)	TCP/443	Acceso a Bus de Servicios (OSB) del ambiente de pruebas
GTA	192.168.61.25	GTAGW-Pruebas.banrep.gov.co	TCP/22	Pruebas

IMPORTANTE: Cada entidad será responsable de configurar el enrutamiento y permisos de conexión a las direcciones anteriormente referenciadas, tanto en las redes internas de la entidad, como de solicitarlo y probarlo con el respectivo proveedor del canal dedicado.

3 SUCED

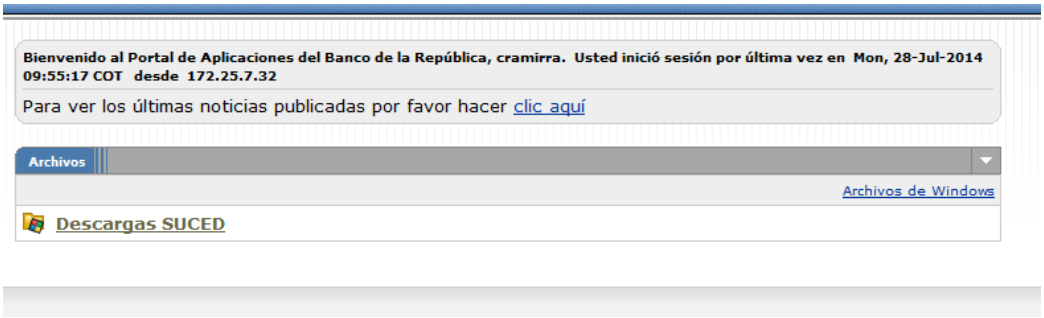
El objetivo principal de la automatización de procesos criptográficos es procesar una cantidad considerable de archivos evitando procedimientos interactivos. Así que es prioritario que cada Entidad establezca las consideraciones de seguridad informática necesarias en la automatización de los procesos, como la ubicación del certificado (.epf) y manejo de contraseña del mismo, dado que una vez sea entregado a la entidad, éste estará bajo responsabilidad de la misma.

[3] La resolución de los WSDL para SUCED CommandLine debe realizarse de forma local. Se recomienda consultar el manual: "**Manual y puesta en marcha de SUCED Command Line**" expuesto en https://caribe.banrep.gov.co/emisor

3.1 DESCARGA DE SUCEDCOMMANDLIINE

La descarga del ***SucedCommandLine*** se debe realizar a través del portal https://caribe.banrep.gov.co/emisor

Ingresar en ***Descargas SUCED***



Descargar la versión disponible de SucedCommandLine, las versiones de sistema operativo certificadas para SucedCommandLine son:

Sistema Operativo	***Nombre Cliente SucedCommandLine***
Windows7 64 Bits	SucedCommandLine-3.1.5-r67566-win7-64Bits.zip
Windows7 32 Bits	SucedCommandLine-3.1.5-r67566-winXP-win7-32bits.zip
Windows XP	SucedCommandLine-3.1.5-r67566-winXP-win7-32bits.zip

Solaris SPARC	SucedCommandLine-3.0.7.2-r66225-SolarisSPARC.zip

La forma de instalación, configuración y operación básica se encuentra en el documento "**Manual y puesta en marcha de SUCED Command Line**" y demás manuales técnicos y de usuario que se obtienen del enlace de descarga.

Para realizar las operaciones criptográficas de firma, cifrado, descifrado y/o verificación se requiere del uso de un certificado digital.

4 GTA

El sistema de Gestión de Transferencia de Archivos (GTA) es el sistema que dispone el Banco de la República para el intercambio de archivos con las entidades usuarias de los servicios electrónicos. A continuación se describe el esquema de uso **No Interactivo** de este sistema.

4.1 PROTOCOLO SEGURO

Las transferencias de archivos entre servidores de la entidad y el Banco de la República serán realizadas por protocolo SFTP, con autenticación de usuario, password y llave pública para asegurar autenticación y no repudio. La contraseña del usuario será fija y no se utilizará token OTP RSA para su autenticación.

4.2 CONTINGENCIA

El Banco de la República NO es responsable por fallas del canal de comunicación o en la conexión SFTP. Por lo tanto, es responsabilidad de las entidades configurar las alertas para identificar este tipo de incidentes, así como utilizar alguna de las contingencias operativas y/o tecnológicas definidas para el servicio o sistema de información.

4.3 POLÍTICAS GENERALES DE USO

A continuación las políticas de uso del servicio de transferencia de archivos no interactivo del Banco de la República:

- Cuando un usuario genérico de transferencia de archivos tenga una conexión fallida hacia el servidor SFTP, este debe esperar un tiempo de 5 segundos como mínimo para volver a intentar conectarse al servidor; en caso de que intente la conexión antes de los 5 segundos, la conexión será rechazada.
- Si un usuario tiene 3 intentos de conexiones fallidas, la conexión SFTP será cerrada.
- El usuario genérico de transferencia de archivos será desconectado de la sesión SFTP después de 3 minutos de inactividad.
- El usuario genérico de transferencia de archivos deberá conectarse al servicio SFTP a través del puerto 22
- Si un usuario genérico de transferencia de archivos tiene 5 intentos de autenticación inválidos en un tiempo de 5 minutos, la IP será bloqueada por intento de ataque por fuerza bruta.
- Si se detectan 60 conexiones invalidas en un tiempo de 5 minutos, la IP será bloqueada por posible ataque de Denegación de Servicio (DoS).
- El usuario genérico de transferencia de archivos podrá estar conectado una sola vez al tiempo. Es decir que no se le permitirán sesiones concurrentes, sino una sola sesión.
- La entidad deberá crear el par de llaves SSH (pública y privada), las cuales deben ser de tipo SSH-2 RSA, con un tamaño de 2048 bits. Debe enviar la llave pública al Banco de la República.
- La entidad deberá informar al Banco de la República cuando se cambie la llave pública del servidor de la entidad para que se continúe con la correcta autenticación del usuario.
- La entidad deberá hacer "**LIST**", "**PUT**" y/o "**GET**" de los archivos a enviar y/o recoger del Banco de la República. Es decir los servidores del Banco de la República **NO** se conectan a la infraestructura de la entidad.
- Es responsabilidad de la entidad realizar el monitoreo de la conexión con sus respectivas notificaciones.

5 ASPECTOS TÉCNICOS PARA CONSUMO DE SERVICIOS WEB DEL BANCO DE LA REPÚBLICA

La conexión a la infraestructura de servicios web del Banco se realiza a través de una infraestructura tecnológica segura de comunicaciones que requiere la integración de la plataforma de red propia de la Entidad Autorizada. El procedimiento de análisis, selección de topología, instalación y configuración de los equipos de red es responsabilidad de la Entidad Autorizada. En caso de ya contar con un canal dedicado con el Banco, se empleará este mismo canal para el consumo de servicios.

El canal de acceso a la infraestructura se asegura mediante el protocolo HTTPS.

5.1 MAPA DE ESTÁNDARES Y TECNOLOGÍAS

Esta sección describe los estándares y tecnologías usados en la Arquitectura de Servicios del Banco de la República. La siguiente tabla presenta estos estándares y tecnologías agrupados en categorías para facilitar su comprensión:

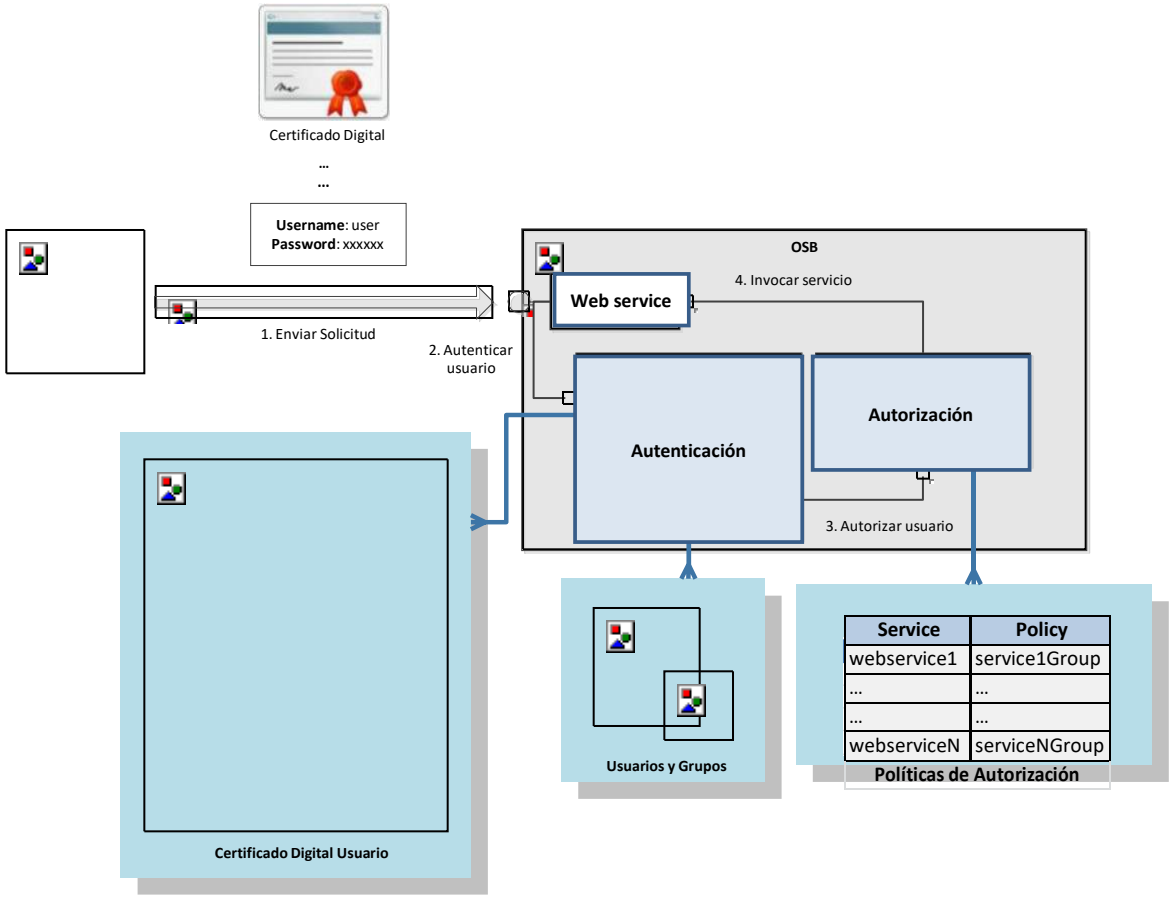
Categoría	Estándar/Tecnología	Versión
Comunicación	SOAP	1.1 / 1.2
	HTTP	1.0,1.1
Seguridad	WS-Security (firma/ cifrado)	1.0
	WS-Policy	1.2
	Username Token Profile	1.0
	X.509 Token Profile	1.0
Definición de Servicios	WSDL	1.1 / 1.2
Registro de Servicios	UDDI	V3
Interoperabilidad	WS-I Basic Profile	1.0

Otras Tecnologías	XSLT	1.0
	XQuery	1.0
	XPath	2.0

Para determinar cuales de estos estándares y tecnologías son utilizadas en cada servicio, por favor consulte el WSDL respectivo.

5.2 AUTENTICACIÓN Y AUTORIZACIÓN DE SERVICIOS

La implementación de la autenticación y autorización de servicios se realiza a través de certificados digitales a nivel de mensaje usando WS-Security. El escenario se describe a continuación:



1. Envío de la Solicitud. El cliente invoca el servicio web proporcionando sus credenciales (certificado digital) para efectos de autenticación.
2. Autenticación del Cliente. Antes de invocar el servicio, La infraestructura de servicios del Banco autentica el usuario usando las credenciales proporcionadas por el cliente.
3. Autorización del Cliente. Una vez autenticado, se determinan los roles y grupos a los que pertenece el cliente, así como los permisos necesarios para consumir el servicio. Las políticas de autorización a nivel de mensaje son definidas por el área de negocio para cada servicio.
4. Invocación del Servicio. Después de determinar el nivel de autorización del cliente, el servicio es finalmente invocado.

5.3 FIRMA DIGITAL DE MENSAJES (REQUEST)

Para efectos de autenticación del cliente, se requiere la firma de la petición (request) de la operación en particular. De este modo, se garantiza la integridad del mensaje enviado. A continuación se describe el flujo correspondiente:

1. El cliente envía una petición firmada digitalmente haciendo uso de su par de llaves.
2. La infraestructura de servicios del Banco valida la firma digital y su cadena de confianza.
3. Después de esta validación, se procede con la autenticación y autorización extrayendo el usuario del certificado digital (de acuerdo a lo explicado en la sección anterior).
4. Si la validación es correcta el servicio es finalmente invocado y la respuesta generada es retornada al cliente que lo invocó.

5.4 FIRMA DIGITAL DE MENSAJES (RESPONSE)

La respuesta (response) retornada por el servicio podrá estar firmada digitalmente para validación por parte del cliente. Para los servicios cuya especificación incluye un mensaje de respuesta firmado por parte del Banco, el cliente dispondrá de un certificado digital con la llave pública del Banco de manera que pueda validar la autenticidad e integridad del mensaje recibido.

El certificado empleado por el Banco para estos efectos es generado por la CA subordinada de Certicamara (CN = AC SUB CERTICAMARA)[4]. El subject del certificado es el siguiente:

CN = BANCO DE LA REPUBLICA
C = CO
E = FRIVASDU@BANREP.GOV.CO
L = BOGOTA D.C.
O = BANCO DE LA REPUBLICA
1.3.6.1.4.1.23267.2.3 = 8600052167
SERIALNUMBER = 427434
OU = FIRMA FORMULARIOS WEB
ST = BOGOTA D.C.

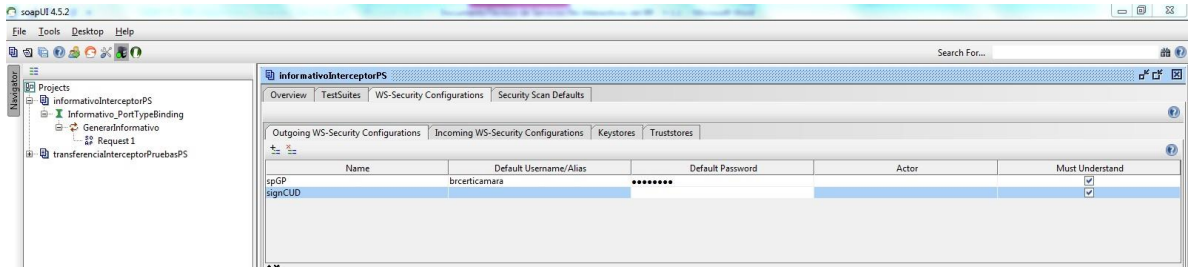
5.5 PRUEBA DE SERVICIOS MEDIANTE SOAPUI

En esta sección se describe como se puede usar la herramienta SoapUI para probar la configuración de los servicios desplegados en el Bus de Servicios del Banco. Se describe la configuración para probar servicios que implementen firma digital, autenticación y autorización.

5.5.1 PRUEBA DE SERVICIOS CON FIRMA DIGITAL

Para probar un servicio que requiera de firma digital realice la siguiente configuración:

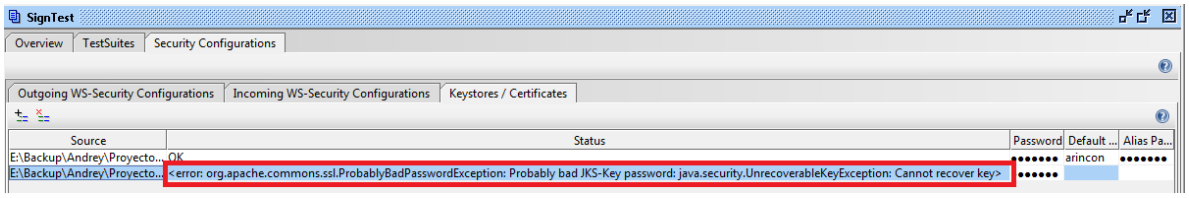
1. Dentro de un proyecto de SoapUI cree una petición al servicio que va a probar.
2. La configuración de seguridad en SOAPUI se realiza a nivel de todo el proyecto. Por lo tanto, seleccione el proyecto y haga clic sobre la pestaña WS-Security Configurations.



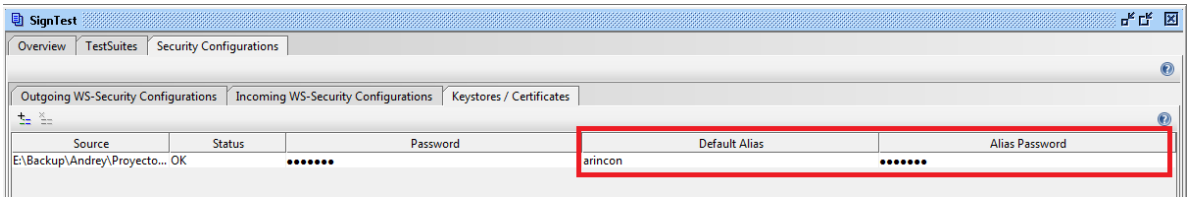
3. En la pestaña Keystore/Certificates registre el keystore donde se encuentran almacenado el par de llaves usado para firmar digitalmente la petición.

[4] Este certificado puede descargarse de la página web del Banco, en Sistema financiero › Servicios electrónicos › Documentos, formatos e información adicional de SEBRA (http://www.banrep.gov.co/es/sebra)

4. Si el password del keystore y el paswword del par de llaves son diferentes es posible que le salga el siguiente error:

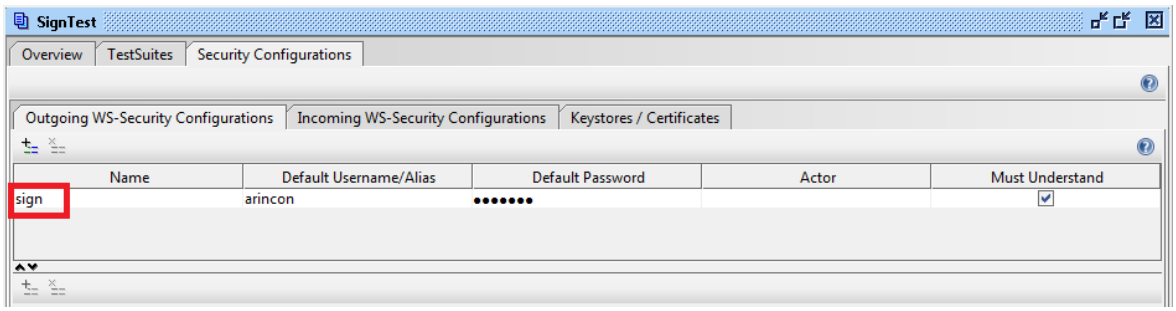


Para solucionarlo ingrese el nombre del alias del par de llaves junto con su password:



Firma digital – Request

5. Vaya ahora a la pestaña Outgoing WS-Security Configurations y cree una nueva configuración para firmar un request ingresando la siguiente información:

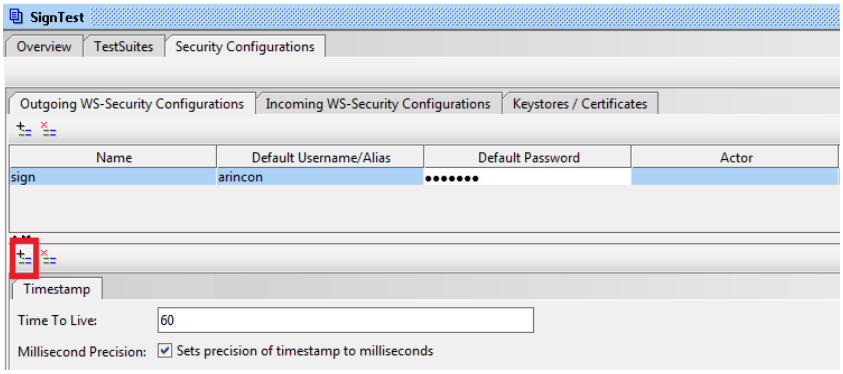


6.

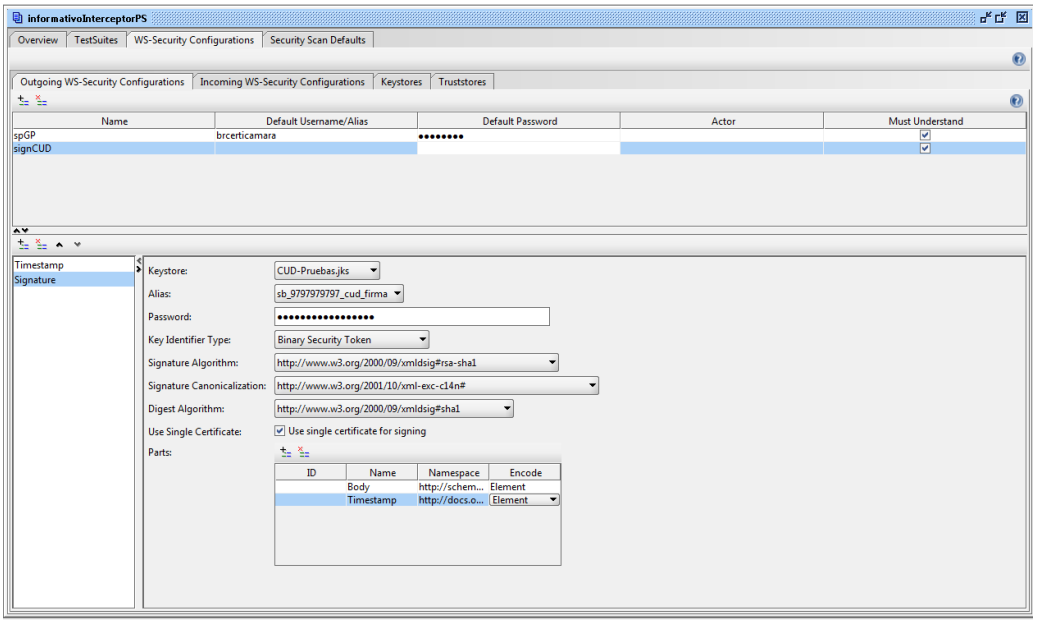
- **Name**: Corresponde al nombre con el que se va a identificar la configuración.
- **Default Username/Alias**: Ingrese el alias asociado al par de llaves usado para firmar digitalmente la petición.
- **Default password**: Ingrese el password del alias seleccionado.
- **Must Understand**: Seleccione esta opción.

6. Seleccione la configuración creada en el paso anterior y adicione las siguientes entradas:

- **Timestamp**. Esta entrada adiciona una estampilla de tiempo a la petición enviada al servicio.



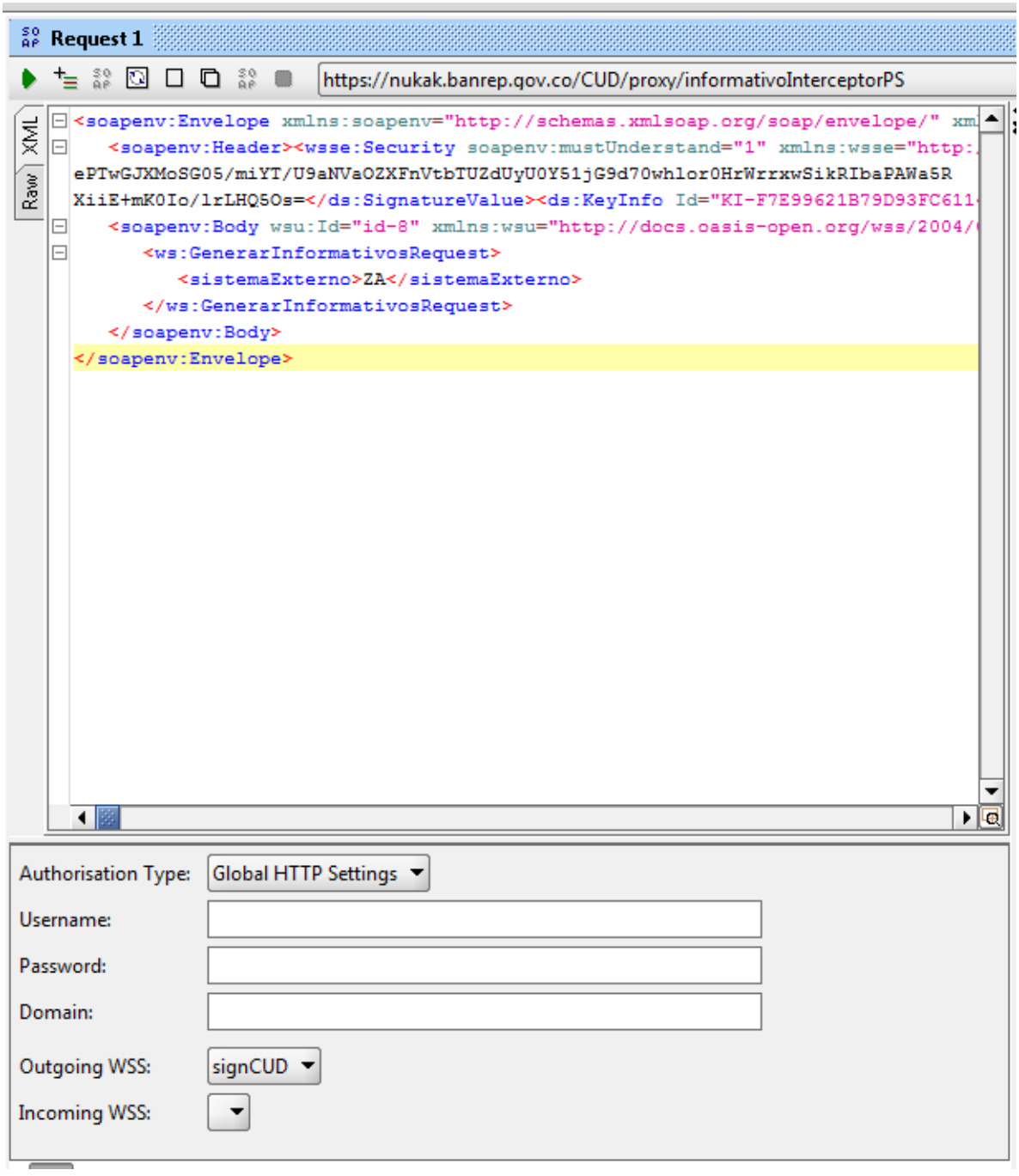
- **Signature**. Esta entrada indica que la petición enviada al servicio debe ser firmada digitalmente. Ingrese la siguiente información:



- **Keystore**: Seleccione el keystore que configuro en el paso 3.
- **Alias**: Seleccione el alias asociado al par de llaves usado para firmar digitalmente.
- **Key Identifier Type**: Seleccione Binary Security Token. Esto indica que el certificado digital asociado al alias debe incluirse en la petición.
- **Signature Algorithm**: Corresponde al algoritmo usado para firmar la petición. Seleccione http://www.w3.org/2000/09/xmldsig#rsa-sha1.0
- **Signature Canonicalization**: Corresponde al método de canonización usado para transformar la petición. Seleccione http://www.w3.org/2001/10/xml-exc-c14n#.

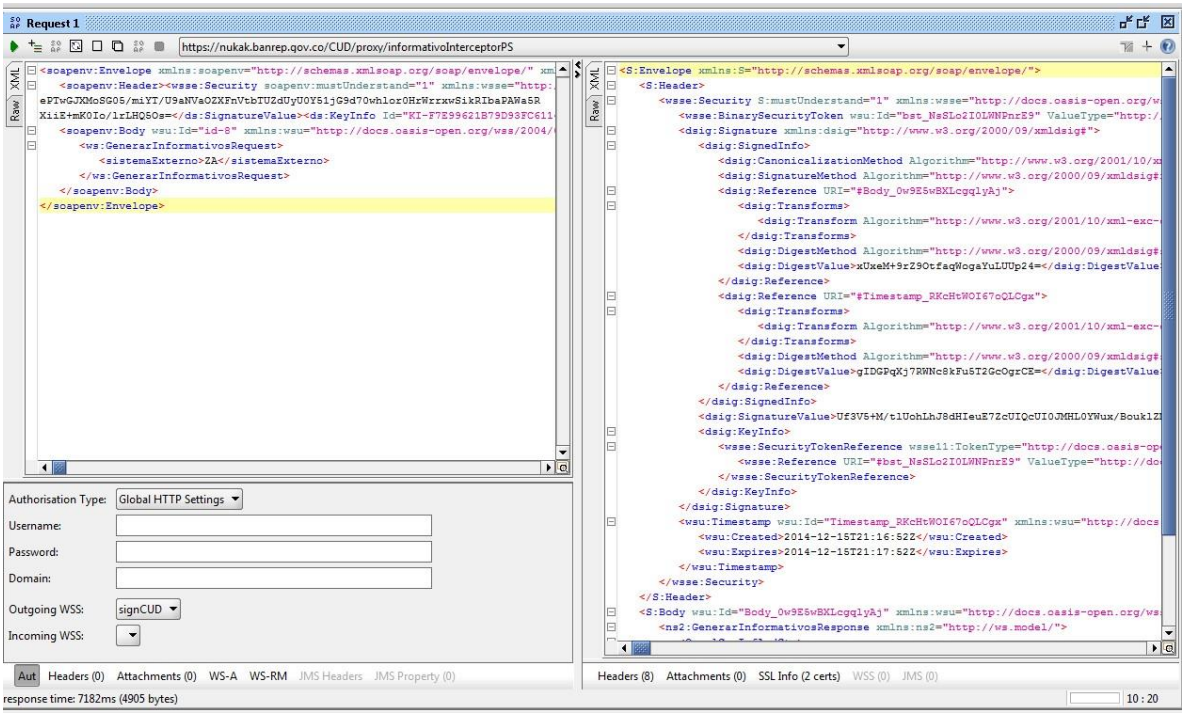
- **Digest Algorithm**: Seleccione http://www.w3.org/2000/09/xmldsig#sha1.
- **Use Single Certificate**: Seleccione esta opción.
- **Parts**. Permite seleccionar las partes del mensaje que serán firmadas. Ingrese:
  - **Body**. Firma el cuerpo de la petición. Ingrese el namespace http://schemas.xmlsoap.org/soap/envelope/. Seleccione en **Encode**, el valor "**Element"**.
  - **Timestamp**. Firma el timestamp adicionado al request. Ingrese el namespace http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd. Seleccione en **Encode**, el valor "**Element"**.

7. Después de crear la configuración, usted debe asociarla a la petición que usara para probar el servicio. Esto se hace seleccionando la petición y escogiendo en la opción Aut > Outgoing WSS la configuración de WS-Security que creo en los pasos anteriores:



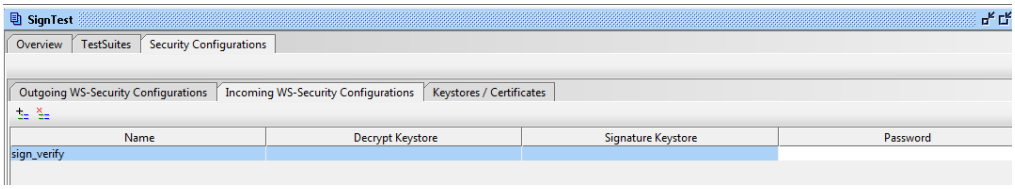
Si después de crear la configuración esta no se encuentra disponible en la lista de selección se recomienda que clone o cree nuevamente el request.

8. Después de realizar esta configuración ya es posible probar el servicio con firma Digital. La prueba debería ser similar a la siguiente imagen:



Firma digital – Response

9. Hasta este punto SOAPUI solamente envía una petición firmada digitalmente y el servicio responde con un mensaje firmado de la misma manera. Si usted también desea validar esta respuesta, debe crear una Incoming WS-Security Configuration.



En esta configuración usted debe especificar solamente el keystore donde se encuentra el certificado digital usado por el servicio para firmar digitalmente el response (Signature Keystore). Adicionalmente, debe seleccionar esta configuración en el request usado para realizar la prueba.

5.6 CERTIFICADOS DIGITALES

Para el consumo de servicios B2B, el Banco suministrará al cliente:

1. Certificado digital (B2B) emitido por la CA del Banco para autenticación, autorización y firma de mensajes mediante WS Security. Se genera un certificado digital para cada sistema de negocio del Banco. Este certificado le permitirá al cliente el consumo de los servicios expuestos por cada sistema en particular.
2. Llave pública del Banco de la República para validación de respuestas de los servicios.

5.7 POLÍTICAS GENERALES DE USO

A continuación las políticas de uso de los servicios web del Banco de la República:

- Se limitará el número de requests por periodo de tiempo. Este parámetro se informará para cada servicio dependiendo de la infraestructura tecnológica del Banco.
- Los mecanismos de control de la infraestructura tecnológica del Banco detectarán comportamientos inusuales en el uso de los servicios web y podrán adelantar acciones de bloqueo por posible ataque de Denegación de Servicio (DoS).

6 PROCEDIMIENTOS

6.1 SOLICITUD DE CERTIFICADO GENÉRICO

Un certificado con propósitos de automatización de procesos criptográficos y comunicaciones B2B (***no interactivos***), hace referencia a un certificado emitido a nombre la entidad y debe ser de uso exclusivo por la aplicación en la que se necesite la integración. El certificado deberá ser solicitado por el Delegado con Responsabilidad Administrativa según lo mencionado en el formulario BR-3-598-0.xls, el cual está publicado en el sitio web del Banco (http://www.banrep.gov.co/es/pki-formatos-administrativos.)

El uso correcto del certificado estará a cargo y bajo responsabilidad del Delegado con Responsabilidad Administrativa de la Entidad. (Ver Documento “Declaración de Prácticas

de Certificación para la ***CA Banrep",*** ubicado en http://www.banrep.gov.co/es/contenidos/page/declaraci-n-pr-cticas-certificaci-n-ca-banrep).

Se debe tener en cuenta que al momento de solicitar el primer certificado digital genérico, la entidad acepta la creación de un usuario genérico en el directorio de usuarios que el Banco dispone (LDAP) y que dicha creación conlleva un costo enmarcado en el contrato Sebra.

6.1.1 CERTIFICADOS PARA LA AUTOMATIZACIÓN DE PROCESOS CRIPTOGRÁFICOS

El Certificado Genérico para realizar la automatización de procesos criptográficos (uso en SucedCommandLine) estará en formato ***EPF*** (Entrust Profile) y tendrá la siguiente nomenclatura en la composición de su CN (Common Name), basando su estructura en tres partes:

- La primera parte está compuesta por el NIT –incluyendo el código de verificación- de la entidad que desea intercambio de archivos con el Banco de la República.

- La segunda parte está asociada con el sistema de información del Banco de la República al cual se dirige la transferencia. Por ejemplo: CUD, CEDEC, CENIT STA, SOI, entre otros.

- La tercera parte corresponde al NIT de la entidad seguido del DN (Distinguish Name) para la Entidad de Certificación Digital CA Banrep.

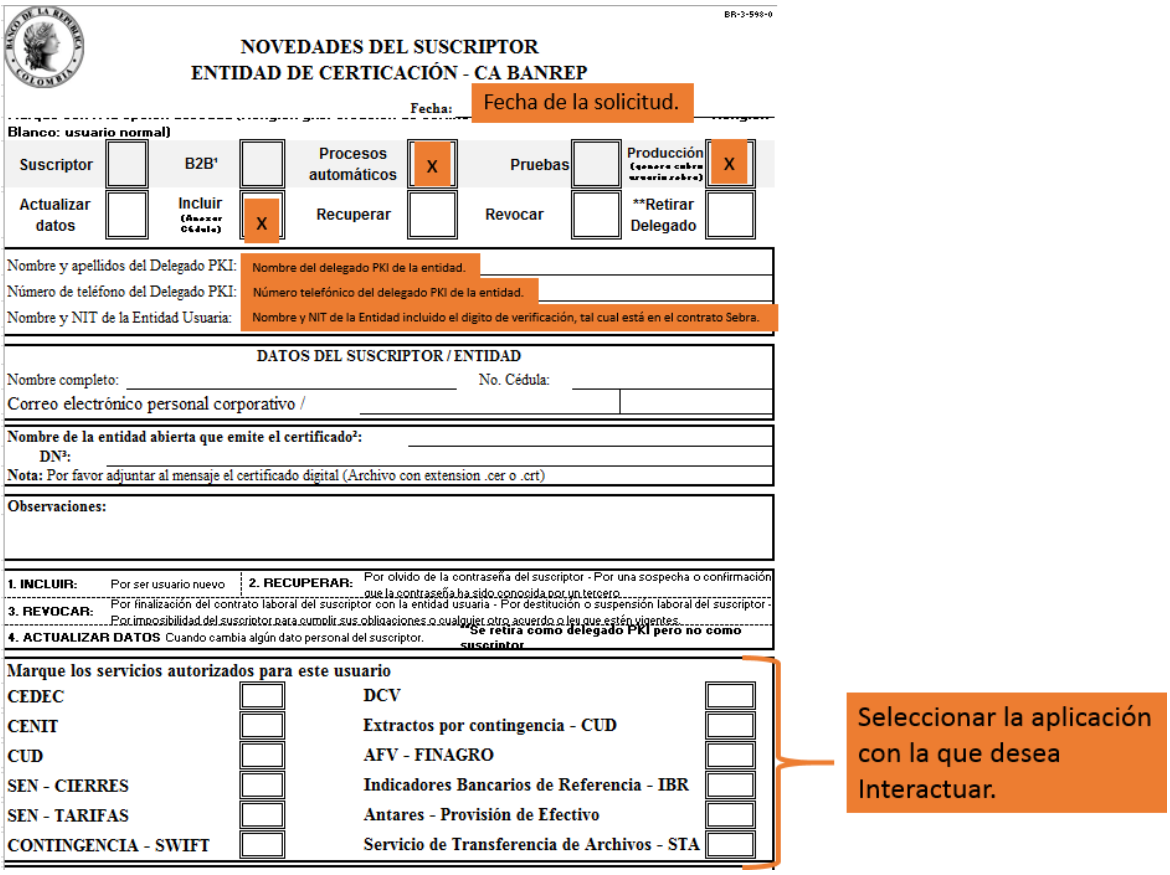
Por lo tanto, el DN para los certificados que serán usados en la implementación de procesos automáticos de Firma Digital y/o cifrado por parte de las Entidades Usuarias estará formados de la siguiente manera:

Componente de Dominio:
dc=co
dc=gov
dc=banrep
Unidad Organizacional:
ou=CA Banrep
ou=NIT de la entidad incluyendo digito de verificación (solo los caracteres numéricos)
Nombre común:
cn=NIT de la Entidad Nemónico de la Aplicación con la que se va a interactuar.

Algunos ejemplos de la composición del DN para certificados Genéricos:

DN Usuario Genérico	Descripción
cn=8909039388 CENIT, ou=8909039388, ou=CA Banrep, dc=Banrep, dc=gov, dc=co	DN del certificado para la automatización de procesos criptográficos de archivos en forma no interactiva de Bancolombia para el sistema CENIT.
cn= 8999990902 SOI, ou=8999990902, ou=CA Banrep, dc=Banrep, dc=gov, dc=co	DN del certificado para la automatización de procesos criptográficos de archivos en forma no interactiva de la Dirección General de Crédito Publico y del Tesoro Nacional para el sistema SOI.

A continuación, se muestra un ejemplo de la forma en la que se debe diligenciar el formato BR-3-598-0 para solicitar un certificado para la automatización de procesos criptográficos, para información del proceso que se debe seguir para la solicitud, remítase al Documento de Declaración de Practicas de Certificación para la ***CA Banrep*** en ubicado en http://www.banrep.gov.co/es/contenidos/page/declaraci-n-pr-cticas-certificaci-n-ca-banrep:



NOVEDADES DEL SUSCRIPTOR
ENTIDAD DE CERTICACIÓN - CA BANREP

Fecha: Fecha de la solicitud.

Blanco: usuario normal)

Suscriptor		B2B¹		Procesos automáticos	X	Pruebas		Producción (genera cobro usuario sobre)	X
Actualizar datos		Incluir (Anexar Cédula)	X	Recuperar		Revocar		**Retirar Delegado	

Nombre y apellidos del Delegado PKI: Nombre del delegado PKI de la entidad.
Número de teléfono del Delegado PKI: Número telefónico del delegado PKI de la entidad.
Nombre y NIT de la Entidad Usuaria: Nombre y NIT de la Entidad incluido el digito de verificación, tal cual está en el contrato Sebra.

DATOS DEL SUSCRIPTOR / ENTIDAD
Nombre completo: No. Cédula:
Correo electrónico personal corporativo /

Nombre de la entidad abierta que emite el certificado²:
DN³:
Nota: Por favor adjuntar al mensaje el certificado digital (Archivo con extension .cer o .crt)

Observaciones:

1. INCLUIR: Por ser usuario nuevo
2. RECUPERAR: Por olvido de la contraseña del suscriptor - Por una sospecha o confirmación que la contraseña ha sido conocida por un tercero
3. REVOCAR: Por finalización del contrato laboral del suscriptor con la entidad usuaria - Por destitución o suspensión laboral del suscriptor - Por imposibilidad del suscriptor para cumplir sus obligaciones o cualquier otro acuerdo o ley que estén vigentes
4. ACTUALIZAR DATOS Cuando cambia algún dato personal del suscriptor. **Se retira como delegado PKI pero no como suscriptor

Marque los servicios autorizados para este usuario

CEDEC		DCV	
CENIT		Extractos por contingencia - CUD	
CUD		AFV - FINAGRO	
SEN - CIERRES		Indicadores Bancarios de Referencia - IBR	
SEN - TARIFAS		Antares - Provisión de Efectivo	
CONTINGENCIA - SWIFT		Servicio de Transferencia de Archivos - STA	

Seleccionar la aplicación con la que desea Interactuar.

6.1.2 CERTIFICADOS PARA COMUNICACIONES B2B

El Certificado Genérico para realizar procesos B2B estará en formato ***EPF*** (Entrust Profile) y podrá ser exportado en formatos JKS (Java Key Store) o P12 (PKCS·12), así mismo tendrá la siguiente nomenclatura en la composición de su CN (Common Name), basando su estructura en tres partes:

- La primera parte está compuesta por el distintivo SB seguido del NIT –incluyendo el código de verificación- de la entidad que desea intercambio de archivos con el Banco de la República.

- La segunda parte está asociada con el sistema de información del Banco de la República al cual se dirige la transferencia. Por ejemplo: CUD, CEDEC, CENIT STA, SOI, entre otros.

- La tercera parte corresponde al NIT de la entidad seguido del DN (Distinguish Name) para la Entidad de Certificación Digital CA Banrep.

Por lo tanto, el DN para los certificados que serán usados en la implementación de procesos automáticos de Firma Digital y/o cifrado por parte de las Entidades Usuarias estará formados de la siguiente manera:

Componente de Dominio:
dc=co
dc=gov
dc=banrep
Unidad Organizacional:
ou=CA Banrep
ou=NIT de la entidad incluyendo digito de verificación (solo los caracteres numéricos)
Nombre común:
cn=SB-NIT de la Entidad-Nemónico de la Aplicación con la que se va a interactuar**.**

Algunos ejemplos de la composición del DN para certificados Genéricos:

DN Usuario Genérico	Descripción
cn=SB-8909039388-CENIT, ou=8909039388, ou=CA Banrep, dc=Banrep, dc=gov, dc=co	DN del certificado para realizar comunicaciones B2B en forma no interactiva de Bancolombia para el sistema CENIT.
cn= SB-8999990902-SOI, ou=8999990902, ou=CA Banrep, dc=Banrep, dc=gov, dc=co	DN del certificado para realizar comunicaciones B2B en forma no interactiva de la Dirección General de Crédito Publico y del Tesoro Nacional para el sistema SOI.

En el caso en que una Entidad interactúe con varios sistemas de información del Banco de la República, se debe generar un certificado genérico para intercambiar información con cada sistema.

El Certificado Genérico tanto para automatización de procesos y comunicación B2B tendrá una vigencia de dos (2) años, el Banco de la República informará vía correo electrónico (que este registrado en la solicitud BR-3-598-0.xls) los próximos certificados a expirar y la fecha de expiración del certificado, así:

- El primer día calendario del mes se informarán los certificados a expirar en los siguientes 60 días calendario.

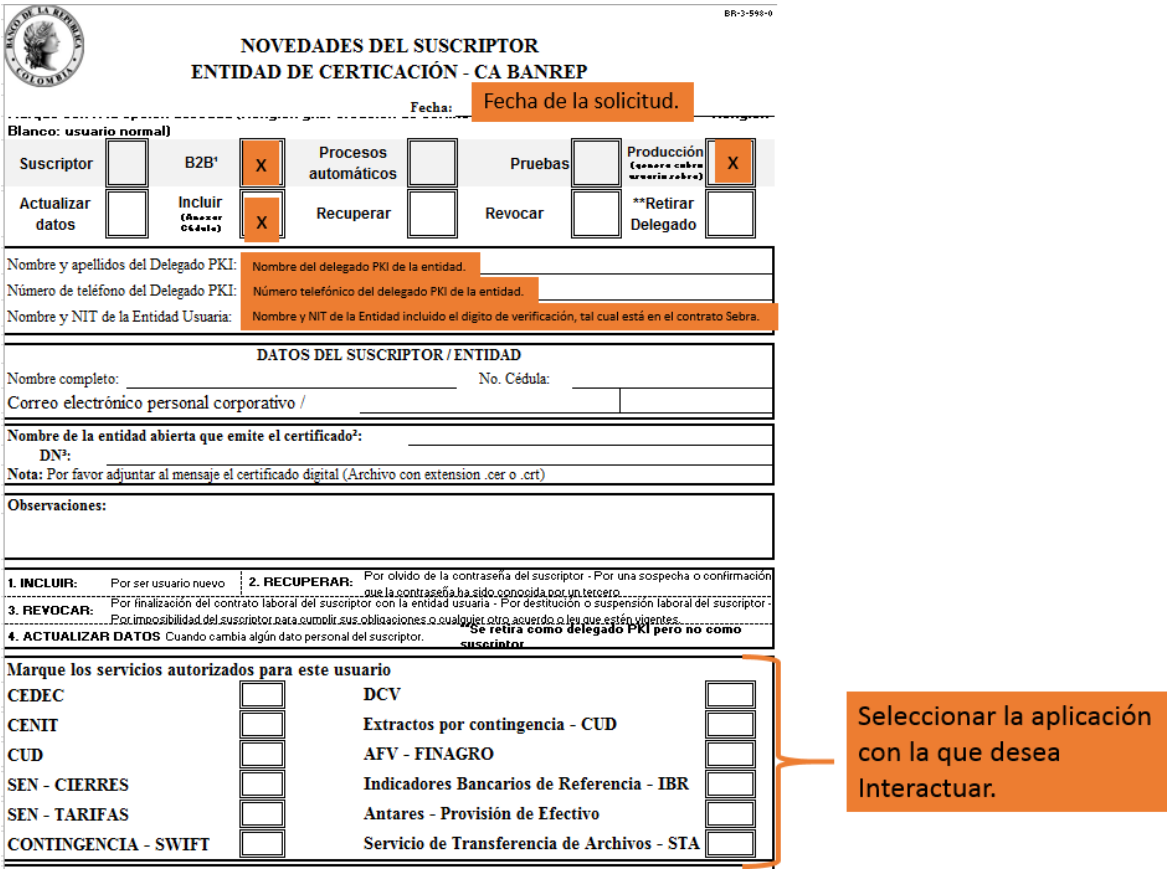
- Todos los días se informarán los certificados a expirar dentro de los siguientes 15 días calendario.

La Entidad será responsable de solicitar la creación del nuevo certificado. Para revisar los términos y condiciones del servicio de creación de certificados. (Ver Documento de Declaración de Practicas de Certificación para la ***CA Banrep*** en ubicado en http://www.banrep.gov.co/es/contenidos/page/declaraci-n-pr-cticas-certificaci-n-ca-banrep).

Normalmente, las credenciales obtenidas para comunicaciones B2B deberán ser exportadas a formato JKS o P12, para tal fin se debe seguir el documento "DSI-GI-97 Manual para la generación y transformación de credenciales emitidas por la CA BANREP" ubicado en la web del Banco de la República[5].

A continuación, se muestra un ejemplo de la forma en la que se debe diligenciar el formato BR-3-598-0 para solicitar un certificado B2B, para información del proceso que se debe seguir para la solicitud, remítase al Documento de Declaración de Practicas de Certificación para la ***CA Banrep*** en ubicado en: http://www.banrep.gov.co/es/contenidos/page/declaraci-n-pr-cticas-certificaci-n-ca-banrep:

[5] http://www.banrep.gov.co/sites/default/files/paginas/dsi_gi_97_2014.pdf



BR-3-598-0

NOVEDADES DEL SUSCRIPTOR
ENTIDAD DE CERTICACIÓN - CA BANREP

Fecha: Fecha de la solicitud.

Blanco: usuario normal)

Suscriptor		B2B¹	X	Procesos automáticos		Pruebas		Producción (genera cobro usuario sobre)	X
Actualizar datos		Incluir (Anexar Cédula)	X	Recuperar		Revocar		**Retirar Delegado	

Nombre y apellidos del Delegado PKI: Nombre del delegado PKI de la entidad.
Número de teléfono del Delegado PKI: Número telefónico del delegado PKI de la entidad.
Nombre y NIT de la Entidad Usuaria: Nombre y NIT de la Entidad incluido el digito de verificación, tal cual está en el contrato Sebra.

DATOS DEL SUSCRIPTOR / ENTIDAD

Nombre completo: No. Cédula:
Correo electrónico personal corporativo /

Nombre de la entidad abierta que emite el certificado²:
DN³:
Nota: Por favor adjuntar al mensaje el certificado digital (Archivo con extension .cer o .crt)

Observaciones:

1. INCLUIR: Por ser usuario nuevo
2. RECUPERAR: Por olvido de la contraseña del suscriptor - Por una sospecha o confirmación que la contraseña ha sido conocida por un tercero
3. REVOCAR: Por finalización del contrato laboral del suscriptor con la entidad usuaria - Por destitución o suspensión laboral del suscriptor - Por imposibilidad del suscriptor para cumplir sus obligaciones o cualquier otro acuerdo o ley que estén vigentes.
4. ACTUALIZAR DATOS Cuando cambia algún dato personal del suscriptor. **Se retira como delegado PKI pero no como suscriptor**

Marque los servicios autorizados para este usuario

CEDEC		DCV	
CENIT		Extractos por contingencia - CUD	
CUD		AFV - FINAGRO	
SEN - CIERRES		Indicadores Bancarios de Referencia - IBR	
SEN - TARIFAS		Antares - Provisión de Efectivo	
CONTINGENCIA - SWIFT		Servicio de Transferencia de Archivos - STA	

Seleccionar la aplicación con la que desea Interactuar.

6.2 SOLICITUD DE USUARIO GTA

Un usuario no interactivo hace referencia a un servidor de una entidad, el cual será solicitado por el formulario **BR-3-917-0** "Novedades del Suscriptor, Gestión de Transferencia de Archivos" (http://www.banrep.gov.co/sites/default/files/paginas/BR-3-917-0.xlsx) usuario tiene la característica que pertenece a la entidad y está a cargo del representante legal o su delegado ante el Banco de la República.

Los usuarios no interactivos tendrán la siguiente nomenclatura de "carga genérica", basando su estructura en tres partes:

- La primera parte está compuesta por la sigla de la herramienta de transferencia de archivos GTA.
- La segunda parte tiene el NIT de la entidad que desea enviar o recibir archivos con el Banco de la República con código de verificación.

- La tercera parte está asociado con el mnemónico del sistema de información del Banco de la República al cual se dirige la transferencia. Por ejemplo: CUD, DCV, STA, SWS, entre otros.

Algunos ejemplos de las cargas genéricas son:

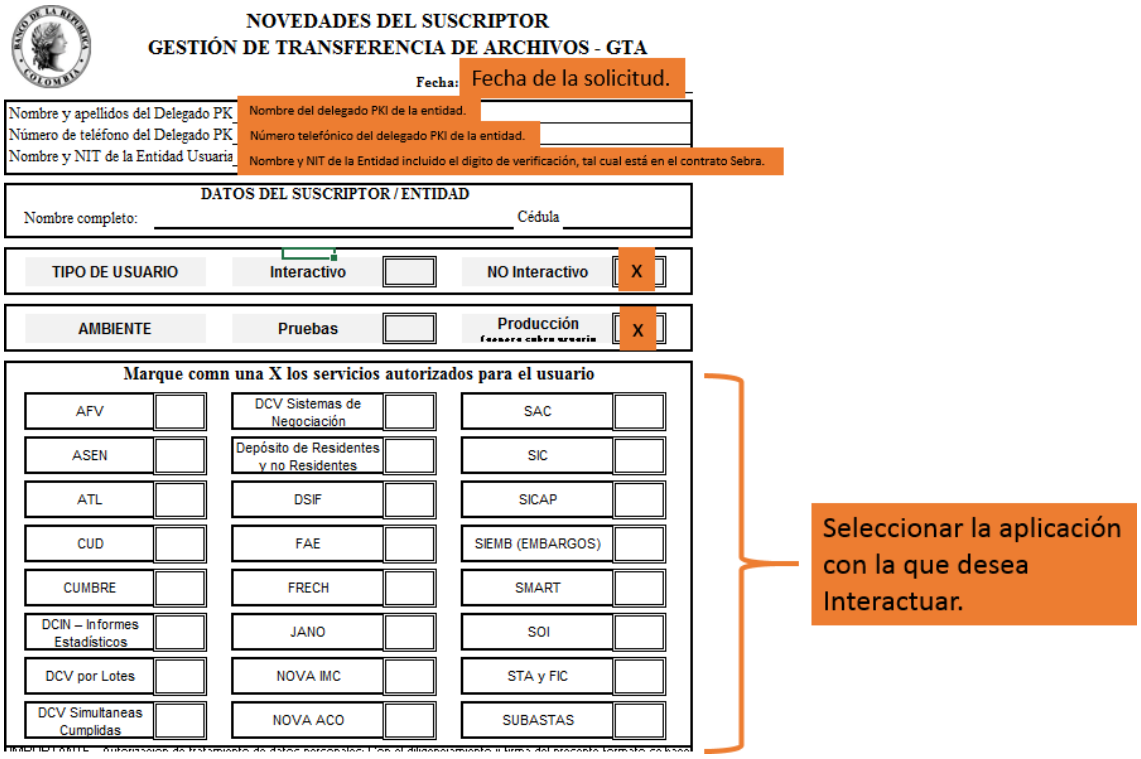
Usuario Genérico	Descripción
gta_8600029644_cud	Usuario de transferencia de archivos no interactivo del Banco de Bogotá entregando archivos al sistema de información CUD del Banco de la República.
gta_8300854261_dcv	Usuario de transferencia de archivos no interactivo de la Bolsa de Valores de Colombia entregando archivos al sistema de información DCV del Banco de la República.
gta_8300785126_sta	Usuario de transferencia de archivos no interactivo de la ACH Colombia entregando archivos al sistema de información STA del Banco de la República.

En el caso en que una entidad interactúe con varios sistemas de información del Banco de la República, se debe generar un usuario genérico para intercambiar información con cada uno de ellos.

A continuación se describen los pasos para solicitar el usuario no interactivo:

1. Generar el par de llaves (pública y privada) tipo SSH-2 RSA, con un tamaño de 2048 bits.
2. Diligenciar formulario **BR-3-917-0** "Novedades del Suscriptor, Gestión de Transferencia de Archivos" (http://www.banrep.gov.co/sites/default/files/paginas/BR-3-917-0.xlsx), seleccionando las aplicaciones del Banco con las que se desea interactuar.
3. Enviar por correo electrónico el formulario BR-3-917-0 y el archivo de la llave pública (.pub) firmados digitalmente por el delegado con responsabilidad administrativa.
4. El Banco de la República ejecuta la solicitud y envía por correo electrónico un archivo que contiene la clave del usuario genérico firmado y cifrado para el delegado con responsabilidad administrativa.
5. Realizar pruebas de conexión: El administrador de GTA se comunicará con el contacto técnico de la entidad para realizar pruebas de conexión.

A continuación, se muestra un ejemplo de la forma en la que se debe diligenciar el formato BR-3-917-0 para usuarios NO interactivos:



NOVEDADES DEL SUSCRIPTOR
GESTIÓN DE TRANSFERENCIA DE ARCHIVOS - GTA

Fecha: Fecha de la solicitud.

Nombre y apellidos del Delegado PK: Nombre del delegado PKI de la entidad.
Número de teléfono del Delegado PK: Número telefónico del delegado PKI de la entidad.
Nombre y NIT de la Entidad Usuaria: Nombre y NIT de la Entidad incluido el digito de verificación, tal cual está en el contrato Sebra.

DATOS DEL SUSCRIPTOR / ENTIDAD

Nombre completo: _____ Cédula _____

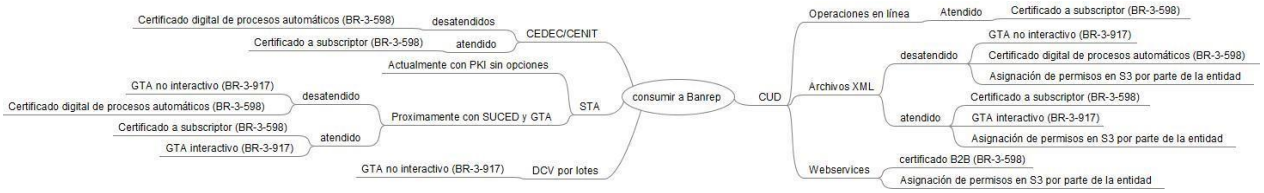
TIPO DE USUARIO	Interactivo		NO Interactivo	X
AMBIENTE	Pruebas		Producción	X

Marque comn una X los servicios autorizados para el usuario

AFV		DCV Sistemas de Negociación		SAC	
ASEN		Depósito de Residentes y no Residentes		SIC	
ATL		DSIF		SICAP	
CUD		FAE		SIEMB (EMBARGOS)	
CUMBRE		FRECH		SMART	
DCIN – Informes Estadísticos		JANO		SOI	
DCV por Lotes		NOVA IMC		STA y FIC	
DCV Simultaneas Cumplidas		NOVA ACO		SUBASTAS	

Seleccionar la aplicación con la que desea Interactuar.

7 CASOS DE USO PARA ESTE DOCUMENTO



8 CONTACTO

Para consultas y solicitudes de información por favor contactar con el Centro de Soporte Informático del Banco de la República al (+571)3431000.

9 HISTORIA DE CAMBIOS DEL REGISTRO

V 1.2 – DGT – JSZM. – Se incluyen imágenes con ejemplos de la forma de diligenciar el formato BR-3-598-0 para solicitar certificados B2B o procesos automáticos y el formato BR-3-917-0 para GTA. Así mismo, se aclara la implicación en costos que conlleva la solicitud de certificados digitales para servicios no interactivos.

V 1.1.1 – DGT-DGI-OZL. - Se actualizan las últimas versiones disponibles del sistema SUCED listadas en la sección 3.1 Descarga de SucedCommandLine.

V 1.1 – DGT-DGI-OZL. – Se incluye información de accesos requeridos para configurar ambiente de Homologación. Se incluye información del certificado empleado por el Banco para firma de las respuestas de servicios web. Se incluye configuración de la herramienta SoapUI para consumo de servicios web seguros. Se elimina la información relacionada con la instalación, configuración y operación básica de SUCED toda vez que esta información está contenida en el documento "**Manual y puesta en marcha de SUCED Command Line**" publicado en el portal https://caribe.banrep.gov.co/emisor