

FIRMADOR, VALIDADOR Y AUTENTICADOR

**GUIA TÉCNICA DE CONFIGURACIÓN DEL
SERVICIO SELLADO**

CANAL PRIVADO

VERSION 1.0



EE-FVA

Contenido

Introducción	3
Términos empleados.....	3
Paso 1: ¿Qué necesito antes de iniciar la configuración de las funcionalidades del servicio sellador?	3
Paso 2: Solicite el acceso al ambiente de pruebas del sellador	4
Solicitud de acceso al ambiente de pruebas.....	4
Resultado	4
Paso 3: Configure el sello	4
Paso 4: Ejecute los escenarios de pruebas	5
Servicios publicados	5
Escenarios de pruebas.....	5
Paso 5: Solicite el acceso al servicio en producción	5
Solicitud	5
Resultado	6
Paso 6: Verifique los requisitos para utilizar las funcionalidades del sellador.....	6
Paso 7: Consuma las funcionalidades del servicio Sellador	7
Anexos.....	8
Configuración de los servidores.....	8
Instalar certificado de agente electrónico de su entidad.....	9

Introducción

El propósito de este documento es facilitar la puesta en marcha en el ambiente de producción los servicios web que consuman las funcionalidades del servicio sellador de GAUDI, provisto por el Banco Central de Costa Rica por medio de una red privada.

Este documento permite a los departamentos de informática de cada entidad, verificar el estado de sus sistemas internos e identificar los ajustes necesarios para evitar contratiempos en la participación de la entidad en el servicio.

Términos empleados

- Para los fines del presente documento, se entenderá por:
 - ☐ SINPE: Sistema Nacional de Pagos Electrónicos.
 - ☐ COS: Centro de Operaciones del SINPE.
 - ☐ BCCR: Banco Central de Costa Rica.
 - ☐ GAUDI: Gestor de Autenticaciones Digitales.
 - ☐ Identidad de marca: Se entiende por identidad de marca un portal web transaccional en donde se brindan servicios que requieren el uso de funcionalidades del sellador. Por ejemplo, para el caso del BCCR, se tiene registrado como identidad de marca a Central Directo y los portales de las superintendencias (SUGEF, SUGESE y SUGEVAL).

Paso 1: ¿Qué necesito antes de iniciar la configuración de las funcionalidades del servicio sellador?

- **Un certificado de agente electrónico de la jerarquía nacional:** Le permitirá asegurar los servicios que va a exponer para que el BCCR los consuma, además este certificado le permitirá al BCCR identificar a la entidad que se encuentra realizando solicitudes de sellado.
- **Una identidad de marca que va a consumir el servicio:** En el proceso es necesario crear una identidad de marca, para esto es necesario el nombre y el logo de dicha identidad. El logo deberá tener un tamaño de 184 px de ancho x 84 px de alto, las extensiones permitidas son .jpg y .png.
- **Un sitio privado configurado en donde el servicio de su entidad va a consumir las funcionalidades del servicio sellador:** Este sitio privado de su entidad va a ser el encargado de solicitar los sellados. Consulte el Anexo "[Configuración de los servidores](#)".

- **Un sello electrónico custodiado:** Para configurar el servicio de sellado, es necesario tener un sello electrónico custodiado del servicio de persona jurídica. Para más información, consulte la [ayuda en línea de persona jurídica](#).

Paso 2: Solicite el acceso al ambiente de pruebas del sellador

Para poder consumir los servicios en el ambiente de producción es necesario valorar el desarrollo realizado contra un ambiente de pruebas.

Solicitud de acceso al ambiente de pruebas

La solicitud se debe realizar por medio del envío de un caso al **COS**, registrado por el Responsable de Servicios de la entidad. Se debe especificar los datos que se describen a continuación:

- Dirección **IP** de los **servidores** en ambiente de **producción**, desde donde se van a realizar las **invocaciones** a los **servicios** web expuestos por el **Sellador** para realizar las pruebas.
 - Si el servicio que realiza las invocaciones está instalado en un clúster de servidores, se debe proporcionar la dirección IP de cada uno de los nodos que conforman el clúster.

Resultado

- La IP del servidor donde se encuentran alojados los servicios web que la entidad deberá consumir del BCCR. Esta información es distinta para cada entidad:
 - La IP del clúster **firmadorinterno.bccr.fi.cr**.
- Las IPs de los servidores donde se publican los servicios de validación de certificados:
 - La IP de del servidor donde se publica el servicio OCSP **ocsp.sinpe.fi.cr**.
 - La IP de del servidor donde se publican los CRL'S hojas **fdi.sinpe.fi.cr**.
 - La IP de CRLs de las jerarquías superiores **www.firmadigital.go.cr**.

Paso 3: Configure el sello

1. Ingrese al sitio de [Central Directo](#) y autentiqúese.
2. Ingrese a la pestaña de Persona Jurídica y seleccione el negocio de Firma Digital.
3. Registre la identidad de marca.
4. Configure el sello: Seleccione la identidad de marca y procesada a configurarlo con el sello electrónico custodiado.

5. Apruebe el uso de GAUDI.

Para más información, consulte la [ayuda en línea de Firma Digital](#).

Paso 4: Ejecute los escenarios de pruebas

Para poder consumir los servicios en el ambiente de producción es necesario valorar el desarrollo realizado contra un ambiente de pruebas.

Servicios publicados

Los servicios publicados para sellar (**Web Service y WCF**) respetan las interfaces, tipos de datos y mensajes especificados en el estándar electrónico. Vea los **Archivos WSDL Sello Electrónico Custodiado para entregar a las entidades externas** que se encuentran publicada en la sección Documentos complementarios.

La funcionalidad de sellado de documentos se publica en estos servicios:

- **WCF:**
<https://firmadorinterno.bccr.fi.cr/wcfv2/Bccr.Fva.Entidades.AmbDePruebas.Sello.Wcf.SI/SelladorElectronicoConControlDeLlave.svc>
- **WS:**
<https://firmadorinterno.bccr.fi.cr/WebServices/Bccr.Fva.Entidades.AmbDePruebas.Sello.Ws.SI/SelladorElectronicoConControlDeLlave.asmx>

Escenarios de pruebas

El detalle de los escenarios de pruebas se encuentra en el documento **Escenarios del ambiente de pruebas para la funcionalidad de sellado** que se encuentra publicado en la sección Documentos complementarios.

Paso 5: Solicite el acceso al servicio en producción

Solicitud

La solicitud se debe realizar por medio del envío de un caso al **COS**, registrado por el Responsable de Servicios de la entidad.

Si para el uso en producción utiliza los mismos servidores utilizados para realizar las pruebas no es necesario abrir el acceso nuevamente, caso contrario, se debe especificar los datos que se describen a continuación:

- Dirección **IP** de los **servidores** en ambiente de **producción**, desde donde se van a realizar las **invocaciones** a los **servicios** web expuestos por el **Sellador**.
 - Si el servicio que realiza las invocaciones está instalado en un clúster de servidores, se debe proporcionar la dirección IP de cada uno de los nodos que conforman el clúster.

Resultado






- La IP del servidor donde se encuentran alojados los servicios web que la entidad deberá consumir del BCCR. Esta información es distinta para cada entidad:
 - La IP del clúster **firmadorinterno.bccr.fi.cr**.
- Las IPs de los servidores donde se publican los servicios de validación de certificados:
 - La IP de del servidor donde se publica el servicio OCSP **ocsp.sinpe.fi.cr**.
 - La IP de del servidor donde se publican los CRL'Shojas **fdi.sinpe.fi.cr**.
 - La IP de CRLs de las jerarquías superiores **www.firmadigital.go.cr**.

Paso 6: Verifique los requisitos para utilizar las funcionalidades del sellador

En Central Directo en las opciones de GAUDI se encuentra una opción para verificar los requisitos, es necesario verificar que todos los requisitos se cumplen, una vez que esté todo correcto se podrá utilizar el sellador en producción.

Los requisitos que cumplir son los siguientes:

Sellador

-  **Identities de Marca registradas**
 - **Detalle:** Es necesario tener registrada al menos una identidad de marca.
-  **Certificado de Agente Electrónico**
 - **Detalle:** Es necesario tener generado al menos un certificado de agente electrónico vigente.
-  **Sello Custodiado**
 - **Detalle:** Es necesario tener generado al menos un certificado de sello custodiado vigente.
-  **Configuración del Sellador**
 - **Detalle:** Es necesario tener configurado el sellador para una identidad de marca.
-  **Aprobación de Uso de GAUDI**
 - **Detalle:** Es necesario tener aprobado el uso de GAUDI.
-  **Pruebas del Sellador Completadas** ([Ver detalle](#))

Paso 7: Consuma las funcionalidades del servicio Sellador

Los servicios con los que cuenta el sellador se encuentran desarrollados utilizando tecnologías Web Service o WCF, en el ejercicio realizado en el ambiente de pruebas la entidad debe haber escogido entre alguno de estos, se recomienda que para el ambiente de producción se utilice la misma tecnología. Un cambio de tecnología podría provocar la presentación de escenarios desconocidos para la entidad, que podrían incidir en el tiempo de salida a producción.

Los servicios publicados para sellar (**Web Service y WCF**) respetan las interfaces, tipos de datos y mensajes especificados en el Estándar Electrónico.

- **WCF:**
<https://firmadorinterno.bccr.fi.cr/wcfv2/Bccr.Firma.Fva.Entidades.Sello.Wcf.SI/SelladorElectronicoConControlDeLlave.svc>
- **WS:**
<https://firmadorinterno.bccr.fi.cr/WebServices/Bccr.Firma.Fva.Entidades.Sello.Ws.SI/SelladorElectronicoConControlDeLlave.asmx>

Anexos

Configuración de los servidores

Se deberán realizar las configuraciones descritas en esta sección, en los servidores de la entidad que publican y consumen servicios del sellador:

1. Descargue los archivos necesarios para la configuración, estos archivos se encuentran publicados en la sección Documentos complementarios en el archivo **Jerarquía Persona Jurídica Producción para entregar a las entidades externas**.
2. Instale los certificados descargados en los servidores de su entidad.
3. Ejecute la **Guía para validar los CRLs de certificados de la jerarquía del ambiente de producción del firmador** que se encuentra publicada en la sección Documentos complementarios. La ejecución de esta guía garantiza que se tiene acceso a los CRLs en el ambiente de producción.
4. En el archivo host del servidor o los servidores desde donde se interactuará con el Sellador, se debe registrar:
 - ✓ El nombre **firmadorinterno.bccr.fi.cr** asociada a la IP de la cual fue entregada por el COS.
 - ✓ El nombre **ocsp.sinpe.fi.cr** asociada a la IP de la cual fue entregada por el COS.
 - ✓ El nombre **fdi.sinpe.fi.cr** asociada a la IP de la cual fue entregada por el COS.
 - ✓ El nombre **www.firmadigital.go.cr** asociada a la IP de la cual fue entregada por el COS.
5. Habilitar los accesos de telecomunicaciones, como se describe en la siguiente tabla:

Desde	Hacia	Puerto
Entidad	firmadorinterno.bccr.fi.cr (#.#.#.58)	443
Entidad	ocsp.sinpe.fi.cr (#.#.#.28)	80
Entidad	fdi.sinpe.fi.cr (#.#.#.28)	80
Entidad	www.firmadigital.go.cr (#.#.#.8)	80

6. Verificar los accesos que se abrieron en el paso anterior.
 - a. Esta verificación se debe realizar desde los servidores donde se van a realizar las **invocaciones** a los **servicios** web expuestos por el **Sellador**. Se debe abrir una consola y ejecutar telnet a las siguientes IP's y puertos.

Desde	Hacia	Puerto
Entidad	firmadorinterno.bccr.fi.cr (###.58)	443
Entidad	ocsp.sinpe.fi.cr (###.28)	80
Entidad	fdi.sinpe.fi.cr (###.28)	80
Entidad	www.firmadigital.go.cr (###.8)	80

- b. Verificar que se puede validar el estado de revocación de un certificado, para esto ejecutar la “Guía para validar los CRLs de certificados de la jerarquía del ambiente de producción del firmador”, la ejecución de esta guía garantiza que se tiene acceso a los CRLs en el ambiente de producción.
7. Recomendamos revisar el documento **Base de datos de conocimiento de la configuración de los servicios** que se encuentra publicado en la sección Documentos complementarios. Este documento contiene información que hemos recolectado de la experiencia de otras instituciones conectándose al firmador.

Instalar certificado de agente electrónico de su entidad

El certificado de agente electrónico que se generó para asegurar el sitio de su entidad debe instalarse en los servidores, puede seguir los siguientes pasos:

1. Ejecute una ventana de comando (CMD) y diríjase a la carpeta donde se encuentra la llave pública del certificado de agente electrónico, este archivo tiene extensión “.cer”.
2. Ejecute el comando “C:\WINDOWS\System32\certreq-accept {nombreDelCertificado}.cer”
3. Verifique en el store personal de certificados o en HSM (dependiendo del proveedor criptográfico utilizado) que se generó la llave privada del certificado de agente electrónico.

