BANCO CENTRAL DE COSTA RICA

FIRMADOR, VALIDADOR Y AUTENTICADOR

NORMA TÉCNICA

CONFIGURACIÓN DE GAUDI PARA EL SERVICIO VALIDADOR DE DOCUMENTOS FIRMADOS CANAL PRIVADO

Público

NT-FVA

Tabla de Contenido

1. 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 validador de documentos 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.

2. Prerrequisitos

- Validar la funcionalidad a usar. Las funcionalidades están disponibles en la página Funcionalidades Disponibles GAUDI
- Tener conocimientos básicos de certificados digitales e infraestructura de llave pública.
- Tener conocimientos de programación y consumo de servicios Web como WFCs, WebServices y servicios tipo API REST.
- Conocimiento en la Norma Técnica - Estándar Electrónico GAUDI, pues acá se describen los posibles métodos a usar en el servicio.

3. Términos empleados

- Para los fines del presente documento, se entenderá por:
  - ⊡ SINPE**:** Sistema Nacional de Pagos Electrónicos.
  - ⊡ OMS: Operación y Monitoreo del SINPE.
  - ⊡ BCCR: Banco Central de Costa Rica.
  - ⊡ GAUDI**:** Gestor de Autenticaciones Digitales.
  - ⊡ Identidad de marca: Se entiende por identidad de marca portal web**1** en donde se brindan servicios que requieren el uso de funcionalidades del validador de documentos firmados. 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). Otro ejemplo: la empresa "Banco Alianza de Costa Rica S.A." podría tener una identidad de marca para su sitio https://www.bancoalianza.fi.cr/ que se llame "Portal Banco Alianza".

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

- **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 validación de documentos. El certificado de agente electrónico solo puede ser gestionado por el

---

1 Puede ser un sitio público o privado o una aplicación que debe ser configurada usando el certificado de agente electrónico de la entidad.

representante legal de la entidad, si desea ver más detalles sobre este requerimiento puede revisarlo en este enlace.

Para consumir los servicios de GAUDI, es necesario asegurar la comunicación con el certificado de PRODUCCIÓN de Agente Electrónico de la entidad.

- **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 pixels de ancho x 84 pixels de alto, las extensiones permitidas son .jpg y .png.
- **Un sitio privado[2] configurado en donde el servicio de su entidad va a consumir las funcionalidades del servicio validador**: Este sitio privado de su entidad va a ser el encargado de solicitar las validaciones. Consulte el Anexo "Configuración de los servidores".

5. Paso 2: Configure la identidad de marca

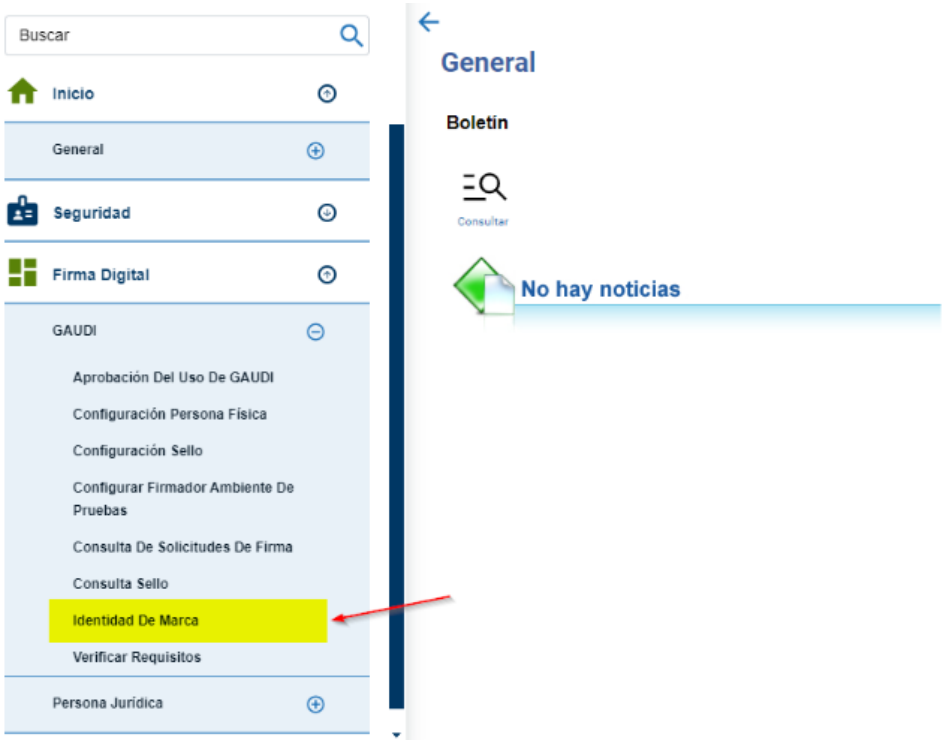
Para configurar la identidad de marca realice los siguientes pasos:

1. Ingrese al sitio de Central Directo y autentíquese.
2. Ingrese a la pestaña de Entidades Jurídicas, de clic en el bloque de "Firma Digital" y seleccione una de las siguientes opciones según corresponda:
    a. Ingrese en la entidad donde es usuario: Seleccione la entidad que representa.
    b. Suscriba una entidad donde usted es Representante Legal Principal o Autorizado: Si la entidad que representa no se muestra en la opción anterior, ingrese la cédula jurídica de la entidad y siga las indicaciones.

[2] *Puede ser un sitio público o privado o una aplicación que debe ser configurada usando el certificado de agente electrónico de la entidad.*

Cree la identidad de marca: Para hacerlo seleccione:

a. Ir al menú “**Firma Digital**” -> “**GAUDI**” -> “**Identidad de Marca**”



b. Clic en la acción “Solicitar”, en la ventana siguiente ingrese el nombre y logo[3] deseado

Para más información, consulte la ayuda en línea de Firma Digital.

6. Paso 3: Solicite el acceso al servicio en producción[3]

6.1.1. Solicitud

La solicitud se debe realizar por medio del envío de un caso al el área de Operación y Monitoreo del Sinpe (OMS), registrado por el **Responsable de Servicios** de la entidad. Se debe especificar los datos que se describen a continuación:

- Dirección **IP** de los **servidores** desde donde se van a realizar las **invocaciones** a los **servicios** web expuestos por el **Validador de documentos** en la red interna del SINPE.
  - 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.

[3] ***Nota:*** *si la entidad ya cuenta con el servicio Firmador GAUDI (para persona física) en el canal privado y va a usar los mismos servidores para invocar al Web Service de validación de documentos firmados, no ocupa incluir un caso al el área de Operación y Monitoreo del Sinpe (OMS), pues es el mismo clúster nuestro (firmador.fdi.cr) el que hospeda dicho Web Service y por tanto ya los permisos de invocación estarían dados a dichos servidores.*

6.1.2. 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 **firmador.gaudi.wan.sinpe.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**

7. Paso 4: Consuma las funcionalidades del servicio Validador de documentos

Los servicios con los que cuenta el Validador se encuentran desarrollados utilizando tecnologías Web Service o WCF o API REST. El desarrollo de su entidad debe estar hecho respetando las interfaces, tipos de datos y mensajes especificados en el **estándar electrónico**, según sea su tipo de consumo (Web Service, WCF Autenticador y API REST).

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

- **WCF**: https://firmador.gaudi.wan.sinpe.fi.cr/wcfv2/Bccr.Firma.Fva.Entidades.ValidarDocumento.Wcf.SI/ValidadorDeDocumentos.svc

- **WS**: https://firmador.gaudi.wan.sinpe.fi.cr/WebServices/Bccr.Firma.Fva.Entidades.ValidarDocumento.Ws.SI/ValidadorDeDocumentos.asmx

- **API:** (En el caso del servicio API para visualizar la documentación de los métodos descargar el **archivo**)

https://servicios-rest-validador.gaudi.wan.sinpe.fi.cr/FVA/Bccr.Firma.Fva.Entidades.ValidarDocumento.API

8. Anexos

8.1. 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 validador de documentos:

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 Validador de documentos, se debe registrar:
   - ✓ El nombre **firmador.gaudi.wan.sinpe.fi.cr** asociada a la IP de la cual fue entregada por el área de Operación y Monitoreo del Sinpe (OMS).
   - ✓ El nombre **ocsp.sinpe.fi.cr** asociada a la IP de la cual fue entregada por el el área de Operación y Monitoreo del Sinpe (OMS).
   - ✓ El nombre **fdi.sinpe.fi.cr** asociada a la IP de la cual fue entregada por el el área de Operación y Monitoreo del Sinpe (OMS).
   - ✓ El nombre **www.firmadigital.go.cr** asociada a la IP de la cual fue entregada por el el área de Operación y Monitoreo del Sinpe (OMS).

5. Habilitar los accesos de telecomunicaciones, como se describe en la siguiente tabla:

Desde	Hacia	Puerto
Entidad	firmador.gaudi.wan.sinpe.fi.cr (#.#.#.38)	443
Entidad	ocsp.sinpe.fi.cr (#.#.#.28)	80
Entidad	fdi.sinpe.fi.cr (#.#.#.28)	80
Entidad	hub.gaudi.sinpe.fi.cr, actualizador.gaudi.sinpe.fi.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 **Validador.** Se debe abrir una consola y ejecutar telnet a las siguientes IP´s y puertos.

Desde	Hacia	Puerto
Entidad	firmador.gaudi.wan.sinpe.fi.cr (#.#.#.38)	443
Entidad	ocsp.sinpe.fi.cr (#.#.#.28)	80
Entidad	fdi.sinpe.fi.cr (#.#.#.28)	80
Entidad	hub.gaudi.sinpe.fi.cr, actualizador.gaudi.sinpe.fi.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.

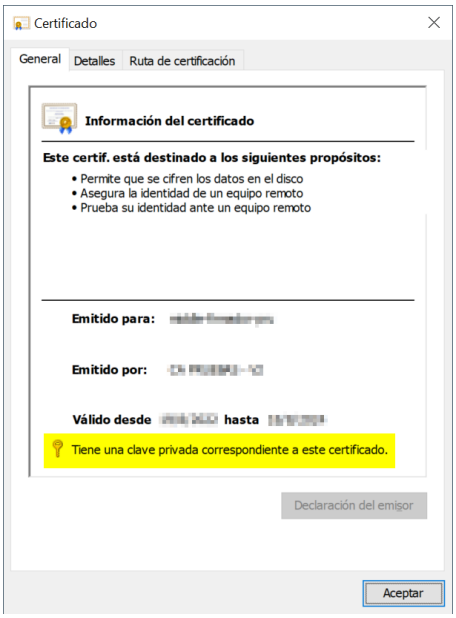
7. Recomendamos revisar el documento Base de datos de conocimiento de la configuración de los servicios que se encuentra publicado en la sección Documentos complementarios. Este documento contiene información que hemos recolectado de la experiencia de otras instituciones conectándose al Firmador GAUDI.

8.2. 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.

4. Garantizar que el certificado queda con la llave privada instalada y además el usuario del pool o de la aplicación debe tener permisos de lectura sobre dicha llave.



En caso de problemas, buscar información en el documento Base de datos de conocimiento de la configuración de los servicios