BANCO CENTRAL DE COSTA RICA

DIVISIÓN SISTEMAS DE PAGO

FIRMADOR, VALIDADOR Y AUTENTICADOR

GUIA TÉCNICA DE CONFIGURACIÓN DEL SERVICIO FIRMADOR PARA PERSONA FISICA

CANAL PÚBLICO (INTERNET)

VERSION 1.1

sinpe

EE-FVA

Contenido

Introducción

El propósito de este documento es facilitar la puesta en marcha en el **AMBIENTE DE PRODUCCIÓN**, de los servicios web que consumen las funcionalidades de GAUDI, provisto por el Banco Central de Costa Rica por medio de INTERNET.

Este documento permite a los departamentos de informática de cada Suscriptor, verificar el estado de sus sistemas internos e identificar los ajustes necesarios para evitar contratiempos en la implementación del firmador GAUDI en personas físicas.

Términos empleados

Para los fines del presente documento, se entenderá por:

- **BCCR**: Banco Central de Costa Rica.
- **GAUDI**: Gestor de Autenticaciones y Firmas Digitales del Banco Central.
- **Suscriptor**: Entidad que desea implementar el uso de los servicios de firma digital GAUDI.
- **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 firmador GAUDI. 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 Firmador?

- **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 firma o autenticación. El certificado de agente electrónico solo puede ser gestionado por el representante legal de la entidad, si desea ver más detalles sobre este requerimiento puede revisarlo en este enlace.
- **Identificar la identidad de marca que va a consumir el servicio**: En el proceso es necesario crear una identidad de marca, para esto es necesario el definir 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 público configurado en donde el servicio de la entidad va a consumir las funcionalidades del servicio Firmador y además se le van a hacer notificaciones**: Este sitio público va a ser el encargado de solicitar las firmas y autenticaciones; además el servicio Firmador GAUDI le va a notificar el resultado de dichas solicitudes al sitio que se indique en la configuración. No necesariamente el sitio que solicita y recibe las notificaciones debe ser el mismo. Consulte el Anexo "Configuración de los servidores".

  Es necesario que el servicio de notificación cumpla con el estándar electrónico. Consulte el Anexo "Publicar el servicio de notificaciones".

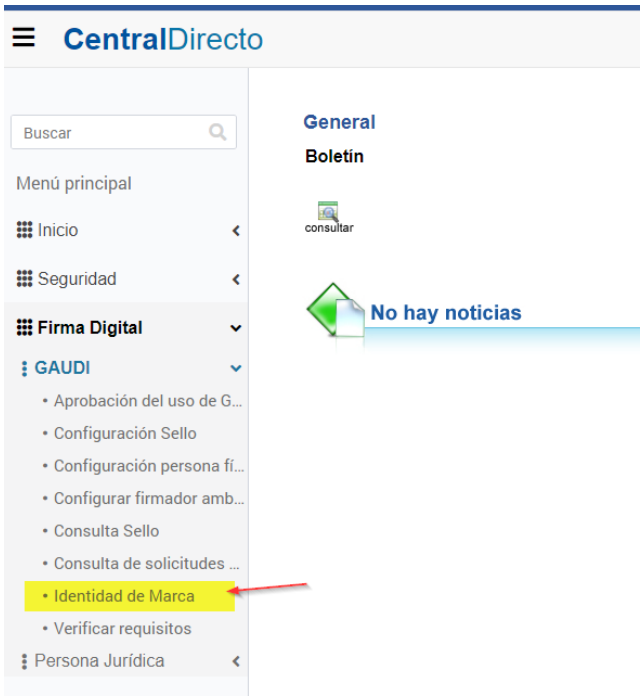
Paso 2: Configure el Firmador para el ambiente de pruebas

Para poder consumir los servicios en el ambiente de producción es necesario valorar el desarrollo realizado contra un ambiente de pruebas. Para realizar este proceso realice los siguientes pasos:

1. Ingrese al sitio de Central Directo y autentíquese[1].
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.

[1] La persona por autenticarse debe ser el representante legal de la institución o un asistente técnico nombrado por él.

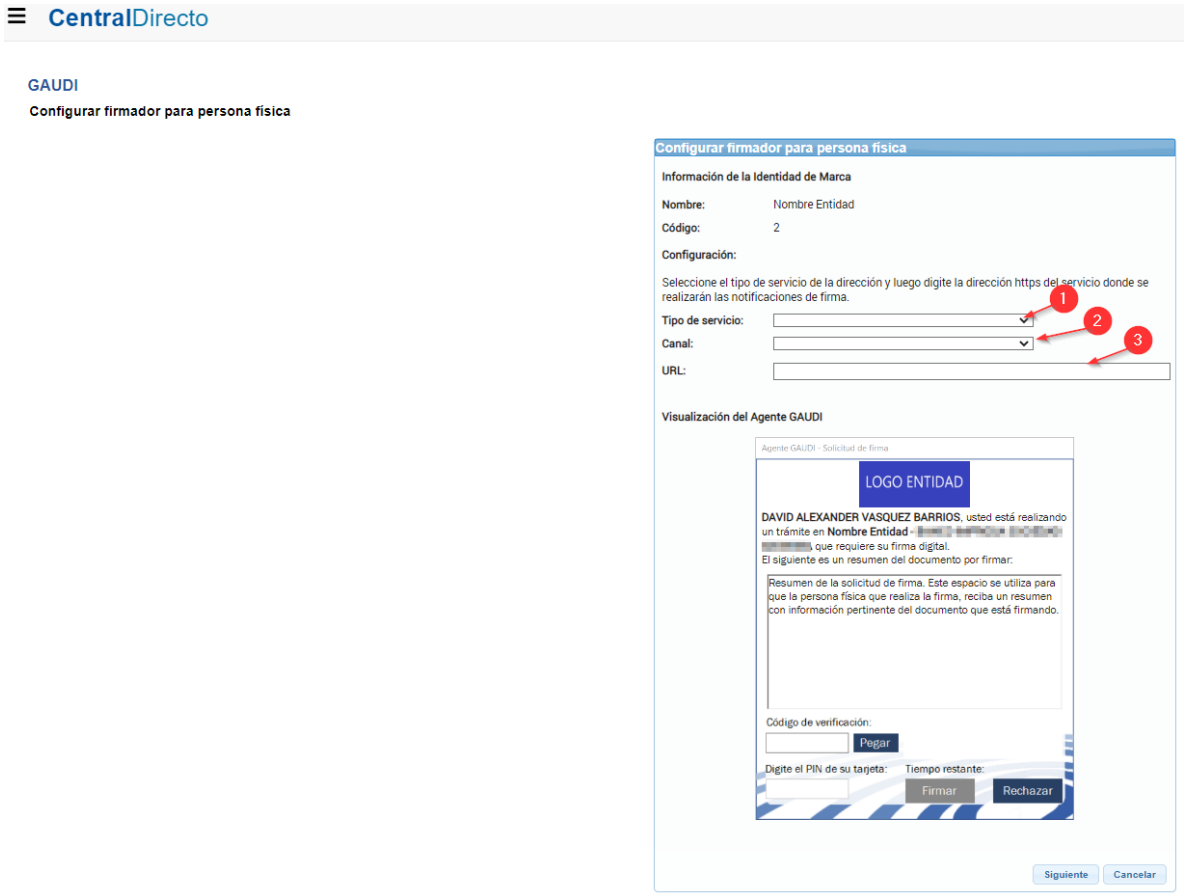
3. Configure la Identidad de Marca:
    a. Cree la identidad de marca: Para hacerlo seleccione:
        i. Ir al menú Firma Digital -> GAUDI -> Identidad de Marca



        ii. Clic en la opción Solicitar, en la ventana siguiente ingrese el nombre y logo[2] deseado

[2] Se permiten logos únicamente de 184 x 84 px

b. Configure la identidad de marca creada: Seleccione: Firma Digital -> GAUDI -> "Configuración persona física" y configure la identidad de marca con el canal público y la URL de notificación del ambiente de pruebas, este URL debe ser en el puerto 8443.



4. Apruebe (habilite) el uso de GAUDI.

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

Paso 3: Ejecute los escenarios de PRUEBAS

Publico

El ambiente de pruebas publica los servicios para firmar (Web Service y WCF Firmador) y autenticar (Web Service y WCF Autenticador) respetando las interfaces, tipos de datos y mensajes especificados en el estándar electrónico.

La funcionalidad de **FIRMA DIGITAL** de documentos se publica en estos servicios:

- **WCF:** https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Fva.Entidades.AmbienteDePruebas.Wcf.BS/Firmador.svc

- **WS:** https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Fva.Entidades.AmbienteDePruebas.Ws.BS/Firmador.asmx

Fecha de última modificación: 18/enero/2024

La funcionalidad de **AUTENTICACIÓN** con firma digital se publica en estos servicios:

- **WCF:** https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Fva.Entidades.AmbienteDePruebas.Wcf.BS/Autenticador.svc

- **WS:** https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Fva.Entidades.AmbienteDePruebas.Ws.BS/Autenticador.asmx

Escenarios de pruebas

La documentación respectiva de los escenarios de pruebas que se deben realizar se encuentra publicada en la sección Documentos complementarios en el archivo **Escenarios del ambiente de pruebas para la funcionalidad de firma y autenticación.**

Paso 4: Configure el Firmador para el ambiente de producción

Los servicios con los que cuenta el Firmador se encuentran desarrollados utilizando tecnologías Web Service o WCF. Los servicios publicados para firmar **(Web Service y WCF Firmador)** y autenticar **(Web Service y WCF Autenticador)** respetan las interfaces, tipos de datos y mensajes especificados en el Estándar Electrónico.

La funcionalidad de **FIRMA DIGITAL** de documentos se publica en estos servicios:

- **WCF**: https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Firma.Fva.Entidades.Wcf.BS/Firmador.svc

- **WS**: https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Firma.Fva.Entidades.Ws.BS/Firmador.asmx

La funcionalidad de **AUTENTICACIÓN** con firma digital se publica en estos servicios:

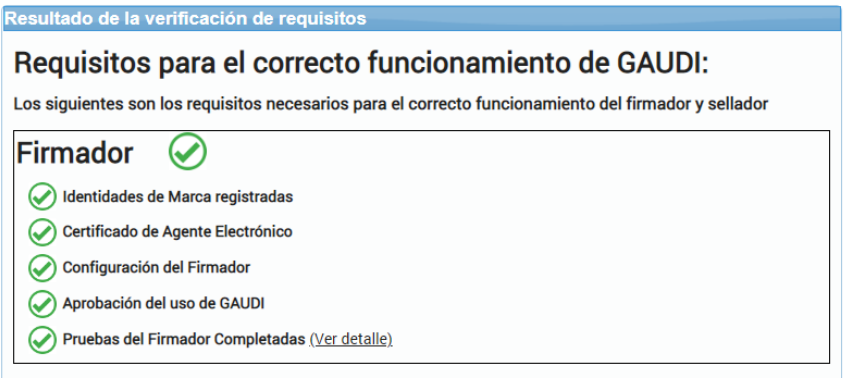
- **WCF**: https://firmadorexterno.bccr.fi.cr/wcfv2/Bccr.Firma.Fva.Entidades.Wcf.BS/Autenticador.svc

- **WS**: https://firmadorexterno.bccr.fi.cr/WebServices/Bccr.Firma.Fva.Entidades.Ws.BS/Autenticador.asmx

Paso 5: Verifique los requisitos para utilizar las funcionalidades del firmador

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

Los requisitos que cumplir son los siguientes:



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 firmador:

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.

Publicar el servicio de notificaciones

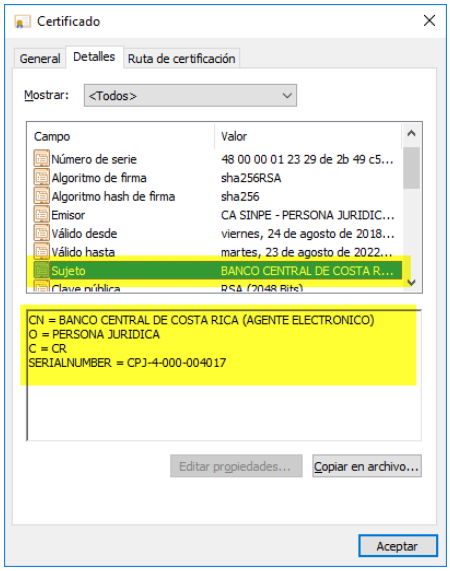
1. La implementación de este servicio es indispensable para que la entidad pueda recibir los resultados de las solicitudes de firma de documentos y de autenticación de personas físicas.
    - El servicio de notificación debe estar asegurado con el certificado de agente electrónico de la entidad.

- El servicio debe ser publicado por el puerto 8443.
- El servicio de notificación deberá implementarse siguiendo las interfaces, tipos de datos y mensajes especificados en el estándar electrónico en la sección Servicios Publicados por las Entidades, consulte los **Archivos WSDL (Firmador, Autenticador, Verificador y ResultadoDeSolicitud) tipo WCF para entregar a las entidades externas**, que se encuentran publicados en la sección Documentos complementarios.
  - Debe estar preparado para manejar archivos de hasta 20 megas.
  - Particularmente la clase "ResultadoDeFirma" debe tener el NameSpace "**Bccr.Firma.Fva.Entidad.Contenedores**".
  - Además, el método "NotifiqueLaRespuesta", debe recibir un parámetro llamado "elResultado" de tipo "ResultadoDeFirma" (se debe respetar el nombre del parámetro).

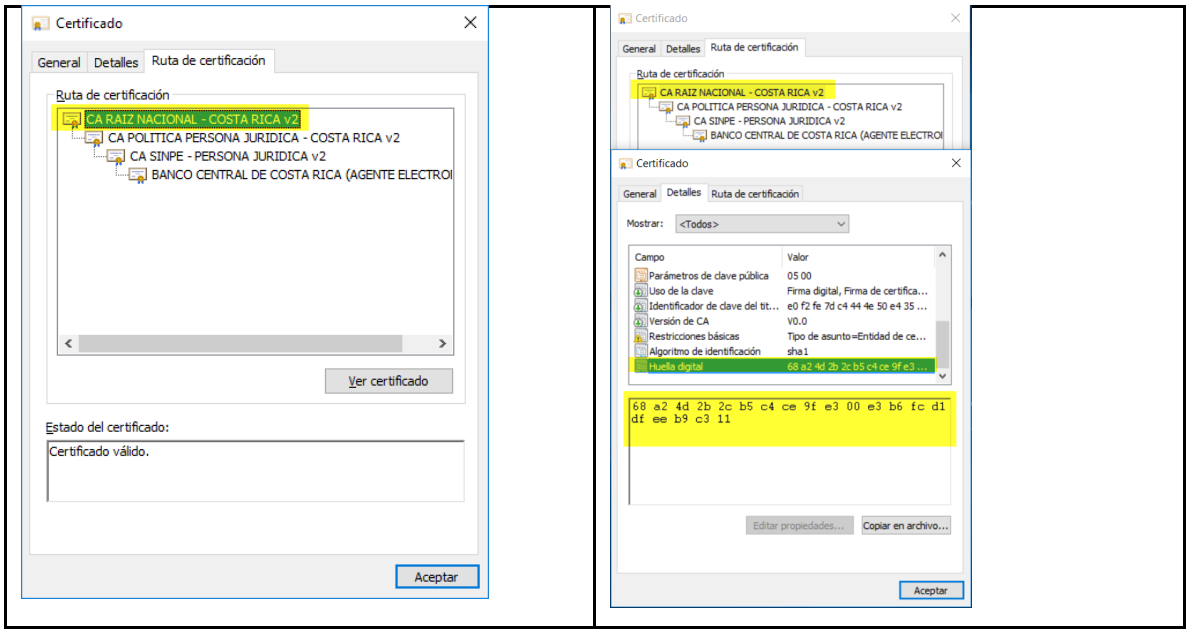
```
<ServiceContract()>
0 references
Public Class ResultadoDeSolicitud
    <OperationContract()>
    0 references
    Public Sub NotifiqueLaRespuesta(elResultado As ResultadoDeFirma)
```

- El servicio de notificación **puede** ser utilizado para notificar a una o varias identidades de marca.
- Recomendamos revisar el documento **Base de datos de conocimiento de la configuración de los servicios** que se encuentra publicado en la sección Documentos complementarios.
  - Si el servicio de notificación va a ser publicado en un servidor web IIS es necesario verificar el punto: "Solución al error The remote server returned an unexpected response: (413) Request Entity Too Large", cuando aparece en el trace del WCF o en la bitácora central del Sinpe, en el servicio de notificación" en dicho documento de la base de conocimiento.
  - Si requiere habilitar el uso de TLS 1.2 es necesario verificar el punto "Configuración para que la aplicación utilice TLS 1.2" de dicho documento.

- El servicio de notificación de la entidad debe garantizar que sólo puede ser consumido con el certificado de agente electrónico que el Banco Central de Costa Rica tiene para ese efecto. En particular, dicho certificado debe:
    - Tener el sujeto: "CN=BANCO CENTRAL DE COSTA RICA (AGENTE ELECTRONICO), O=PERSONA JURIDICA, C=CR, SERIALNUMBER=CPJ-4-000-004017". Al realizar la validación, respetar las mayúsculas y el espacio después de cada coma (,).



    - La huella del **certificado raíz de la jerarquía** a la que pertenece el certificado de agente del BCCR, sea la siguiente: "68A24D2B2CB5C4CE9FE300E3B6FCD1DFEEB9C311". Al realizar la validación la huella debe ir en mayúsculas y sin espacios.

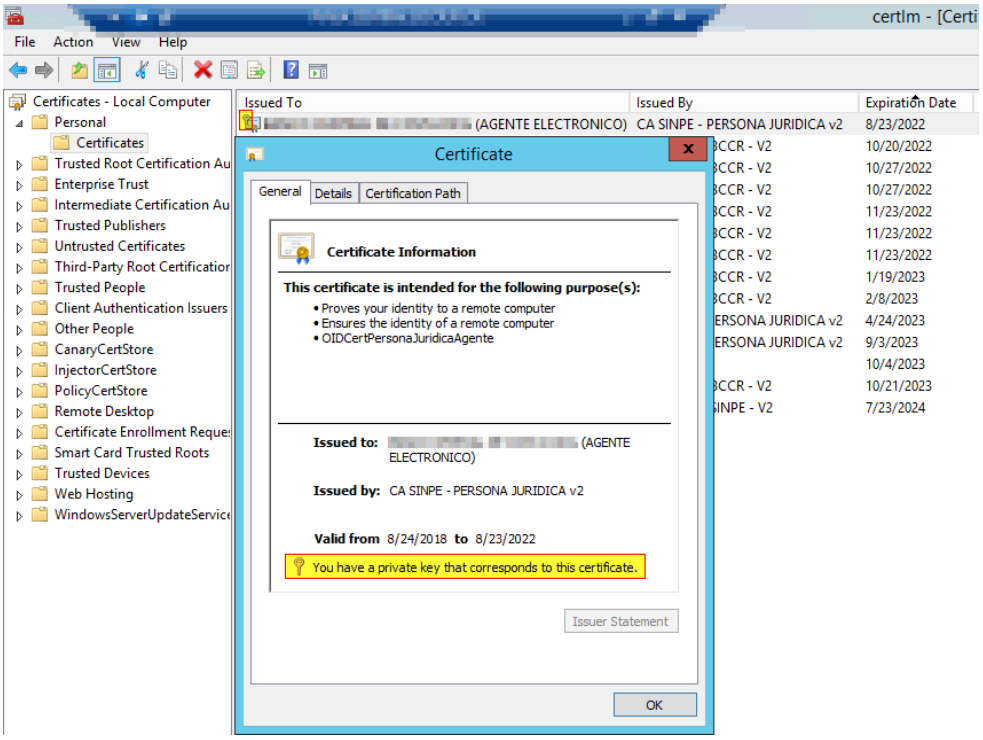


- Debe validarse que sea vigente y no haya sido revocado.

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 visualiza **el ícono de la llave privada** del certificado de agente electrónico.


certlm - [Certi
File Action View Help
Certificates - Local Computer
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Other People
CanaryCertStore
InjectorCertStore
PolicyCertStore
Remote Desktop
Certificate Enrollment Reque
Smart Card Trusted Roots
Trusted Devices
Web Hosting
WindowsServerUpdateServic
Issued To
Issued By
Expiration Date
(AGENTE ELECTRONICO)
CA SINPE - PERSONA JURIDICA v2
8/23/2022
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Ensures the identity of a remote computer
• OIDCertPersonaJuridicaAgente
Issued to:
(AGENTE ELECTRONICO)
Issued by: CA SINPE - PERSONA JURIDICA v2
Valid from 8/24/2018 to 8/23/2022
You have a private key that corresponds to this certificate.
Issuer Statement
OK