BANCO CENTRAL DE COSTA RICA

DIVISIÓN SISTEMAS DE PAGO

AMBIENTE DE PRUEBAS
SERVICIO FIRMADOR

FIRMADOR, VALIDADOR Y AUTENTICADOR

PREGUNTAS FRECUENTES

VERSION 1.6

sinpe

PF-FVA

Contenido

Introducción

Durante la fase de utilización del ambiente de pruebas por parte de las entidades financieras, se han generado consultas, que, en conjunto con el equipo de expertos del Banco Central de Costa Rica, se han ido solventando. Esto como parte del apoyo que se les brinda a las entidades para lograr una integración de los sistemas de las mismas con el servicio Firmador.

Es de este proceso que se ve la necesidad de crear un documento de preguntas frecuentes, el cual puede ser solicitado al Centro de Operaciones del SINPE, por las entidades que se encuentran interesadas en utilizar el ambiente de pruebas.

Términos empleados

- Para los fines del presente documento, se entenderá por:
  - ⊡ BCCR: Banco Central de Costa Rica.
  - ⊡ SINPE: Sistema Nacional de Pagos Electrónicos.
  - ⊡ GAUDI: Gestor de Autenticaciones Digitales.
  - ⊡ COS: Centro de Operaciones del SINPE.

Sobre el servicio Firmador

1. ¿Qué es el Servicio Firmador?
   Es un servicio desarrollado por el Banco Central de Costa Rica, que permite la implementación de firma digital, por parte de entidades asociadas al SINPE que tengan poco o nulo conocimiento de este tema. Las entidades pueden acceder a distintos servicios únicamente configurando los portales que necesitan utilizarlos.

2. ¿Qué es FVA?
   Son las siglas del servicio, que significan Firmador Validador Autenticador.

3. ¿Por qué se recomienda la utilización de GAUDI?
   La utilización de GAUDI abstrae a las entidades de la complejidad de realizar desarrollos para firma digital. A nivel nacional se ha notado que muchos de los desarrollos actuales tienen problemas de diversa índole, desde lo más simples como verificar la validez de un certificado, hasta la creación de firmas electrónicas de formato avanzado.

   Con GAUDI se tiene el respaldo del BCCR, el cual cuenta con una infraestructura robusta y segura para la comunicación con las entidades, además de que se garantiza contar con servicios de alta disponibilidad y creación de firmas electrónicas avanzadas basadas en estándares internacionales.

4. ¿Qué servicios ofrece el Firmador?
   Se brindan servicios enfocados para persona física, los cuales se detallan a continuación:
   - ✓ Firma electrónica avanzada de documentos XML, utilizando los tipos co-firma y contrafirma.

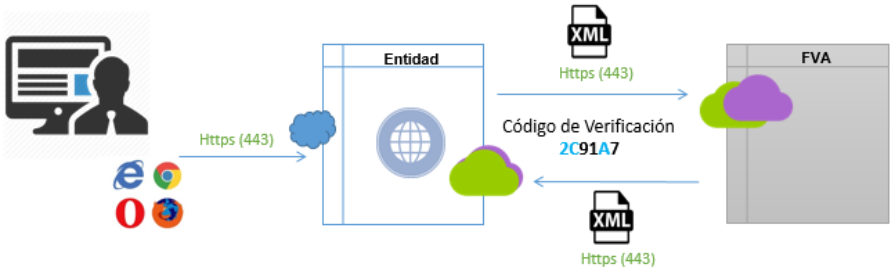
- ✓ Firma electrónica avanzada de documentos ofimáticos de Microsoft, para los documentos que cuenten con las extensiones .docx, .xlsx y .pptx.
- ✓ Firma electrónica avanzada de documentos ofimáticos de Formato de Documento Abierto (ODF, por sus siglas en inglés), para los documentos con extensión .odt, .ods y .odp.
- ✓ Firma electrónica avanzada de documentos PDF.
- ✓ Autenticación de un suscriptor, este se utiliza para el ingreso a portales, ya que permite verificar si un usuario es quien dice ser.

5. ¿Cómo funciona el Servicio Firmador?

La entidad interesada debe realizar las configuraciones necesarias en el portal o portales que van a requerir utilizar firma. El funcionamiento se describirá con un ejemplo de una solicitud de firma digital:

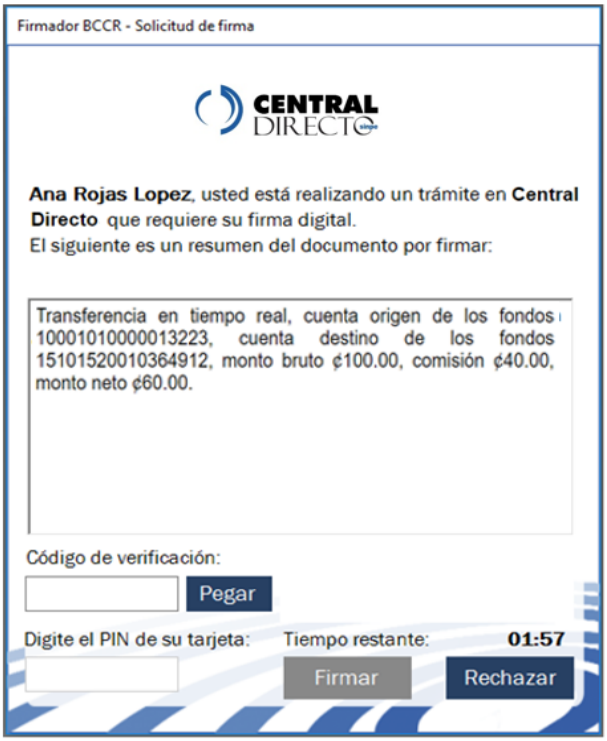
a. Un usuario ingresa a un portal web de una entidad que utiliza el Servicio Firmador.

b. Para realizar una firma digital, la entidad consume el servicio de firma (según corresponda) del Firmador, el cual le indica un código de solicitud y un código de verificación.



c. La entidad le muestra un resumen al usuario, el cual debe contener el código de verificación que se le entregó en el paso 1.

d. Al usuario se le despliega la ventana del Agente GAUDI, donde se le solicita la firma, colocar el código de verificación y el PIN de la tarjeta inteligente.



e. El servicio Firmador le notifica a la entidad el resultado del proceso.

6. ¿Un documento puede ser firmado digitalmente por varias personas?
   Si, un documento que ya ha sido firmado puede ser firmado por otra persona. El flujo de trabajo que requiere firmas múltiples debe ser diseñado por la entidad.

7. ¿Existe un documento donde se indique el detalle técnico del servicio Firmador?
   El Firmador para personas físicas cuenta con un estándar electrónico donde se describe el detalle técnico, requisitos y configuraciones, que debe realizar una entidad para hacer uso de los servicios. Este documento puede ser solicitado al COS.

Sobre el ambiente de pruebas

8. ¿Qué es el ambiente de pruebas?
   El ambiente de pruebas está diseñado para que las entidades realicen simulaciones del consumo de los servicios web expuestos por el Firmador. Permite que las entidades ejerciten todos los escenarios y las configuraciones que deben realizar, tanto a nivel de desarrollo de software como a nivel de telecomunicaciones, así como que se familiaricen con la utilización del servicio Firmador, antes de la puesta en producción.

9. ¿Cómo puedo acceder al ambiente de pruebas?
   Se debe realizar una solicitud al COS.

10. ¿Cómo debo proceder si se me presenta algún error al utilizar el ambiente de pruebas?
    Se debe designar una persona en la entidad para que se comunique con el COS, el cual se encargará de atender las inquietudes de la entidad. Si el COS no puede resolver el problema

de inmediato, se abrirá un caso para que el equipo técnico realice el análisis respectivo y le brinde una solución a la entidad.

11. ¿Existe un documento de sirva como guía para utilizar el ambiente de pruebas?
    El BCCR creó un documento llamado "Detalles técnicos del ambiente de pruebas para entidades", el cual describe todos los detalles a tomar en cuenta para que la entidad consuma servicios del ambiente de pruebas del servicio Firmador. Este documento se le puede solicitar al COS.

Sobre la comunicación segura

12. ¿Qué es TLS 1.2?
    TLS (Transport Layer Secure) es un protocolo criptográfico que permite proteger los datos que viajan entre las aplicaciones, mediante la creación de un canal seguro entre el cliente y el servidor. Existen diversas versiones de TLS (también llamado SSL/TLS), pero la recomendada actualmente es la versión TLS 1.2, debido a que en esta se han solventado incidentes de seguridad que se presentaron en las versiones posteriores.

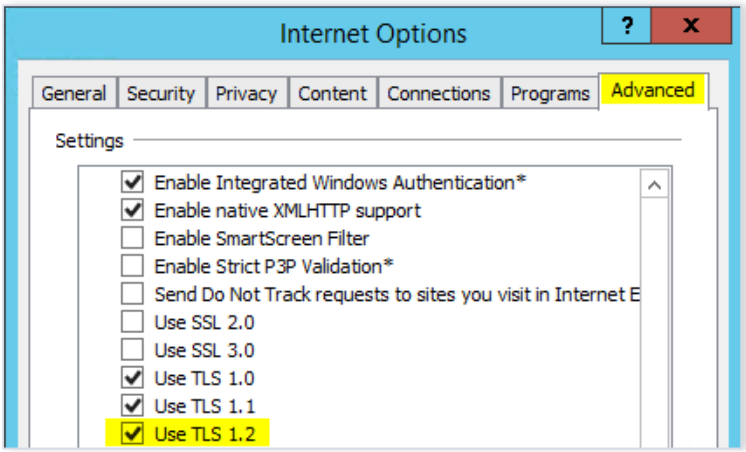
13. ¿Qué aspectos debo tomar en cuenta para establecer una comunicación segura?
    Además de tener una aplicación que cuente con la capacidad de utilizar el protocolo seguro TLS 1.2, se debe considerar:

    - ✓ El servicio web (WCF o Web Service) debe encontrarse configurado para utilizar seguridad de transporte.
    - ✓ Al consumir servicios web seguros, se debe realizar una configuración a nivel de Web.Config que coincida con la realizada al crear los servicios que se están consumiendo.
    - ✓ La versión del sistema operativo instalado en el servidor web que va a alojar la aplicación, debido a que existen sistemas operativos que no utilizan por defecto TLS 1.2 o del todo no lo soportan.
    - ✓ La utilización de TLS 1.2 debe encontrarse habilitada en el servidor.
    - ✓ Se debe contar con un certificado de agente electrónico que en el SAN contenga el dominio de la entidad, la llave privada de este debe estar instalada en el servidor web que aloja el servicio web seguro.
    - ✓ El servidor web debe tener configurado la utilización de SSL.
    - ✓ Al menos una suite de cifrado del servidor web, debe coincidir con la lista de suites de cifrado configuradas en el servidor web del BCCR.
    - ✓ El servidor web debe soportar los algoritmos SHA256 y SHA512.

14. ¿Qué es HTTPS?
    HTTPS es la versión segura de HTTP que conocemos comúnmente, el cual cifra las solicitudes que se realizan al servicio, utilizando un certificado SSL, esto con el fin de establecer un canal seguro entre el cliente y el servidor.

15. ¿Cómo puedo verificar si TLS 1.2 se encuentra habilitado?

En los servidores que utilizan el sistema operativo Windows, se puede verificar la habilitación de TLS 1.2 desde Internet Explorer, ingresando a Opciones de Internet, en el tab Avanzadas



16. ¿Cuáles son las suites de cifrado soportadas por el BCCR?

Esta es la lista de suites de cifrado que se soportan para TLS 1.2, se encuentran en orden de prioridad. La entidad debe soportar al menos uno.

```
  Supported Server Cipher(s):
Preferred TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-384 DHE 384
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  256 bits  AES256-SHA
```

17. ¿Cómo puedo verificar las suites de cifrado con las que cuenta el servidor web?

En el mercado existen diversas herramientas que permiten visualizar las suites de cifrado configuradas en un servidor, lanzando una consulta al dominio o dirección donde se encuentre alojado un sitio o servicio seguro, entre estas se puede mencionar SSLScan, TestSSLServer4 y Qualys.

18. ¿Cómo puedo verificar los algoritmos que soporta el servidor web?

Este dato se puede verificar vía Registry, en la entrada "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010003"

```
3.Algoritmos soportados:
RSA/SHA512,ECDSA/SHA512,RSA/SHA256,RSA/SHA384,RSA/SHA1,ECDSA/SHA256,ECDSA/SHA384,ECDSA/SHA1,DSA/SHA1
```

19. ¿Cómo se debe instalar la jerarquía de certificados?

    Existe una guía llamada “Guía para instalar los certificados de la jerarquía del ambiente de pruebas del Firmador”, la cual se le puede solicitar al COS.