Especificaciones Técnicas

Lote 1 - FIRMA ELECTRÓNICA

1. Objeto y descripción de los Servicios requeridos

El presente proyecto tiene como objetivo disponer de una aplicación informática que brinde el servicio de Servidor de Firma Electrónica. Esto es con el objetivo de habilitar a las aplicaciones informáticas que dan soporte a la operativa de la organización la posibilidad de eliminar el papel y, en su lugar, firmar documentos electrónicos con validez equivalente.

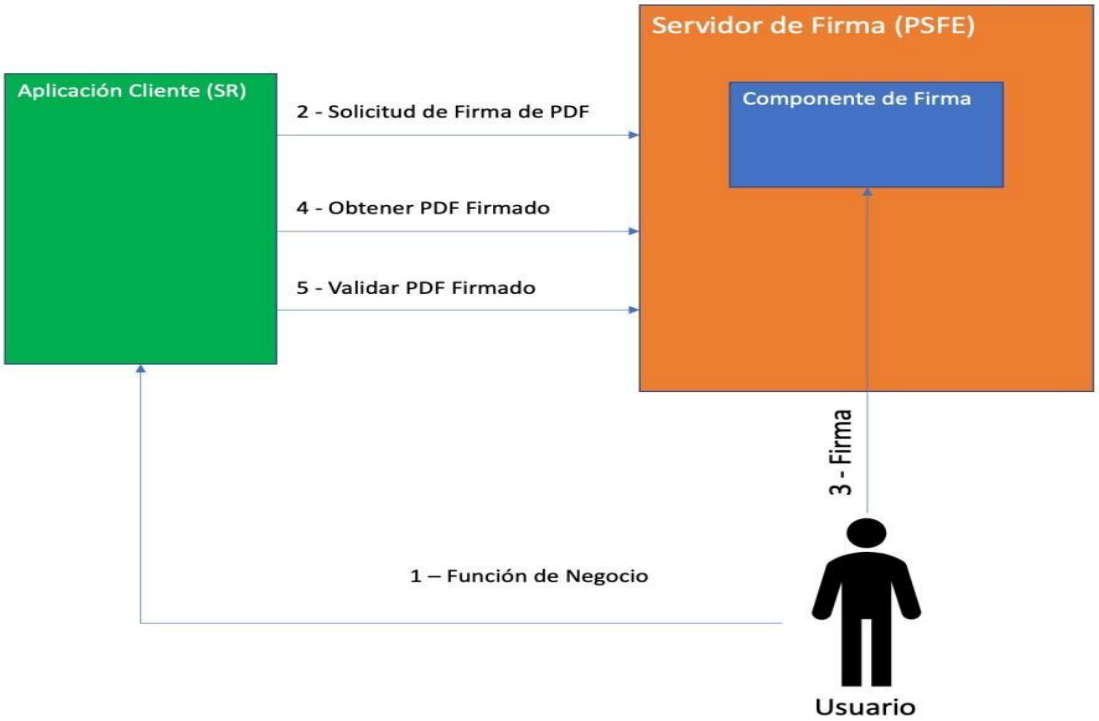
A tal efecto se desea implementar una solución basada en un Servidor de Firma Electrónica el cual permitirá en forma centralizada operar las tareas sobre las distintas aplicaciones que así lo requieran. El Servidor de Firma Electrónica deberá contar con las funcionalidades necesarias para la Institución las cuales se describen más abajo en este documento. Es importante destacar que se deberá prever las funcionalidades necesarias para determinar la autenticidad, integridad y no repudio de un documento firmado.

A continuación, se detalla el alcance del servidor de firma para darle soporte a las necesidades del MOPC.

2. Producto de Servidor de Firma Electrónica

2.1. Arquitectura de la solución deseada

A continuación, se muestra el diagrama de la arquitectura macro que se desea.



El Servidor de Firma Electrónica tiene como objetivo proveer una solución centralizadora de las firmas electrónicas para el MOPC. Este servidor recibirá pedidos de firma y de validación de firma de las distintas aplicaciones y sistemas pre existente o futura del Ministerio, y se encargará de que

los usuarios finales firmen los documentos electrónicamente. Estos documentos electrónicos, son devueltos al sistema originario del pedido para que ellos continúen con el flujo de trabajo habitual. A su vez, el Servidor de Firma Electrónica brindara funcionalidades de validación de firmas contra las entidades certificadoras parametrizadas en él. Los tipos de documentos a ser soportados se indican más abajo.

3. Componentes de Servidor de Firma

El Servidor de Firma Electrónica deberá constar mínimamente con de los siguientes componentes funcionales para su integración con los sistemas actualmente disponibles y futuros en la institución:

3.1.1. Solicitador de Servicio (SR)

Componente de sistema que solicita el servicio de firma electrónica. Permite la integración a los sistemas previamente existentes y los nuevos en el Ministerio. De este modo se podrán modificar los sistemas en sus flujos para la utilización del Servidor de Firma Electrónica. La solución deberá ser compatible con toda la tecnología de modo a que pueda realizar pedidos y redirecciones HTTP, sea o no GeneXus. Debe ser compatible con sistemas cliente (SR) desarrollados en Java, .Net, PHP, entre otros.

3.1.2. Proveedor Servicio Firma Electrónica (PSFE)

Es el proveedor de los servicios de Firma Electrónica. Es el sistema a adaptar e implementar.

3.1.3. Componente de Firma electrónica

Deberá contar con un Componente de firma electrónica a ser utilizada por el Servidor de Firma Electrónica.

3.2. Tecnología Base

El Servidor de Firma Electrónica deberá poder utilizar un servidor de aplicaciones Java (Tomcat 8.5 o superior o Wildfly 14 o superior) y una base de datos, pudiendo ser SQL Server 2012 o superior, Postgres 7.X o superior o MySQL 4.x o superior. El servidor de firma deberá poder ser desplegado en un esquema de Alta Disponibilidad (HA) utilizando un esquema de balanceo de carga con afinidad de sesión (stickyness).

3.3. Funcionalidades de Firma

El Servidor de Firma (PSFE) deberá poseer mínimamente tres ramas de funcionalidades para realizar firmas electrónicas y validarlas:

Firma por parte del usuario final

Firma por parte de un sistema cliente (SR)

Validación de firmas para un sistema cliente (SR)

A continuación, se detallan cada una de ellas:

3.3.1. Firma por parte del usuario final

El SR le comunica al PSFE un documento PDF para firmar. El PSFE despliega el documento y permite realizar la firma por parte del cliente. El PSFE valida la firma y redirige al usuario con el SR.

3.3.2. Firma por parte de un sistema cliente (SR)

El SR envía un documento y el identificador del certificado a utilizar. Con estos datos, el PSFE firma el documento y lo retorna firmado. El PSFE retorna un error si el certificado a utilizar no se encuentra habilitado para el SR (Control de Acceso).

3.3.3. Validación de Firma

El SR envía un documento a través de un servicio (Web Service) al PSFE. El PSFE valida la firma con la(s) cadena(s) de confianza especificadas para el SR.

3.3.4. Firma masiva de documentos

Siendo que los pasos para la firma de un documento son varios tales como: Introducción de PIN del token usb, seleccionar posición de Firma, etc., lo cual hace el proceso más extenso y repetitivo en el caso de la firma de varios documentos del mismo formato/tipo. En consecuencia se deberá poder firmar todos los documentos de una sola vez.

3.3.5. Posición de la Firma

Siempre es requerido que se elija la posición de la Firma en el documento PDF, y no existe forma de establecer una posición predeterminada que también ayudaría a la firma de varios documentos del mismo formato/tipo.

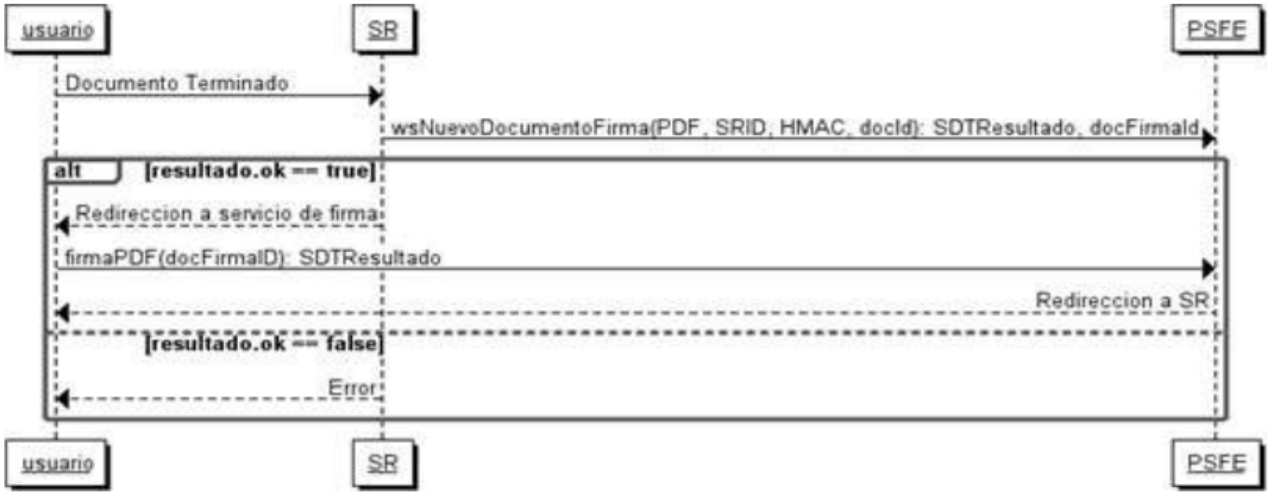
3.3.6. Múltiples firmas en el mismo documento

Se deberá poder firmar varias veces el MISMO documento y esto sin invalidar las firmas anteriores. Es decir al documento se le deberá poder adicionar más de 3 firmas de modo tal que las 3 sean válidas y sin superposición de ninguna de ellas.

3.4. Flujos de firma

De preferencia el que el Flujo de firma debería seguir los siguientes procesos y características:

3.4.1. Proceso de Firma por parte de un usuario final



1. Cuando el SR requiere que el usuario firme un documento, se lo notificará al PSFE a través de un web service.

2. Esta acción se realiza a través de la operación wsNuevoDocumentoFirma, la cual es un ws que espera cuatro parámetros:

   i. **PDF:** Un string en representación del PDF en base64.
   ii. **SRID:** El ID del SR, este valor será un GUID.
   iii. **HMAC:** Para obtener el HMAC se debe cifrar el hash obtenido de hacer un SHA256 del SRID y el PDF en base64 (en ese orden). Para cifrar el hash usar AES128CBC. La clave de encriptación y el índice de vector proporcionados (ambos forman el SRSecret) estarán cifrados en base64.
   iv. **docId:** Id del documento para el SR.

3. El PSFE intentará validar estos parámetros y se le devolverá al SR un SDTResultado. Este SDT contiene tres atributos, uno booleano con el cual se sabrá si la operación fue realizada con éxito y un string en el cual se especificará el error en caso contrario. El atributo restante corresponde al id del documento. También devuelve un GUID llamado docFirmaId, que representa un ID para esta solicitud de firma de documento.
4. Si el servidor pudo validar los parámetros recibidos como correctos, entonces el SR re-direccionará al usuario al servicio de firma, donde se le mostrará el PDF. De lo contrario le mostrará el error correspondiente.
5. Una vez que el usuario esté en el servidor de firma, podrá efectivamente firmar el documento. Cuando el usuario haga click en el botón firmar, el PSFE intentará firmar el documento y volcará la información en un SDTResultado.
6. Luego de mostrado el mensaje de error o de éxito, el usuario será redireccionado nuevamente al SR.
7. Finalmente, con wsObtenerDocFirmado, el SR podrá acceder al documento firmado en Base64. Este ws recibe los siguientes parámetros:

   i. **SRID:** GUID que representa el ID del SR.
   ii. **HMAC:** El método para obtener este valor es igual al utilizado para obtener el HMAC enviado en web service anterior. Para generar el hash usar el SRID y el docFirmaId, en ese orden. Luego cifrar este valor con AES128CBC, usar la misma clave e índice de vector.
   iii. **docFirmaId:** ID utilizado para identificar el pedido de firma. Este docFirmaId es el mismo que devuelve el ws anterior
8. El PSFE intentará validar estos parámetros. De ser los valores correctos, el SDTResultado tendrá el atributo booleano en true y PDF tendrá el valor del documento firmado, en base64. De lo contrario PDF irá vacío, SDTResultado tendrá el booleano en false y el string de error con la descripción del mismo.

3.4.2. Firma de SR (Server Side)

A través de un web service, el servidor de firma (PSFE) deberá poder realizar la firma de un documento PDF en nombre del SR, retornando el documento firmado.

3.4.3. Validación de documentos

Dado un documento PDF firmado y una fecha y hora (opcionales), el servicio deberá retorna si las firmas del documento son válidas para ese momento de tiempo dado. Este servicio se invocará a través de un web service por el SR.

3.5. Funcionalidades de Backend

Sera un URL diferente al servicio de firma, se brindará un backend de configuración que cuenta con autenticación y autorización de acceso. En este backend, se parametrizarán los Service Requesters (Sistemas usuarios del servicio de firma) y otras configuraciones requeridos para el funcionamiento del servicio.

El proceso para integrar un SR al PSFE implicara dar de alta dicho SR a los sistemas aceptados para la firma. En el SR se deberá almacenar su Identificador por el cual lo conocerá el PSFE, así como el Secreto para que luego pueda hacer uso del servicio. Además, cada SR deberá tener asociado la o las CAs en la/s que confíe.

3.5.1. Certificate Authority (CA)

Compuesto por un id (entero autogenerado), nombre, path al certificado, path al archivo con revocados y/o web service correspondiente (OCSP si corresponde). Al momento de firmar el documento, el servidor intentará validar la firma contra la(s) autoridad(es) certificadora(s). Solo se intentará verificar contra las autoridades que tenga asociado el service requester desde el que se está haciendo la solicitud de firma.

3.5.2. Certificados de Firma (Server Side)

El PSFE contará con un backend que permite configurar los certificados electrónicos gestionados por el PSFE, la cadena de confianza y los SR que soportará, así como cada una de sus configuraciones.

3.5.3. Service Requester (SR)

Esta transacción representara los sistemas que quieran firmar en algún momento algún documento, y está compuesta por un id (GUID), nombre, URL y un Secreto.
La URL es a donde se deberá redirigir al usuario luego de firmado el documento (lo mejor es que sea a una pantalla que haga el llamado al WebService para obtener el documento firmado).
El secreto será la key usada para encriptar algunos que se envían a través de los WebServices.
Además, esta transacción tendrá un subnivel, que serán las autoridades certificadoras en las que confía ese service requester.

3.5.4. Control de acceso del Backend

Corresponderá a las funcionalidades de control de acceso al backend. Incluirá gestión de usuarios, roles, contraseñas de los usuarios y su recuperación.

4. Entregables

Como parte de los entregables a realizar se plantean los siguientes:

- Artefactos generados del PSFE (WAR, Scripts de base de datos)
- Manuales de instalación, configuración e integración para los PSFE en formato editable
- Entorno de Prueba (Cliente de Test)

- La solución se instalara en un ambiente de TEST

5. Plan de Trabajo

A continuación, se presenta el plan de trabajo propuesto en términos de la identificación de actividades necesarias para alcanzar los objetivos planteados, el dimensionamiento del esfuerzo previsto y los supuestos que lo sustentan.

5.1. Setup del ambiente de Test

Apoyo para la configuración del servidor de aplicaciones y de base de datos para poder instalar el servidor de firmas, (mínimo 50 hs.). Se brinda la instalación sin alta disponibilidad.

Se contará con el siguiente entorno:

- Acceso al servidor de test vía VPN o similar.
- El Sistema Operativo sera Windows, RedHat Linux, Centos o Ubuntu.
- Un servidor de aplicaciones accesible en el ambiente (Tomcat o WildFly). Es posible realizar la entrega del servidor de firma en una imagen de Docker.
- Existirá una base de datos previamente creada y accesible de uno de los DBMS soportados e indicados más arriba.

5.2. Instalación Servidor de Firmas

Se instalará la aplicación de servidor de firmas y se parametriza, como ser la CA a utilizar, la lista de revocación y otros parámetros de ambiente.

Capacitación

Se realizará la configuración del cliente de prueba, con el servidor de firma de prueba instalado, de preferencia en modalidad training on the job, capacitando al personal en forma práctica (mínimo 8 hs.).

5.3. Soporte para la implementación inicial

Se dará Soporte a la implementación inicial (mínimo 50 hs.) para facilitar la adopción y la introducción en su contexto real.

6. Licencias y Servicios de instalación, capacitación e implementación

- Licencia del producto (por servidor instalado en producción)
- Mínimo de 25 hs. para instalación pudiendo ser local o remota.
- Mínimo de 8 hs. de capacitación pudiendo ser local o remota.
- Mínimo de 50 hs. de soporte para la implementación inicial pudiendo ser local o remota.

7. Debe incluirse Soporte y Mantenimiento el primer año

Con la contratación del Soporte y Mantenimiento anual se deberá tener acceso a:

- Mantenimiento del Componente de Firma Electrónica incluido en la licencia del Servidor de Firma:
  - Soporte en los generadores Java y .NET de GeneXus. o Soporte en el servidor y en el navegador del usuario para firma de PDFs.

- Soporte mediante extensión para las nuevas versiones de los navegadores modernos Chrome (>55) y Firefox (>52).
- Soporte mediante applet para IE.
- Soporte mediante JNLP para Microsoft Edge y Safari.
- Soporte para firma simple o de múltiples documentos a la vez en los navegadores soportados.
- Soporte para las nuevas versiones de los sistemas operativos Windows, MacOS y Ubuntu
- Nuevas versiones del componente que se liberen (con los bug fixes y pudiendo contener nuevas funcionalidades).
- Soporte de "Previous version compatible" Web User Experience.

LOTE 2 – Renovación del Servicio AVYCE y Herramientas de Desarrollo GENEXUS y Adquisición de Licencia Genexus Smart Device

Ítem 1	**GX-retoma AVYCE** **Retoma del Servicio Anual AVYCE**
Descripción	
Actualización de Versiones y Corrección de Errores para: • 15 Licencias GeneXus IDE (Integrated Development Environment) • 3 Generadores Cliente-Servidor GeneXus • 5 Generadores JAVA GeneXus • 3 Genexis.NET Generador • 2 Licencia Generador GeneXus Smart Device • 30 Inbox GXFlow • 1 Licencia GXFlow Developer Pack • 15 Licencias GXQuery • 1 Licencia Generador GeneXus RPG	
Instalación, Capacitación y Soporte para la utilización de las nuevas versiones. -	

LOTE 3 - Suscripción de Redhat (actualización)

Ítem	Descripción	Cantidad
1	Red Hat Enterprise Linux Server Suscripción Standard (Physical or Virtual Nodes) Para servidores de hasta 2 sockets (3 años)	4
2	Red Hat Enterprise Linux for Virtual Datacenters Suscripción Standard (Ilimitados Virtual Guests) Para servidores de hasta 2 sockets (3 años)	1
Los Servicios deberán incluir: Instalación, configuración y puesta en marcha. Antes de iniciar cualquier servicio, se debe realizar una reunión con los encargados designados por el MOPC a fin de obtener las directivas y los detalles de las implementaciones a llevar a cabo. Todos los servicios funcionando. Tiempo mínimo de acompañamiento de 30 horas por parte de un Técnico con la Certificación RHCE de la empresa oferente. Instaladores: En medio físico (DVD/CD), o link oficial del portal de la marca que permita ser bajado.		
Carta de Autorización del fabricante o Distribuidor. En caso de presentar autorización del representante o distribuidor, se deberá presentar igualmente la cadena de autorizaciones hasta el fabricante del bien. Las autorizaciones deberán estar actualizadas, máximo dentro de los 12 meses anteriores a la fecha de apertura del llamado.		
Presentación de las Especificaciones Técnicas Ofertadas, en forma impresa, firmada y sellada, conforme a lo establecido en la Sección III Especificaciones Técnicas.		

ANEXO I