Objeto: Adquirir los servicios de confianza digital para la generación de firmas digitales mediante la provisión e integración de una interfaz de programación de aplicaciones (API) para la Superintendencia Financiera de Colombia, incluido soporte técnico.

1. Relación de servicios

Los servicios objeto de la presente contratación son los siguientes:

Detalle	Unidad	Cantidad
API para firma digital con Vigencia de 18 meses	Licencia	1
Transacción de firma digital, PAdES incluye la funcionalidad con LTV (Long- Term Validation)	Transacción	122.759
Transacción de estampa cronológica	Transacción	122.759
Transacción de firma digital HASH	Transacción	2.700
Ambiente de pruebas	Ambiente	1

2. API consumo del servicio web para firma digital centralizada.

- La Entidad requiere un componente de API REST que permita integrar el certificado digital centralizado con el gestor documental de la entidad.
- La API instalada deberá ser compatible con los certificados digitales emitidos actualmente y los adquiridos.
- El servicio deberá estar disponible para su uso de manera continua, las veinticuatro (24) horas del día, los siete (7) días de la semana (7x24), garantizando un nivel de disponibilidad mínimo del **99.8%** durante toda la vigencia del API.
- La cantidad de transacciones contratadas deberá estar asociada al volumen de utilización proyectado para los servicios de firma digital, firma con validación a largo plazo (LTV), estampado cronológico y firma mediante HASH, garantizando la disponibilidad necesaria para atender la demanda de la Entidad durante la vigencia contractual.
- La autenticación del API debe contemplar:
    - Clave encriptada
    - Token Bearer
    - Autenticación mutua SSL/TLS

- Adicionalmente, la Superintendencia Financiera de Colombia requiere disponer de ambientes de pruebas durante toda la vigencia de 18 meses para los servicios de firma digital suministrados por el proveedor, teniendo en cuenta que el gestor documental de la entidad, Solución Integral de Procesos (SOLIP) se encuentra en un proceso permanente de evolución funcional, mantenimiento correctivo, adaptativo y perfectivo, así como de adecuación a cambios normativos y regulatorios. Como plataforma transversal que soporta múltiples procedimientos y flujos documentales institucionales, SOLIP demanda la ejecución recurrente de actividades de desarrollo, ajustes, estabilización y optimización que deben ser previamente validadas en ambientes de pruebas antes de su despliegue a producción.
- El contratista deberá contar con la autorización vigente como Entidad de Certificación Abierta, expedida por la ONAC. Dicho documento deberá presentarse junto con la oferta y mantenerse vigente durante toda la ejecución del contrato.
- Dentro del plazo de ejecución, el contratista deberá realizar la habilitación, entrega y activación de los servicios contratados.

2.1 Autenticación

Operación POST para realizar la autenticación y obtener un token para el consumo de las operaciones de firma.

2.1.1 Parámetros

Objeto JSON que debe cumplir con los siguientes atributos:

Nombre	Tipo	Tamaño	Obligatorio	Descripción
Usuario	Cadena	30	Si	Usuario para autenticación
Clave	Cadena	30	Si	Clave del usuario

2.1.2 Respuesta

Como respuesta de la operación de autenticación se obtiene un JSON con la siguiente estructura:

Nombre	Tipo	Tamaño	Obligatorio	Descripción
token	Alfanumérico	Max	No	Token para autenticación
expiracion	Fecha hora	20	No	Fecha hora en la que expira el token

httpStatus	Numérico	3	Si	Código http del estado de la transacción
codigoRespuesta	Alfanum érico	5	Si	Código del resultado de la transacción
descripcionRespuesta	Alfanumérico	Max	Si	Descripción del código de la transacción
detalleRespuesta	Listado alfanum érico	Max	No	Especificación de inconsistencias en los parámetros

2.1.3 Valores para el atributo de código Respuesta

Código	Descripción
200	Transacción completada con éxito
400	Error al digitar información
401	Credenciales invalidas
409	Error en conexión externa
500	Error inesperado
503	Mantenimiento

2.2 Firma digital

Operación POST que permite realizar la firma digital de un documento pdf con el envío de un objeto JSON. Como resultado del firmado se obtendrá un objeto en formato JSON con la respuesta de la transacción. El método de acceso se realiza mediante Bearer Authentication el cual es un esquema de autenticación http que involucra tokens de seguridad (Bearer Token), generado por el servicio de autenticación.

2.2.1 Parámetros de entrada

- Objeto JSON que debe cumplir con los siguientes atributos

Nombre	Tipo	Tamaño	Obligatorio	Descripción
numeroDocumento	Alfanumérico	20	Si	Identificador del certificado digital
clave	Alfanumérico	20	Si	Clave del certificado
usuarioTSA	Alfanumérico	20	No	Usuario de la TSA, es obligatorio cuando se

				desea agregar marca de tiempo en la firma
claveTSA	Alfanumérico	20	No	Clave de la TSA, es obligatorio cuando se desea agregar marca de tiempo en la firma
Ubicación	Alfanumérico	30	No	Campo ubicación del detalle de la firma
Razón	Alfanumérico	30	No	Campo razón del detalle de la firma
conLTV	Boolean	-	Si	Indica si se desea la firmar como **LTV**
conEstampa	Boolean	-	Si	Indica se coloca una marca de tiempo en el documento
firmaVisible	Boolean	-	Si	Indica si se desea colocar la firma visible en el documento PDF
imagenFirma	imagenFirma	Max	No	Especifica las propiedades de la firma visible
Base64	Alfanumérico	5 MB	Si	Documento PDF para firmar codificado en base64

- Objeto de entrada ImagenFirma

Nombre	**Tipo**	**Tamaño**	**Obligatorio**	**Descripción**
x	float		Si	Posicionamiento en el eje Y de la imagen.
y	float		Si	Posicionamiento en el eje Y de la imagen.
ancho	float		Si	Ancho de la imagen
alto	float		Si	Alto de la imagen

Campofirma	Bolean	-	-	Documentos con campos de firma predefinidos
imagen	Alfanumérico	MAX		Imagen codificada en base64
predefinida	Bolean	-	-	Firma manuscrita en forma de grafico predefinido
pagina	int			Página en la que se va a posicionar la imagen de la firma

2.2.3 Respuesta

Como respuesta de la operación firma digital se va a devolver un JSON con la siguiente estructura:

Nombre	Tipo	Tamaño	Obligatorio	Descripción
mensaje	Alfanumérico	Max	Si	Descripción de la respuesta
documentoFirmado	Alfanumérico	Max	Si	Documento firmado y codificado en base64
validarFirma	Alfanumérico	Max	No	Para firma electrónica únicamente
httpStatus	Numérico	3	Si	Código http del estado de la transacción
codigoRespuesta	Alfanumérico	5	Si	código de respuesta obtenido del proceso de firma

2.3 Estampar documento (estampado cronológico)

Operación POST que permite realizar la estampa de un documento pdf con el envío de un objeto JSON. Como resultado del estampado se obtendrá un objeto en formato JSON con la respuesta de la transacción.

El método de acceso se realiza mediante Bearer Authentication el cual es un esquema de autenticación http que involucra tokens de seguridad Bearer Token), generado por el servicio de autenticación.

2.3.1 Parámetros de entrada

Objeto JSON que debe cumplir con los siguientes atributos

Nombre	Tipo	Tamaño	Obligatorio	Descripción
Usuario	Alfanumérico	50	Si	Usuario de la TSA.
clave	Alfanumérico	100	Si	Clave de la TSA.
base64	Alfanumérico	5 MB	Si	Documento pdf en formato base64.

2.3.2 Respuesta

Como respuesta de la operación de autenticación se obtiene un JSON con la siguiente estructura:

Nombre	Tipo	Tamaño	Obligatorio	Descripción
mensaje	Alfanumérico	50	Si	Descripción de la respuesta.
base64	Alfanumérico	100	Si	Documento estampado y codificado en base64.
codigoRespuesta	Alfanumérico	5	Si	Código de respuesta obtenido del proceso de firma
httpStatus	Numérico	3	Si	Código http del estado de la transacción.

2.3.3 Valores para el atributo de código Respuesta

Código	Descripción
200	Transacción completada con éxito
400	Error al digitar información

401	Credenciales invalidas
409	Error en conexión externa
500	Error inesperado
503	Mantenimiento

2.4 Firma hash

La firma hash es un mecanismo de firma electrónica que permite garantizar la integridad y autenticidad de un documento en formatos admisibles por la solución, sin necesidad de transmitir el archivo completo, ya que opera sobre el resumen criptográfico (hash) generado a partir de su contenido. Este servicio se expone mediante una API REST, lo que permite a las aplicaciones cliente integrarlo de forma ágil dentro de sus flujos transaccionales, enviando el hash del documento y recibiendo la firma digital correspondiente en tiempo real. Esta modalidad optimiza el rendimiento y reduce la carga de red frente a la firma de documentos completos, siendo especialmente eficiente en escenarios de alto volumen transaccional. Este mecanismo debe realizarse una vez finalizada la actuación y efectuado el cierre del expediente electrónico, sobre la versión definitiva del índice electrónico en formato XML

3. AMBIENTE DE PRUEBAS API'S DE INTEGRACIÓN

Ambiente de pruebas independiente del ambiente de producción que permita realizar actividades de validación, desarrollo, parametrización, pruebas funcionales, pruebas de regresión, homologación y puesta en operación de nuevas funcionalidades, sin afectar la continuidad de los servicios institucionales ni comprometer la integridad de la información administrada en producción, durante la vigencia del servicio firma digital mediante API REST.

Durante la vigencia de la solución, el contratista, dispone de un ambiente de pruebas con certificados digitales centralizados, destinados a soportar las operaciones de firmado de documentos en ambientes no productivos.

Los certificados de prueba deberán permitir la validación integral de todos los servicios contratados, incluyendo firma digital, firma con validación a largo plazo (LTV), estampado cronológico y firma mediante HASH, con el fin de verificar su correcta integración, interoperabilidad y funcionamiento dentro de las aplicaciones institucionales.

4. SOPORTE TÉCNICO

Prestar soporte técnico telefónico y/o vía Web, cuando el supervisor de contrato lo solicite, durante la vigencia del servicio de API, de lunes a viernes en el horario de 8:00 a.m. a 5:00 p.m., sin costo adicional para la Superintendencia Financiera.

a. La ejecución de los servicios de soporte se realizará en horario de lunes a viernes de 8:00 am a 5:00 pm, salvo las ventanas de mantenimiento que se lleguen a programar con la debida anticipación y que para garantizar la continuidad en SUPERINTENDENCIA FINANCIERA DE COLOMBIA FIN CONDICIONES TÉCNICAS MÍNIMAS. y con el fin de garantizar la continuidad y disponibilidad de los servicios tecnológicos, especialmente los relacionados con la operación de la API, dichas actividades deben realizarse en horario nocturno, fines de semana o días festivos.

b. El contratista deberá brindar atención a los incidentes reportados por el supervisor del contrato de acuerdo con la prioridad de los incidentes indicada a continuación y resolver en los tiempos descritos aquí, so pena de incurrir en incumplimiento.

   Prioridad 1: Perdida total del servicio

   Efectividad de resolución <= 16 horas hábiles

   Prioridad 2: Perdida parcial del servicio

   Efectividad de resolución <= 20 horas hábiles

c. El contratista deberá entregar al supervisor del contrato, documentación técnica para la integración de las APIs con el gestor documental SOLIP. Además, debe prestar soporte para la integración o por fallas derivadas de cambios de la plataforma del contratista.

d. El contratista deberá presentar al supervisor del contrato, con periodicidad mensual, un informe detallado del consumo de las transacciones utilizadas por la Entidad, discriminado por cada uno de los servicios contratados, incluyendo firma digital, firma con validación a largo plazo (LTV), estampado cronológico y firma mediante HASH. El informe deberá indicar el número de transacciones consumidas durante el periodo reportado, el saldo disponible y el porcentaje de ejecución frente a la cantidad total contratada.

e. El contratista deberá enviar una notificación oficial al supervisor del contrato donde indique que realizará actualizaciones, ventanas de mantenimientos o cambios que puedan generar indisponibilidad total o parcial del servicio, lo cual deberá contener:
   - Horas/días
   - Fecha y hora de inicio de la actividad.
   - Duración estimada de la intervención.
   - Posibles afectaciones o niveles de indisponibilidad previstos.
   - Plan de contingencia propuesto, en caso de aplicar.
   - Detalle técnico de la actualización
     Indicar claramente el tipo de cambio o actualización, su propósito y los componentes afectados.
   - Responsable asignado
     Incluir el nombre, cargo y datos de contacto de la persona encargada de atender cualquier incidente o inquietud durante el proceso.
   - Confirmación de restablecimiento
     Una vez finalizada la actividad, enviar un mensaje oficial confirmando el restablecimiento total del servicio y el resultado de las validaciones realizadas.
   - Registro de incidentes
   - Ventana de pruebas
     En caso de que se presenten fallas no previstas durante la actividad, se solicita reportarlas de inmediato y activar el protocolo de atención establecido.

- **Niveles de criticidad**

Nivel de Criticidad	Descripción
1	Categoría A (Critica) - Caída total no permite la Operación, afectando a todos los servicios, máxima prioridad
2	Categoría B (Alta) – Indisponibilidad parcial de la operación para uno o más servicios
3	Categoría C (Media) – Eventos que no detienen la operación que afectan a un servicio
4	Categoría D (Baja) – Dudas de la operación de la herramienta y/o dudas sobre nuevas funcionalidades, eventos leves, preguntas básicas de funcionamiento y parametrización.

- **Niveles de soporte**

ANS	Definido por categorías: • Critico: 4 a 6 Hrs hábiles • Alto: 6 a 8 Hrs hábiles • Medio:8 a 10 Hrs hábiles • Bajo: 10 a 16 Hrs hábiles
Tiempos de Solución	Definido por categorías: • Critico: 16 Hrs hábiles • Alto: 20 Hrs hábiles • Medio: 24 Hrs hábiles • Bajo: 26 Hrs hábiles
Reportes recibidos al finalizar el horario de atención, serán gestionados en el siguiente día hábil y de conformidad con el orden de llegada de los mensajes y prioridad del caso.	

Glosario:

- JSON Es un formato de texto sencillo para el intercambio de datos. Se trata de un subconjunto de la notación literal de objetos de JavaScript, aunque, debido a su amplia adopción como alternativa a XML.
- Bearer Authentication: Esquema de autenticación http que involucra tokens de seguridad Bearer Token), puede entenderse como dar acceso al portador.
- Firma PAdES (por sus siglas en inglés, *PDF Advanced Electronic Signatures*) es un estándar técnico para aplicar firmas electrónicas avanzadas directamente dentro de documentos en formato PDF.
- LTV (Long-Term Validation o Validación a Largo Plazo) en una firma digital permite verificar la validez de un documento firmado incluso muchos años después de que el certificado original haya caducado o sido revocado

En constancia de lo anterior firma,

ROSELIS SILVA CUADRADO Firmado digitalmente por ROSELIS SILVA CUADRADO Fecha: 2026.09.08 18:26:57 -05'00'	EDGAR YESID GARAY MEDINA Firmado digitalmente por EDGAR YESID GARAY MEDINA Fecha: 2026.09.08 21:09:22 -05'00'
Roselis Silva Cuadrado Profesional Grupo de Ciberseguridad Institucional y Continuidad Tecnológica	**Edgar Yesid Garay Medina** Coordinador del Grupo de Ciberseguridad Institucional y Continuidad Tecnológica