



SERVICIO DE
CONTRATACIÓN ONLINE,
FIRMA ELECTRÓNICA,
SELLO DE TIEMPO Y
VERIFICACIÓN DE IDENTIDAD

HTTPS/API

INDICE

Contenido

INDICE	2
API HTTPs SERVICIOS FIRMA	3
1.-- INTRODUCCIÓN.....	3
2.-- COMPATIBILIDAD Y VERSIONES	3
3.-- SERVIDORES PARA PETICIONES	3
4.-- DATOS IMPORTANTES A TENER EN CUENTA.....	4
5.-- FUNCIONES	5
5.1.- ENVÍO DE CONTRATOS PARA FIRMA	5
5.2.- OBTENCIÓN/DESCARGA DE CONTRATO CERTIFICADO	12
5.3.- VERIFICAR IDENTIDAD.....	13
5.4.- SERVICIO DE SELLADO DE TIEMPO DE LA CASA DE LA MONEDA.....	17
5.5.- SELLADO DE TIEMPO DE PDFs DESDE APLICACIONES	18

API HTTPs SERVICIOS FIRMA

1.--- INTRODUCCIÓN

API de integración de servicios de contratación, firma, sello y verificación de identidad.

2.--- COMPATIBILIDAD Y VERSIONES

La versión 2 es compatible con versiones anteriores de la API

Versión 1.0 – 1.7: Última actualización 2017. Se recomienda la actualización a versión 2.0 o superior. Versiones no soportadas actualmente. Contactar con soporte para ayuda a la migración.

Versión 2.0 – 2.3: última actualización: 2019. Se añaden parámetros a las peticiones para utilizar más posibilidades de firma, sello de tiempo y contratación. Se añade el servicio de verificación/certificación de identidad online mediante vídeo.

3.--- SERVIDORES PARA PETICIONES

Las peticiones se pueden realizar por HTTPs (conexión segura) y los parámetros pueden ser enviados en peticiones POST (por cuestiones de seguridad no se admiten peticiones GET, ni peticiones no seguras en las funciones sensibles).

Datos peticiones HTTPs (seguras):

Servidor Funciones: <https://www.lofirmo.com/api/> (para puerto 443 -SSL por defecto-)

Servidor Sello de tiempo: <https://www.lofirmo.com/tsa/> (para puerto 443 -SSL por defecto-)

4.--- DATOS IMPORTANTES A TENER EN CUENTA

Conexiones en vacío:

Es importante tener en cuenta que una conexión errónea de forma repetida será tratada por el sistema como spam y podrá llegar a bloquear temporalmente la conexión.

Es conveniente evitar realizar repetidas conexiones con datos erróneos o conexiones rápidas 'en vacío' (sin realizar envíos) con los mismos datos para obtener, por ejemplo, el número de créditos. O peticiones continuas sin crédito en la cuenta.

Para obtener reports de forma óptima en tiempo real (por ejemplo para recibir el estado de firma de un contrato enviado) se recomienda activar desde su panel de usuario la recepción de reports en su web o solicitar un correo automático cuando se finalice el proceso.

Respuesta de las peticiones:

La mayoría de las funciones disponen de un parámetro denominado 'Resp'. Este parámetro define el formato de la respuesta que se devolverá. Puede ser TXT, JSON, XML o no definido.

Se recomienda siempre definir este parámetro ya que todas las funciones, por compatibilidad con versiones anteriores de la API, responden por defecto (si no se define este parámetro) tal y como lo hacían en versiones antiguas. En estos resultados de versiones de API anteriores se obvian algunas de las variables que se incluyen en esta versión de la API y que consideramos importantes para facilitar la integración e información de la cuenta.

En los ejemplos incluidos siempre se tiene en cuenta que ha definido el parámetro. Si está trabajando directamente con la API versión ≥ 2 , asumiremos que ha definido el parámetro en todas las peticiones.

5.--- FUNCIONES

5.1.- ENVÍO DE CONTRATOS PARA FIRMA

Objetivo:

Envío de contratos y configuración del mismo para su firma por uno o varios firmantes.

Petición a:

<https://www.lofirmo.com/api/v2/enviarcontrato>

Parámetros POST:

- **Correo:** (Obligatorio). String con el correo del usuario que envía (en LOFIRMO.COM / MENSATEK / SMSCERTIFICADO.ES).
- **Passwd:** (Obligatorio). String con la contraseña del usuario que envía (El de acceso al panel de usuario).
- **Firmantes:** (Obligatorio). Array JSON con los datos de los firmantes. El array debe contener los siguientes datos por firmante:
 - **Nombre:** (obligatorio) Nombre y apellidos del firmante
 - **NIF:** (obligatorio) NIF/DNI del firmante
 - **Email:** (opcional email o teléfono) Email del firmante.
 - **Telefono:** (opcional email o teléfono) Teléfono móvil del firmante.
 - **Orden:** (opcional) Orden de firma para varios firmantes

Ejemplo para 2 firmantes:

```
[
  {
    "Nombre": "Pedro Pérez Gómez",
    "NIF": "00000000T",
    "Email": "firmante1@dominio1.com",
    "Telefono": "600000001",
    "Orden": 1
  },
  {
    "Nombre": "Ana Fernández Hernández",
    "NIF": "00000001T",
    "Email": "firmante2@dominio2.com",
    "Telefono": "600000002",
    "Orden": 2
  }
]
```

- **Documentos:** (Obligatorio). Array JSON con la configuración de los documentos y tipo de los mismos, es necesario en función del tipo, cumplimentar:
 1. **TIPO PLANTILLA:** Son plantillas creadas dentro del panel de usuario, debe especificarse:
 - a. **Plantilla:** Número de la plantilla (el id/número se encuentra en el listado de plantillas dentro del panel de usuario).
 - b. **Tipo:** PLANTILLA
 - c. **Nombre:** Nombre del documento que verá el firmante.
 - d. **Aceptacion:** (0 ó 1) Especifica si el firmante debe 'ver' hasta el final del documento antes de firmar. Si es 1 el sistema pedirá al firmante que haga 'scroll' hasta el final del documento previamente a la firma.
 2. **TIPO PDF:** Ficheros PDF, los parámetros a enviar son:
 - a. **Tipo:** PDF
 - b. **Contenido:** contenido del fichero codificado en base64
 - c. **Nombre:** Nombre del documento que verá el firmante.
 - d. **Aceptacion:** (0 ó 1) Especifica si el firmante debe 'ver' hasta el final del documento antes de firmar. Si es 1 el sistema pedirá al firmante que haga 'scroll' hasta el final del documento previamente a la firma.
 3. **TIPO CHECKBOX:** Son preguntas que se realizan al firmante antes de la firma, por ejemplo para cumplimentar el reglamento GDPR, consultar sobre envío de ofertas, etc... Se deben enviar los siguientes parámetros:
 - a. **Tipo:** CHECKBOX
 - b. **Texto:** Pregunta o texto que se le mostrará al firmante

- c. **Inicial:** (0 ó 1): Estado inicial del checkbox/casilla de verificación. 0: desactivada o 1: activada
- d. **Final:** (0 , 1 ó 2): Estado final que debe tener la casilla. 0: debe estar desactivada, 1: debe quedar activada ó 2 para elección libre.

Ejemplo:

```
[
{
  "Tipo": "PDF",
  "Contenido": "JVBER...",
  "Nombre": "Nombre mostrado del PDF",
  "Aceptacion": "1"
},
{
  "Tipo": "PLANTILLA",
  "Plantilla": "XXXXX-XX",
  "Nombre": "Nombre a mostrar de la Plantilla",
  "Aceptacion": "0"
},
{
  "Tipo": "CHECKBOX",
  "Texto": "¿Permite la utilización de sus datos para su
utilización en el perfeccionamiento del presente contrato?",
  "Inicial": "0",
  "Final": "1"
},
{
  "Tipo": "CHECKBOX",
  "Plantilla": "¿Desea que le enviemos ofertas basadas en
sus preferencias personales?",
  "Inicial": "0",
  "Final": "2"
}
]
```

- **Personalizacion:** JSON con los datos de personalización de la plantilla. Si se añade una o varias plantillas y desea que se rellenen de forma automática, debe indicar aquí los valores de cada variable que quiera rellenar. Las variables que no indique/especifique en este parámetro deberán ser rellenas por el primer firmante.

```
{
  "Nombre de Empresa": "La empresa",
  "CIF": "B800000000",
  "Nombre Apoderado": "Pedro Fernández",
  "Variable ...": "Valor",
}
```

- **TipoFirma:** (Por defecto 3) Es el tipo de firma que deberán utilizar los firmantes. Las opciones son:

- 1: Aceptación explícita
- 2: PIN OTP o PIN de un único uso (debe indicarse el móvil de los firmantes donde recibirán el PIN de firma)
- 3: Firma manuscrita/biométrica: Cada firmante deberá realizar la firma dibujándola con el dedo sobre su propio teléfono móvil.
- 4: Firma certificada: Se utilizará para la firma el certificado o DNI de cada firmante. Atención: Debe asegurarse de que los firmantes disponen de certificado de firma en sus dispositivos o lector de DNI.

- **Mensaje:** Es el mensaje que se le enviará a cada firmante con el link de firma. Se pueden utilizar variables, las variables disponibles son:

- [LINK]: Link de firma
- [NOMBRE]: Nombre del firmante
- [NIF]: Número de DNI del firmante.

El valor por defecto de este parámetro (si no se especifica) es: 'A la Atención de [NOMBRE] con NIF [NIF], según lo acordado, le enviamos el contrato para su firma. Pulse en el siguiente link: [LINK] para comenzar el proceso.'

- **MedioComunicacion:** Es el medio de comunicación que se utilizará en el mensaje de firma.

- 1: Por SMS
- 2: Por Email.
- 3: Por SMS Certificado (los recordatorios no se harán por este medio, sólo el primero de los mensajes)

- **VerificacionIdentidad:** (Por defecto 0) si se establece a 1, el sistema identificará mediante vídeo a cada firmante y certificará la identificación incluyendo validez del DNI, si la persona identificada es real (no es foto) y si la persona identificada es la del DNI. Para ello, el sistema hará un vídeo de la persona a identificar y le solicitará que muestre a la cámara el DNI.

- **EmailReport:** Correo electrónico que recibirá el report. Si no se utiliza y se ha seleccionado Report=1, se enviará al correo registrado como usuario en

MENSATEK.(ATENCIÓN: Debe ser un correo válido).

- **Accesible:** Indica si cada firmante tendrá acceso al documento firmado. Realmente tendrá acceso al certificado final con todos los datos de firma.
- **AlternaMedios:** (por defecto 0) si se establece en 1, le indica al sistema que alterne la comunicación entre SMS y Email en cada recordatorio de firma hasta que los firmantes hayan finalizado el proceso.
- **Recordatorios:** (Por defecto 3) es el número de días entre recordatorios de firma. Si cada firmante no ha finalizado el proceso, lo ha dejado a medias o no ha accedido aún, el sistema le envía cada X días un recordatorio.
- **FechaLimite:** Es la fecha en la que el sistema dejará de enviar recordatorios si no se ha finalizado el proceso y dará el contrato como no firmado.
- **Idioma:** (Por defecto 'es') Es el idioma en el que se muestra el proceso de firma.
- **MinimoCheck:** Si ha incluido CheckBoxes en los documentos es el número mínimo de ellos que debe activar cada firmante (ON) antes de continuar el proceso. La utilidad de Mínimo y Máximo podría ser:
 - 1.- Caso en el que se trata de una votación firmada. Se debería elegir a uno y solo uno de las opciones (por ejemplo) mínimo y máximo se establecerían en 1 para que cada firmante eligiese a un único candidato.
 - 2.- Caso de solicitar preferencias por ejemplo, necesitaríamos supongamos entre 2 y 3 preferencias de cada firmante.
 - Etc...
- **MaximoCheck:** Si ha incluido CheckBoxes en los documentos es el número máximo de ellos que debe activar cada firmante (ON) antes de continuar el proceso.
- **Resp:** (String) Tipo de respuesta a mostrar.

Posibles valores:

- TXT: salida texto. Ejemplo:

```
Res:1;  
ContratoId:XXXXXXXX-XXXX;  
Cred:12345.67;  
Firmantes:2;  
Documentos:3;
```

- JSON: Respuesta en formato json. Ejemplo:

```
{
  "Res":1,
  "ContratoId":XXXXXXXX-XXX,
  "Cred":19808.45,
  "Firmantes":3,
  "Documentos":3
}
```

- XML: Respuesta en formato XML. Ejemplo:

```
<?xml version="1.0"?>
<result>
  <Res>1</Res>
  <ContratoId>123456789</ContratoId>
  <Cred>12345.67</Cred>
  <Firmantes>1</Firmantes>
  <Documentos>1</Documentos>
</result>
```

Respuesta:

DEVUELVE: string de la respuesta de la página:

- **Res:**Número

Significado del Número:

- 1 Correcto.
- 1 Error de autenticación
- 2 No hay firmantes.
- 3 El JSON del parámetro firmantes no es un json válido.
- 4 No hay documentos en el contrato
- 5 El JSON enviado con los documentos no es válido
- 6 El parámetro documentos es mayor de 7Mb
- 7 No ha incluido todos los datos de los firmantes debe incluir Nombre, NIF, Orden y (Email y/o Teléfono)
- 8 No ha indicado todos los datos de los documentos. Recuerde indicar los datos necesarios de cada tipo de documento.
- 9 Debe rellenar sus datos de configuración para certificaciones/contratos

en su panel de usuario TUS DATOS->Configurar Cuenta

-10 a -12 Error en el contrato, los datos no son correctos.

-13 a -16 Problemas en los datos firmantes enviados

-17 a -20 Problemas en los datos de documentos enviados

-21 problema general en los datos enviados.

-22 los datos enviados en la personalización de la plantilla no son un JSON válido.

-23 La plantilla enviada tiene identificador incorrecto

- **ContratoId:** identificador de contrato enviado para identificaciones posteriores en llamadas posteriores a la PI (por ejemplo para descarga del Contrato Certificado)
- **Cred:**Número (Float) de créditos restantes del usuario en MENSATEK.
- **Firmantes:** Número de firmantes del contrato
- **Documentos:** Número de documentos enviados (plantillas, PDFs y checkboxes)

5.2.- *OBTENCIÓN/DESCARGA DE CONTRATO CERTIFICADO*

Objetivo:

Descarga, una vez finalizado el proceso , del documento certificado.

Petición a:

<https://www.lofirmo.com/api/v2/descargacontrato>

Parámetros GET o POST:

- **Correo:** String con el correo del usuario que envía (en MENSATEK).
- **Passwd:** String con la contraseña del usuario que envía (en MENSATEK).
- **ContratoId:** String con el número de identificador de mensaje obtenido en la función enviar.

DEVUELVE: string con el PDF del contrato certificado o

-1 en caso de no existir el contrato

-2 en caso de datos incorrectos enviados

5.3.- VERIFICAR IDENTIDAD

Objetivo:

Solicitud de verificación automática de identidad de una persona a distancia mediante vídeo.

Petición a:

<https://www.lofirmo.com/api/v2/verificaridentidad>

Parámetros GET o POST:

- **Correo:** String con el correo del usuario que envía (en MENSATEK).
- **Passwd:** String con la contraseña del usuario que envía (en MENSATEK).
- **DNI:** (Opcional) número de DNI que debe verificar el destinatario. Si no coincide con la persona identificada. Sirve para verificar que la persona identificada coincide con la que queremos identificar.
- **Mensaje:** String Mensaje a enviar con la petición de identificación. Debe incluir la palabra [LINK] que se sustituirá por el link de inicio del proceso. Por ejemplo: "Pulse en el siguiente LINK para comenzar el proceso que verifica su identidad [LINK]"
- **Remitente:** (Opcional) Remitente del SMS que le llegará con la petición. Normalmente el nombre de la empresa que inicia el proceso (máximo 11 caracteres).
- **Telefono:** String Móvil del destinatario al que se enviará el proceso de identificación por SMS. (Atención, debe ser un móvil inteligente, con cámara y con actualizaciones de seguridad).
- **Fecha:** (Opcional) con formato AAAA-MM-DD HH:mm Fecha en el que enviará la petición. Si no se indica se envía de inmediato.
- **URLReport:** (Opcional) , es la URL a la que se enviará, por método POST peticiones con eventos del servicio (terminación y validación). Debe ser una dirección correcta tipo <https://www.tudominio.com/script>
 - PETICIÓN AL TERMINAR EL PROCESO: Se realiza una petición cuando el usuario termina la validación, se envían como parámetros:

- ID: Identificación original de la petición obtenida como respuesta inicial.
- IDContrato: Si se trata de un Contrato, aquí se indica el identificador del contrato.
- Telefono: Teléfono al que se ha enviado la petición.
- DNI_Nombre: Nombre que aparece en el DNI
- DNI_Apellidos: Apellidos según aparecen en el DNI
- DNI_Reverso: Número de DNI que aparece en el reverso
- DNI_Anverso: Número de DNI que aparece en el anverso (debería coincidir con el número del reverso)
- DNI_Expira: Fecha de finalización de la validez del DNI. Formato: DD/MM/AAAA
- DNI_NumeroDeSerie: Número de Serie que figura en el DNI
- DNI_Pais: País de expedición del documento (abreviatura, por ejemplo ESP para España)
- DNI_Nacionalidad: Nacionalidad de la Persona tal como aparece en el DNI (por ejemplo ESP)
- DNI_FechaNacimiento: Fecha de nacimiento según aparece en el DNI. Formato: DD/MM/AAAA
- DNI_Sexo: Sexo que se indica en el DNI: M para varón , F para Mujer
- EsDNIPeticion: Si se ha incluido el parámetro DNI en la petición inicial, indica si corresponde con el número detectado. Posibles valores:
 - SI: Coincide
 - NO: No coincide
 - -1: No se indicó el parámetro DNI en la petición
- PruebaVida: Indica si ha pasado la prueba de vida (se ha detectado una persona con seguridad) Posibles valores:
 - SI: Ha pasado la prueba
 - NO-X-Y : No la ha pasado, X e Y son valores de referencia, para pasar el filtro Y no debería ser mayor que $X * 50$
- EdadAparente: Es una edad estimada en función del vídeo de la prueba de vida. En forma de rango, por ejemplo entre 30 y 40 años se indicaría como 30/40
- ParecidoPruebaVida: Es necesario comprobar que la prueba de vida la hace siempre la misma persona, por ello este parámetro (parecido en el vídeo de la persona detectada) debe superar 85-90%
- ParecidoDNI: es el parecido entre la persona que aparece en el DNI y la persona que realiza el proceso. Normalmente se requiere superior a 70% pero, por debajo del 75% debería validarse mediante el panel.
- SexoAparente: El sexo que parece tener la persona del vídeo de detección. Se indica también la probabilidad, por ejemplo Hombre/99 significa que es un hombre con una probabilidad del

99%.

- PETICIÓN AL VALIDAR EL PROCESO: Una vez que el destinatario ha realizado el proceso, aparecen los datos de la validación en el panel de usuario. Un operador debe 'validar' en función de los datos que se muestran y de las indicaciones del sistema. Si existen puntos problemáticos lo indica (por ejemplo no ha pasado la prueba de vida, el DNI está caducado, etc..). Una vez validado, se genera otra petición con los siguientes datos en formato POST:

- ID: Identificación original de la petición obtenida como respuesta inicial.
- IDContrato: Si se trata de un Contrato, aquí se indica el identificador del contrato.
- Telefono: Teléfono al que se ha enviado la petición.
- Resultado:
 - SI: Ha sido validado por el operador
 - NO: Ha sido rechazado por el operador.

- **Resp:** (String) Tipo de respuesta a mostrar.

Posibles valores:

- TXT: salida texto. Ejemplo:

```
Resp:1;  
Cred:12345.67;  
Id: 23598
```

- JSON: Respuesta en formato json. Ejemplo:

```
{  
  "Resp": "1",  
  "Cred": "12345.67",  
  "Id": "23598"  
}
```

- XML: Respuesta en formato XML. Ejemplo:

```
<?xml version="1.0"?>  
<result>  
  <Resp>1</Resp>  
  <Cred>12345.67</Cred>  
  <Id>23598</Id>  
</result>
```

DEVUELVE: string de la respuesta de la página:

- **Resp:**Número

Significado del Número:

1 Operación realizada correctamente.

-1 Error de autenticación

-2 No hay suficientes créditos

-3 No hay destinatario

-4, -5, -6 : Errores en la petición

-7: Si especifica el Mensaje a enviar en la petición debe incluir la etiqueta [LINK] que se sustituirá por el link de inicio del proceso de identificación

-10: La cuenta no tiene autorización para utilizar el servicio.

- **Cred:** Créditos en la cuenta del usuario.
- **Id:** Identificador de la petición único para cada petición y usuario.

5.4.- *SERVICIO DE SELLADO DE TIEMPO DE LA CASA DE LA MONEDA*

Objetivo:

Solicitud de sellado de tiempo según el estándar RFC 3161 .

Petición a:

<https://www.lofirmo.com/tsa>

PETICIÓN:

- En la cuenta de Cliente encontrará el usuario/contraseña para realizar las peticiones. Cualquier sistema o API que pueda sellar podrá configurarse para utilizar el servidor. Si desea realizar peticiones directas contacte con soporte para que le indiquemos cómo hacerlo. El funcionamiento según el estándar RF3161

5.5.- SELLADO DE TIEMPO DE PDFs DESDE APLICACIONES

Objetivo:

Si no dispone de una API de sellado o desea incorporar el sellado en sus PDF, puede utilizar esta utilidad.

La utilidad está desactivada por defecto y debe solicitar activación en su cuenta.

Petición a:

<https://www.lofirmo.com/api/v2/sellarPDF>

Parámetros POST:

- **Correo:** String con el correo del usuario que envía (en MENSATEK).
- **Passwd:** String con la contraseña del usuario que envía (en MENSATEK).
- **Contenido:** (Opcional) Contenido Base64 del fichero a sellar.
- **Tipo:** Forma de enviar el contenido del fichero
 - FILES: (Por defecto) como un POST de Fichero. En este caso, la variable contenido debe estar vacía.
 - BASE64: El string en base64 en la variable Contenido.
- **Resp:** Tipo de respuesta en caso de error. Posibilidades
 - JSON
 - XML
 - TXT

En caso de error, devuelve el código de error.

-1 Error de autenticación

-15: No se ha podido cargar el fichero

-16: Fichero demasiado grande, consulte con soporte para ampliar límites

-17: Ha ocurrido un error en la carga del fichero.

-18: Función no habilitada en esta cuenta, contacte con soporte



En caso de éxito, devuelve el contenido del fichero sellado en tiempo.