
H. AYUNTAMIENTO DE MORELIA
Administración 2024 – 2027

Servicio de Firma Web

Firmador-web (eFirma)

Documentación Técnica de Integración de API
Versión 1.0.0

Índice

1	Introducción	1
2	Configuración del Servidor y Entornos	1
3	Autenticación	1
4	Flujo de Trabajo Básico (Paso a Paso)	1
5	Endpoints	3
5.1	1. Enviar documento para prefirma	3
5.2	2. Firmar un archivo XML	4
5.3	3. Consulta de estatus administrativo por ID	4
5.4	4. Validación de autenticidad de XML	5
5.5	5. Descargar archivo XML por UUID	6

1 Introducción

Este documento describe la interfaz del servicio web **Firmador-web**, un sistema de firma digital basado en la eFirma. Permite cargar documentos para prefirma, aplicar firmas criptográficas, validar documentos XML firmados y consultar el estado actual del proceso de firma.

2 Configuración del Servidor y Entornos

Las peticiones deben dirigirse a uno de los siguientes entornos según corresponda:

- **Desarrollo:** <http://10.0.227.19:8005>
- **Interno:** <http://10.1.222.71:8008>
- **Externo:** <https://consultalic.morelia.gob.mx/apis/>

3 Autenticación

La API utiliza un esquema de API Key en los encabezados HTTP para todas las operaciones. Debe ser enviada en cada petición con la cabecera correspondiente:

X-API-KEY: <tu_api_key>

4 Flujo de Trabajo Básico (Paso a Paso)

El proceso general para completar una firma digital consta de los siguientes pasos:

1. **Generar la Prefirma:** Se consume el endpoint `/prefirma`. Aquí se envían los datos base en formato JSON (es obligatorio incluir los parámetros `sistema` y `asunto`), la lista de firmantes y el documento a firmar (preferiblemente PDF menor a 10MB).

2. **Ejecutar Firma:** Una vez obtenida la prefirma, se consume el endpoint `/firmar`. Las llaves criptográficas (`.cer`, `.key`) y contraseñas ya se encuentran resguardadas de manera segura dentro de la infraestructura interna, por lo que solo se requiere especificar el identificador único del XML y el RFC del firmante.
3. **Descarga y Consulta de Estado:** El XML resultante firmado se puede recuperar a través de la ruta de descarga. Además, se puede consultar el estado del flujo de firmas en cualquier momento utilizando el ID de la solicitud.
4. **Validación Externa:** Si se cuenta con el archivo XML físico firmado y se desea verificar su autenticidad e integridad, se utiliza el endpoint de validación técnica.

5 Endpoints

Todos los endpoints que reciben parámetros utilizan codificación de tipo **multipart/form-data**.

5.1 1. Enviar documento para prefirma

- **Método:** POST
- **Ruta:** /prefirma

Inicia el proceso de firma registrando los metadatos iniciales y asociando los participantes.

Cuerpo de la Petición (multipart/form-data)

- **documento** (Opcional, Archivo): Archivo a firmar (de preferencia formato PDF, peso menor a 10MB).
- **datos** (Requerido, JSON string): Datos de la operación. **Es mandatorio incluir sistema y asunto.**
- **firmantes** (Requerido, JSON string): Arreglo con la lista de firmantes asignados y su orden.
- **descarga** (Opcional, string): Opción para solicitar el formato de retorno (XML o JSON).

Ejemplo del campo JSON datos

```
{
  "id_unico": "6546541d6s14fds",
  "sistema": "pruebas",
  "asunto": "prefirma"
}
```

Ejemplo del campo JSON firmantes

```
[
  {
    "rfc": "CMS941215JF7",
    "rol": "Empleado",
    "orden": 1
  }
]
```

Ejemplo de Respuesta Exitosa (200 OK)

Al realizar la prefirma de manera correcta, obtendrás una respuesta estructurada que incluye el XML base generado, la URL del código QR para la validación y la información de los sellos:

```
{
  "url_xml": "http://10.0.227.19:8005/descargar_xml/bbcd00cd-a440...",
  "xml": "<Signature>\n <SignedInfo>\n...",
  "id": "bbcd00cd-a440-4686-9b46-17d19d705d17",
  "qr": "http://10.0.227.19:8005/genera_qr/bbcd00cd-a440...",
  "sellos": [
```

```
{
  {
    "rfc": "RFC_CONFIGURADO",
    "sello": "IDENTIFICADOR_UNICO_GENERADO_APARTIR_DE_LOS_DATOS"
  }
]
```

¿Qué es el Sello?

El **sello** es un identificador criptográfico único generado de forma automática a partir de la combinación de los datos del documento y la información del firmante configurado. Funciona como una pre-validación de identidad y asegura la integridad de los datos que van a ser firmados posteriormente con la eFirma.

5.2 2. Firmar un archivo XML

- **Método:** POST
- **Ruta:** /firmar

Aplica la firma electrónica al documento correspondiente. Para garantizar la máxima seguridad, las contraseñas y claves privadas están alojadas en el almacén seguro interno, por lo que este endpoint no las solicita directamente.

Cuerpo de la Petición (multipart/form-data)

- `xml_id` (Requerido, String / UUID): Identificador único del archivo XML generado en el paso de prefirma.
- `rfc` (Requerido, String): RFC de la persona que va a firmar.

5.3 3. Consulta de estatus administrativo por ID

- **Método:** POST
- **Ruta:** /consulta

Permite verificar **únicamente el estado de flujo actual** del proceso de firma en la base de datos, así como los detalles de los firmantes que ya han estampado su eFirma utilizando el identificador de la solicitud.

Nota: Este endpoint solo consulta el estatus lógico del proceso. No valida si la estructura del archivo XML físico o su contenido han sido alterados criptográficamente. Para validar la autenticidad técnica del archivo, utilice el método de validación.

Cuerpo de la Petición (multipart/form-data)

- `id` (Requerido, UUID): ID único de la solicitud (generado durante la prefirma).

Ejemplo de Respuesta Exitosa (200 OK)

```
{
  "status": 1,
  "mensaje": "Estatus del firmado",
  "xml_url": "https://consultalic.morelia.gob.mx/apis/descargar_xml/a809ea...",
  "Documento": {
    "datos": {
      "document_uuid": "a809ea30-417e-40e2-a1de-05b7e20bc60d",
      "fecha_firma": "01/06/2026",
      "meta_datos": {
        "asunto": "prefirma",
        "contrarecibo": "3a114ce8-a329-4972-957e-4e231f1f0e92",
        "sistema": "pruebas",
        "document_uuid": "a809ea30-417e-40e2-a1de-05b7e20bc60d",
        "fecha_firma": "01/06/2026"
      }
    }
  },
  "firmas": {
    "firmante_1": {
      "Status": 1,
      "mensaje": "Firma valida.",
      "nombre": "NOMBRE_DEL_FIRMANTE",
      "rfc": "RFC_USADO",
      "rol": "EMPLEADO",
      "serial": "NUMERO_DE_SERIE_DEL_CERTIFICADO",
      "email": "CORREO_REGISTRADO_EN_EL_CERTIFICADO",
      "sello": "IDENTIFICADOR_UNICO_GENERADO_APARTIR_DE_LOS_DATOS"
    }
  }
}
```

5.4 4. Validación de autenticidad de XML

- **Método:** POST
- **Ruta:** /validar

Verifica la **autenticidad e integridad física** de un archivo XML firmado. Analiza de forma matemática que el archivo no haya sido alterado con posterioridad a las firmas estampadas y que los certificados del SAT que lo componen sean vigentes y válidos.

Cuerpo de la Petición (multipart/form-data)

- `xml` (Requerido, Archivo): Archivo XML firmado que se desea someter a validación.

Ejemplo de Respuesta Exitosa (200 OK)

```
{
```

```

"datos": {
  "document_uuid": "a809ea30-417e-40e2-a1de-05b7e20bc60d",
  "fecha_firma": "01/06/2026",
  "meta_datos": {
    "sistema": "pruebas",
    "asunto": "prefirma",
    "contrarecibo": "3a114ce8-a329-4972-957e-4e231f1f0e92"
  }
},
"Firmas": {
  "firmante_1": {
    "Status": 1,
    "mensaje": "Firma valida.",
    "rfc": "RFC_USADO",
    "rol": "EMPLEADO",
    "serial": "NUMERO_DE_SERIE_DEL_CERTIFICADO",
    "email": "CORREO_REGISTRADO_EN_EL_CERTIFICADO",
    "sello": "IDENTIFICADOR_UNICO_GENERADO_APARTIR_DE_LOS_DATOS"
  }
}
}

```

5.5 5. Descargar archivo XML por UUID

- **Método:** GET
- **Ruta:** /descargar_xml/{uuid}

Descarga el XML final firmado utilizando su identificador único.

Parámetros de Ruta (Path Params)

- **uuid** (Requerido, String / UUID): Identificador único del archivo XML.