

Firma Digital

Web Service Firmador

Envío de solicitudes de firma digital de archivos

CONEXIÓN.....	3
AUTENTICACIÓN	4
SERVICIOS	6
FIRMADOR	6
FIRMADOR MASIVO.....	8
FIRMADOR HASH	10
FIRMADOR HASH MASIVO	11
ESTADOS.....	12
RECIBIR HASH FIRMADOS.....	13
FIRMADOR XML MASIVO	14
RECIBIR XML FIRMADOS	15

Conexión

URL: <http://Firmador.tucertificado.com.ar>

Autenticación

La autenticación al servicio web se realiza implementando **HMAC (Hash-based message authentication code)**

El cliente y el servidor comparten una **clave privada** y un **Identificador de cliente**

El **Identificador de cliente** identifica a la empresa como entidad autorizada a hacer uso de la API de firmado.

Paso 1

El cliente crea una cadena de caracteres combinando los siguientes datos

- **Identificador de Cliente**
- HTTP Method
- Request URI
- Request Time Stamp
- Nonce
- Hash MD5 codificado en Base 64 del Contenido del Request

Request URI: En minúscula y codificada.

Request Time Stamp: se calcula usando UNIX Time (Cantidad de segundos desde el 01/01/1970) para evitar inconvenientes con diferencias de zonas horarias entre el cliente y el servidor.

Nonce: Numero/cadena de caracteres arbitrario que se usa una única vez. Se utiliza para evitar ataques de replay. Son 32 caracteres que pueden ser números o letras.

Ejemplo: 235890d3ca0f4d299b7347d261992bef

Paso 2

El cliente calcula el hash de la cadena de caracteres construida en el primer paso utilizando el algoritmo SHA256 y la **clave privada**. El resultado de este hash es una firma única para este Request.

Paso 3

La firma generada en el paso anterior se envía en el encabezado **Authorization** usando como esquema "hmac".

Los datos en el encabezado Authorization van a contener el identificador del cliente, Request Time Stamp y el nonce separados por ":".

El formato del encabezado Authorization va a ser:

[Authorization: hmac APPIId:Signature:Nonce:Timestamp]

Paso 4

El cliente envía el request con los datos generados en el paso anterior en el encabezado Authorization

Servicios

Firmador

URL: <http://Firmador.tucertificado.com.ar/api/Firmador>

Método: POST

JSON:

```
{"CUILPersona":"123","NombreArchivo":"Prueba.pdf","HashArchivo":"12345678","Razon":"Informe","CUITEmpresa":"123","CoordenadaX":"10","CoordenadaY":"8","Ancho":"100","Alto":"100","NumeroPagina":"1","Visible":"true"}
```

Resultado: Se devuelve un SessionID. El SessionID es una cadena de caracteres que identifica unívocamente a la solicitud enviada.

Aclaraciones

- El HashArchivo se calcula con SHA-1
- En este Request no se envía el contenido binario del archivo PDF. El archivo PDF se sube por SFTP antes de llamar a esta API
- En caso de que se especifique que la firma no va a ser visible, no es necesario que se envíen las coordenadas, el ancho, el alto y el número de página.

Mensajes de Error

Código de Estado HTTP: 204 (No Content)

Frase: Debe enviar un número de CUIL de la persona que debe firmar el documento

Código de Estado HTTP: 204 (No Content)

Frase: Debe enviar el hash del archivo

Código de Estado HTTP: 204 (No Content)

Frase: Debe enviar el nombre del archivo

Código de Estado HTTP: 204 (No Content)

Frase: Se produjo un error con el archivo recibido

Código de Estado HTTP: 204 (No Content)

Frase: El usuario no posee un método de autenticación OTP

Código de Estado HTTP: 204 (No Content)

Frase: El CUIL ingresado no es valido

Código de Estado HTTP: 500 (Internal Server Error)

Frase: Error de servidor

Firmador Masivo

URL: <http://Firmador.tucertificado.com.ar/api/FirmadorMasivo>

Método: POST

JSON:

```
{ "CUILPersona": "123", "CUITEmpresa": "123", "Archivos": [ { "NombreArchivo": "Prueba1.pdf", "HashArchivo": "12345678", "Razon": "Conforme", "CoordenadaX": 5, "CoordenadaY": 7, "Ancho": 10, "Alto": 10, "NumeroPagina": 1, "Visible": true }, { "NombreArchivo": "Prueba2.pdf", "HashArchivo": "123456789", "Razon": "No Conforme", "CoordenadaX": 9, "CoordenadaY": 1, "Ancho": 20, "Alto": 20, "NumeroPagina": 1, "Visible": false } ] }
```

Resultado: Se devuelve un SessionID. El SessionID es una cadena de caracteres que identifica unívocamente a la solicitud enviada.

Aclaraciones

- El HashArchivo se calcula con SHA-1
- En este Request no se envía el contenido binario del archivo PDF. El archivo PDF se sube por SFTP antes de llamar a esta API
- En caso de que se especifique que la firma no va a ser visible, no es necesario que se envíen las coordenadas, el ancho, el alto y el número de página.

Mensajes de Error

Código de Estado HTTP: 204 (No Content)

Frase: Debe enviar un número de CUIL de la persona que debe firmar el documento

Código de Estado HTTP: 204 (No Content)

Frase: Debe enviar el hash del archivo

Código de Estado HTTP: 204 (No Content)

Frase: Debe enviar el nombre del archivo

Código de Estado HTTP: 204 (No Content)

Frase: Se produjo un error con el archivo recibido

Código de Estado HTTP: 204 (No Content)

Frase: El usuario no posee un método de autenticación OTP

Código de Estado HTTP: 204 (No Content)

Frase: El CUIL ingresado no es valido

Código de Estado HTTP: 500 (Internal Server Error)

Frase: Error de servidor

Firmador Hash

URL: <http://Firmador.tucertificado.com.ar/api/FirmadorHash>

Método: POST

JSON:

```
{"CUILPersona":"123","CUITEmpresa":"123","Hash":[67,0,67,0,50,0,56,0,50,0,66,0,50,0,69,0,48,0,55,0,55,0,66,0,66,0,66,0,49,0,55,0,69,0,56,0,49,0,66,0,66,0,53,0,50,0,57,0,68,0,69,0,51,0,70,0,65,0,56,0,49,0,70,0,57,0,54,0,52,0,65,0,49,0,48,0,52,0,70,0]}
```

Resultado: Se devuelve un SessionID. El SessionID es una cadena de caracteres que identifica unívocamente a la solicitud enviada.

Aclaraciones

- El HashArchivo se calcula con SHA-1. Se envía el array de bytes

Firmador Hash Masivo

URL: <http://Firmador.tucertificado.com.ar/api/FirmadorHashMasivo>

Método: POST

JSON:

```
{"CUILPersona":"123","CUITEmpresa":"123","Hash":[{"Hash":[67,0,67,0,50,0,56,0,50,0,66,0,50,0,69,0,48,0,55,0,55,0,66,0,66,0,66,0,49,0,55,0,69,0,56,0,49,0,66,0,66,0,53,0,50,0,57,0,68,0,69,0,51,0,70,0,65,0,56,0,49,0,70,0,57,0,54,0,52,0,65,0,49,0,48,0,52,0,70,0]},{
"Hash":[67,0,67,0,50,0,56,0,50,0,66,0,50,0,69,0,48,0,55,0,55,0,66,0,66,0,66,0,49,0,55,0,69,0,56,0,49,0,66,0,66,0,53,0,50,0,57,0,68,0,69,0,51,0,70,0,65,0,56,0,49,0,70,0,57,0,54,0,52,0,65,0,49,0,48,0,52,0,70,0]}}]}
```

Resultado: Se devuelve un SessionID. El SessionID es una cadena de caracteres que identifica unívocamente a la solicitud enviada.

Aclaraciones

- El Hash se calcula con SHA-1. Se envía el array de bytes

Estados

URL: [http://Firmador.tucertificado.com.ar/api/EstadoSolicitud?SessionsID\[\]=1&SessionsID\[\]=2](http://Firmador.tucertificado.com.ar/api/EstadoSolicitud?SessionsID[]=1&SessionsID[]=2)

Método: GET

Respuesta JSON: [{"CodigoEstado":1,"MensajeEstado":"Pendiente de Validacion","SessionID":"1","HashFirmado":"123"}, {"CodigoEstado":1,"MensajeEstado":"Pendiente de Validacion","SessionID":"2","HashFirmado":"123"}]

Posibles Estados:

CodigoEstado: 0

MensajeEstado: La Solicitud no ha sido validada aún con el OTP/PIN correspondiente

CodigoEstado: 1

MensajeEstado: El tiempo para validar la Solicitud ha expirado

CodigoEstado: 2

MensajeEstado: La Solicitud fue encolada pero el archivo aún no ha sido firmado.

CodigoEstado: 3

MensajeEstado: La Solicitud fue encolada y el archivo está en proceso de firma

CodigoEstado: 4

MensajeEstado: El archivo ya está firmado.

CodigoEstado: 5

MensajeEstado: Se produjo un error al intentar firmar el archivo.

Recibir Hash Firmados

URL: <http://Firmador.tucertificado.com.ar/api/HashFirmado?SessionID=1>

Método: GET

Respuesta JSON:

```
[{"Hash":"CCC","HashFirmado":"DDD","DetalleError":"","CUIL":"2000000001"},  
{"Hash":"EEE","HashFirmado":"GGG","DetalleError":"","CUIL":"2000000001"}]
```

Firmador Xml Masivo

URL: <http://Firmador.tucertificado.com.ar/api/FirmadorXmlMasivo>

Método: POST

JSON: {"CUILPersona":"123","CUITEmpresa":"123","Xml":[{"Hash":"123","xml":"ccc"}, {"Hash":"456","xml":"bbb"}]}

Resultado: Se devuelve un SessionID. El SessionID es una cadena de caracteres que identifica unívocamente a la solicitud enviada.

Recibir Xml Firmados

URL: <http://Firmador.tucertificado.com.ar/api/XmlFirmado?SessionID=1>

Método: GET

Respuesta JSON:

```
[{"Hash":"CCC","XmlFirmado":"DDD","DetalleError":"","CUIL":"2000000001"},  
{"Hash":"EEE","XmlFirmado":"GGG","DetalleError":"","CUIL":"2000000001"}]
```