SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

SAT
Servicio de Administración Tributaria

Documentación del Servicio de Aceptación/Rechazo

Fecha: Julio 2018

Versión 1.0

Tabla de Contenido

1. Introducción

El servicio de Aceptación / Rechazo se diseñó para permitir al Receptor de CFDI aceptar o rechazar, a través de un PAC, la cancelación de una factura recibida que no cumpla con los requisitos para una cancelación directa. Esto mediante un servicio publicado en la página del SAT desde internet, siendo que este servicio solo puede ser consumido por los PAC por medio de autenticación, con lo cual se protege esta información.

El presente documento contiene la información necesaria para conocer y utilizar dicho servicio.

2. Prerrequisitos

Contar con el Certificado de Sello Digital (CSD).

Estar dado de alta como PAC (Proveedor Autorizado de Certificación).

3. Modo de Uso para Servicios

A fin de utilizar los servicios web descritos en el presente documento es necesario crear el cliente de servicios web correspondiente a partir de la URL del Servicio y/o la URL del WSDL de acuerdo con las instrucciones de la plataforma desde la que se vaya a consumir el servicio web.

En la descripción de cada uno de los servicios se proporcionará la URL del servicio y / o del WSDL para generar el cliente del servicio web.

Para mayor información acerca de la manera en la que se genera el cliente del servicio web consulte la documentación de la plataforma desde la que consumirá el servicio.

Una vez que se creó el cliente el siguiente paso es verificar el tipo de certificado a enviar para poder realizar la autenticación y posterior consumo de los servicios.

En el siguiente paso se habla específicamente de cómo realizar dicha autenticación.

4. Autenticación para Servicios

Adicionalmente, para utilizar los servicios web descritos en el presente documento es necesario autenticarse ante el servidor de servicios web mediante un par de llaves proporcionados por el SAT, estas llaves son las correspondientes al certificado de Sello Digital (CSD).

El tipo de autenticación del servicio cumple con las especificaciones de Web Services Security v1.0 (WS-Security 2004):

https://www.oasis-open.org/standards#wssv1.0

A continuación, se muestra la parte del WSDL de cada uno de los servicios que menciona el método de autenticación que se requiere para el consumo de los servicios:

Servicio Autenticación

A fin de facilitar la autenticación mediante el uso del CSD, se recomienda utilizar el almacén local de llaves criptográficas para almacenar y recuperar una llave para utilizarla posteriormente, a continuación se muestra un ejemplo de código en C# de cómo obtener un certificado especifico.

Ejemplo:

```
private static X509Certificate2 ObtenerKey(string thumbPrint)
{
    X509Store store = new X509Store(StoreName.My, StoreLocation.LocalMachine);
    store.Open(OpenFlags.ReadOnly);
    var certificates = store.Certificates;
    var certificateEnc = certificates.Find(X509FindType.FindByThumbprint, thumbPrint, false);
    if (certificateEnc.Count > 0)
    {
        X509Certificate2 certificate = certificateEnc[0];
        return certificate;
    }

    return null;
}
```

Una vez seleccionado el certificado a utilizar como medio de autenticación se tiene que mandar la petición hacia el servicio de autenticación para poder obtener el token que se requiere para poder usar los servicios como son recepción y cancelación, esto se realiza de la siguiente manera:

Ejemplo

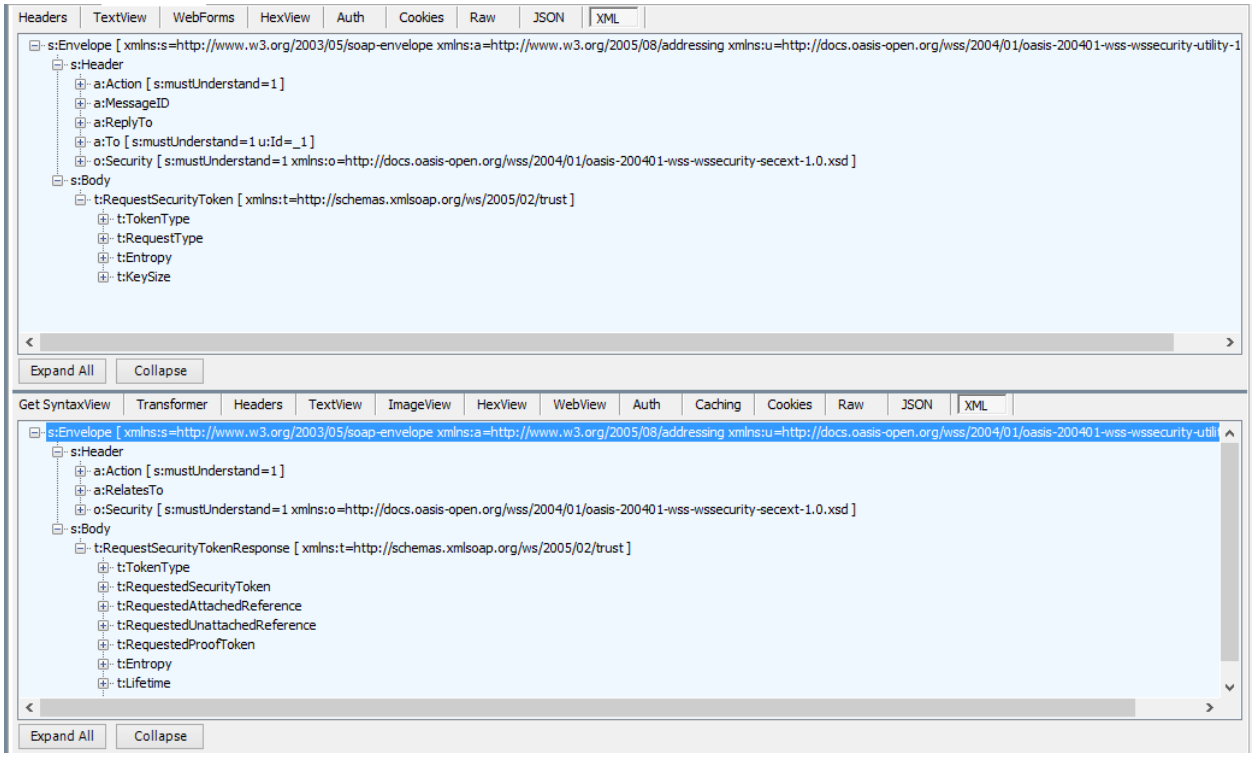
Servicio Autenticación

```
autentificacion.ClientCredentials.ClientCertificate.Certificate = certi[0];
string token = autentificacion.Autentica();
```

El código mostrado anteriormente es en C#, pero sirve como ejemplo para ilustrar como enviar estos certificados a los servicios descritos y poder obtener el token de autenticación correspondiente.

Ahora se muestra un ejemplo de cómo se ve una petición hacia el servicio de autenticación:

Servicio Autenticación



Si existe algún error durante la autenticación y no se obtiene el token no se podrá utilizar los demás servicios; otro punto a considerar es que al consumir los servicios se validara el token enviado si este es válido se podrá hacer uso de los métodos expuestos de cada uno, en caso contrario se mandara una excepción de autenticación y no se podrá hacer eso del Web Services.

Es importante mencionar también que para poder hacer uso de los Servicios Web se tiene que estar dado de alta como PAC, de no ser así la autenticación no será satisfactoria.

El alta como PAC seguirá un proceso definido por el SAT (Servicio de Administración Tributaria).

5. Servicio Aceptación/Rechazo

Es un servicio web que permite consultar las solicitudes de cancelación que se tienen pendientes para un receptor en específico, así como aceptar o rechazar dichas solicitudes de cancelación por parte de los PAC's y devolver un acuse con el estatus de la petición. Este WS está compuesto por las siguientes operaciones:

ObtenerPeticionesPendientes

Esta operación permite consultar las solicitudes de cancelación que se encuentran en espera de una respuesta por parte del receptor, así mismo regresa un acuse con el resultado o estatus de la petición realizada.

Los parámetros que requiere esta operación son los siguientes:

Parámetro	Tipo de Dato	Descripción	Tipo de Parámetro
Token Autenticación	Header	Contiene el token de autenticación que se obtuvo en el servicio correspondiente, se debe de usar el nombre “Authorization” y el valor debe de ser en el siguiente formato “WRAP access_token="Token"”	Entrada
rfcReceptor	String	Contiene el RFC del receptor del cual se quiere consultar las solicitudes de cancelación pendientes	Entrada
ObtenerPeticionesPendientesResult	ObtenerPeticionesPendientesResult	Contiene el resultado de la petición con el código de respuesta y los UUID de los CFDIs de los cuales se solicitó la cancelación, pero se encuentran en espera de una confirmación por parte del receptor.	Salida

Ejemplo de petición a la operación ObtenerPeticionesPendientes del servicio Aceptación/Rechazo

```
POST https://anexo20cfdicancelacion.cloudapp.net/Cancelacion/AceptacionRechazoService.svc HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
SOAPAction: "http://cancelacfd.sat.gob.mx/IAceptacionRechazoService/ObtenerPeticionesPendientes"
Authorization: WRAP access_token="eyJhbGciOiJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzA0L3httbGRzaWctbW9yZSNobWFjLXNoYTI1NiIsInR5cCI6IkpXVCJ9.eyJuYmYiOjE1MTY0MDEyMzAsImV4cCI6MTUxNjQwMTgzMCwiaWF0
Content-Length: 367
Host: anexo20cfdicancelacion.cloudapp.net
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.1.1 (java 1.5)

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:can="http://cancelacfd.sat.gob.mx">
   <soapenv:Header/>
   <soapenv:Body>
      <can:ObtenerPeticionesPendientes>
         <!--Optional:-->
         <can:rfcReceptor>BAF060524EV6</can:rfcReceptor>
      </can:ObtenerPeticionesPendientes>
   </soapenv:Body>
</soapenv:Envelope>
```

En el ejemplo anterior se puede visualizar que la petición va dividida en dos partes:

- La primera de ellas es el Header que contiene el token de autenticación, del cual se puede encontrar el detalle en el tema 4 Autenticación para servicios.
- La segunda es aquella que contiene la petición hacia el servicio con los parámetros ya establecidos anteriormente, como se mencionó en el punto de la autenticación esta operación del Web Services solo podrá ser usada siempre y cuando se haya autenticado de manera exitosa y el token sea válido en el tiempo que se está intentando consumir.

Ejemplo de respuesta de la operación ObtenerPeticionesPendientes del servicio Aceptación/Rechazo

En el ejemplo mostrado en la imagen anterior se puede ver que la respuesta contiene dos partes:

- La primera de ellas es el Header que contiene temas relacionados con la seguridad.
- La segunda de ellas es el body que contendrá los parámetros de salida mencionados anteriormente.

Mensajes recibidos desde la operación ObtenerPeticionesPendientes del servicio Aceptación/Rechazo

	Descripción del Código	Código	Observaciones
Estatus Petición	Usuario No Válido	300	Este código de error se regresa cuando la autenticación del usuario no fue exitosa.
	XML Mal Formado	301	Este código de error se regresa cuando el request posee información invalida, ejemplo: un RFC de receptor no válido
	Se obtuvieron las peticiones del RFC Receptor de forma exitosa	1100	
	No existen peticiones para el RFC Receptor	1101	Este código se regresa cuando la consulta se realizó de manera exitosa, pero no se encontraron solicitudes de cancelación para el rfc receptor

ProcesarRespuesta

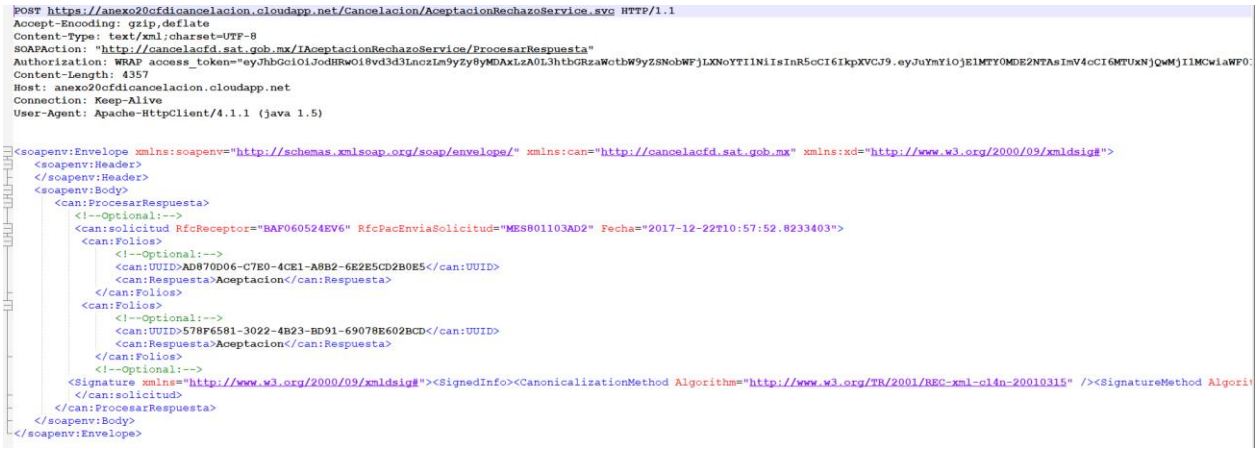
Esta operación permite dar una respuesta de “Aceptación” o “Rechazo” a las solicitudes de cancelación que se encuentran en espera de dicha resolución por parte del receptor, así mismo regresa un acuse con el resultado o estatus de la petición realizada.

Los parámetros que requiere esta operación son los siguientes:

Parámetro	**Tipo de Dato**	**Descripción**	**Tipo de Parámetro**
Token Autenticación	Header	Contiene el token de autenticación que se obtuvo en el servicio correspondiente, se debe de usar el nombre “Authorization” y el valor debe de ser en el siguiente formato “WRAP access_token="Token"”	Entrada
Solicitud	Solicitud	Contiene la información requerida para procesar las respuestas a las solicitudes de cancelación, este parámetro está compuesto por los atributos: • RfcReceptor • RfcPacEnviaSolicitud • Fecha Y puede contener dese 1 hasta 500 elementos de tipo **Folios**.	Entrada
RfcReceptor	String	Contiene el RFC del receptor al cual pertenecen los CFDIs	Entrada
RfcPacEnviaSolicitud	String	Contiene el RFC del PAC que está realizando la petición	Entrada
Fecha	DateTime	Contiene la fecha actual de cuando se está realizando la petición	Entrada
Folios	Folios	Este parámetro está compuesto por los elementos UUID y Respuesta	Entrada
UUID	String	Contiene el UUID correspondiente al CFDI del cual se solicitó una	Entrada

		cancelación y se encuentra en espera de una respuesta por parte del receptor.	
Respuesta	TipoAccionPeticionCancelacion	Contiene la resolución que se le dará a la solicitud de cancelación, este parámetro solo puede contener los valores: • Aceptacion • Recchazo	Entrada
Signature	Signature	Firma realizada con el certificado csd correspondiente al receptor al cual pertenecen los CFDIs que se les dará respuesta a su solicitud de cancelación.	Entrada
ProcesarRespuestaResult	ProcesarRespuestaResult	Contiene el resultado de la petición con un código general y un código de respuesta individual para cada uno de los Folios.	Salida

Ejemplo de petición a la operación ProcesarRespuesta del servicio Aceptación/Rechazo



```
POST https://anexo20cfdicancelacion.cloudapp.net/Cancelacion/AceptacionRechazoService.svc HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
SOAPAction: "http://cancelacfd.sat.gob.mx/IAceptacionRechazoService/ProcesarRespuesta"
Authorization: WRAP access_token="eyJhbGciOiJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzA0L3htbGRzaWctbW9yZSNobWFjLXNoYTI1NiIsInR5cCI6IkpXVCJ9.eyJuYmYiOjE1MTY0MDE2NTAsImV4cCI6MTUxNjQwMjI1MCwiaWF0
Content-Length: 4357
Host: anexo20cfdicancelacion.cloudapp.net
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.1.1 (java 1.5)

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:can="http://cancelacfd.sat.gob.mx" xmlns:xd="http://www.w3.org/2000/09/xmldsig#">
   <soapenv:Header>
   </soapenv:Header>
   <soapenv:Body>
      <can:ProcesarRespuesta>
         <!--Optional:-->
         <can:solicitud RfcReceptor="BAP060524EV6" RfcPacEnviaSolicitud="MES801103AD2" Fecha="2017-12-22T10:57:52.8233403">
            <can:Folios>
               <!--Optional:-->
               <can:UUID>AD870D06-C7E0-4CE1-A8B2-6E2E5CD2B0E5</can:UUID>
               <can:Respuesta>Aceptacion</can:Respuesta>
            </can:Folios>
            <can:Folios>
               <!--Optional:-->
               <can:UUID>578F6581-3022-4B23-BD91-69078E602BCD</can:UUID>
               <can:Respuesta>Aceptacion</can:Respuesta>
            </can:Folios>
            <!--Optional:-->
         <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" /><SignatureMethod Algori
         </can:solicitud>
      </can:ProcesarRespuesta>
   </soapenv:Body>
</soapenv:Envelope>
```

En el ejemplo anterior se puede visualizar que la petición va dividida en dos partes:

- La primera de ellas es el Header que contiene el token de autenticación, del cual se puede encontrar el detalle en el tema 4 Autenticación para servicios.
- La segunda es aquella que contiene la petición hacia el servicio con los parámetros ya establecidos anteriormente, como se mencionó en el punto de la autenticación

esta operación del Web Services solo podrá ser usada siempre y cuando se haya autenticado de manera exitosa y el token sea válido en el tiempo que se está intentando consumir.

Ejemplo de respuesta de la operación ProcesarRespuesta del servicio Aceptación/Rechazo

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Encoding: gzip
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Fri, 19 Jan 2018 22:41:46 GMT
Content-Length: 1236

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><ProcesarR
```

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
   <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <ProcesarRespuestaResponse xmlns="http://cancelacfd.sat.gob.mx">
         <ProcesarRespuestaResult RfcReceptor="BAF060524EV6" RfcPac="MES801103AD2" CodEstatus="1000" Fecha="2018-01-19T16:41:45.2817393">
            <Folios Respuesta="Aceptacion">
               <UUID>AD870D06-C7E0-4CE1-A8B2-6E2E5CD2B0E5</UUID>
               <EstatusUUID>1000</EstatusUUID>
            </Folios>
            <Folios Respuesta="Aceptacion">
               <UUID>578F6581-3022-4B23-BD91-69078E602BCD</UUID>
               <EstatusUUID>1000</EstatusUUID>
            </Folios>
            <Signature Id="SelloSAT" xmlns="http://www.w3.org/2000/09/xmldsig#">
               <SignedInfo>
                  <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                  <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#hmac-sha512"/>
                  <Reference URI="">
                     <Transforms>
                        <Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
                           <XPath>not(ancestor-or-self::*[local-name()='Signature'])</XPath>
                        </Transform>
                     </Transforms>
                     <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
                     <DigestValue>VvHSsj5sUT6Ws1lDKwtpJdoRwvo0lh0IWbRtJihjs1s+E/HKH5XYHpyXwi+b2nfxQ1vWLaoqkWm2w/xaiMKRaA==</DigestValue>
                  </Reference>
               </SignedInfo>
               <SignatureValue>B9iZ7vNKayE6iosd+CkiTZweHm3VwJ14HEMnr2pyV1fWpN+1XbwN4yCFXb88tPggf+oqfqMc49CyNdtwDmTHew==</SignatureValue>
               <KeyInfo>
                  <KeyName>BF66E582888CC845</KeyName>
                  <KeyValue>
                     <RSAKeyValue>
                        <Modulus>n5YsGT0w5Z70ONPbqszhExfJU+KY3Bscftc2jxUn4wxpSjEUhnCuTd88OK5QbDW3Mupoc61jr83lRhUCjchFAmCigpC10rEntTfEU+7qtX8ud/jJJDBla9lTIB6bhBN//X8IQDjhmHrfKvfen3p7
                        <Exponent>AQAB</Exponent>
                     </RSAKeyValue>
                  </KeyValue>
               </KeyInfo>
            </Signature>
         </ProcesarRespuestaResult>
      </ProcesarRespuestaResponse>
```

En el ejemplo mostrado en la imagen anterior se puede ver que la respuesta contiene dos partes:

- La primera de ellas es el Header que contiene temas relacionados con la seguridad.
- La segunda de ellas es el body que contendrá los parámetros de salida mencionados anteriormente.

Mensajes recibidos desde la operación ProcesarRespuesta del servicio Aceptación/Rechazo

Evento	Mensaje	Observaciones
300	Usuario No Válido	Este código de error se regresa cuando la autenticación del usuario no fue exitosa.
301	XML Mal Formado	Este código de error se regresa cuando el request posee información invalida, ejemplo: un RFC de receptor no válido
302	Sello Mal Formado	

304	Certificado Revocado o Caduco	El certificado puede ser inválido por múltiples razones como son el tipo, la vigencia, etc.
305	Certificado Inválido	El certificado puede ser inválido por múltiples razones como son el tipo, la vigencia, etc.
309	Patrón de Folio inválido	El patrón de folios para registro fiscal no coincide. Aplicable únicamente a cancelaciones de CFDI de RIF
310	CSD Inválido	
1000	Se recibió la respuesta de la petición de forma exitosa	
1001	No existen peticiones de cancelación en espera de respuesta para el uuid	Se recibió la respuesta de forma exitosa, sin embargo, no se encontró ninguna solicitud de cancelación pendiente
1002	Ya se recibió una respuesta para la petición de cancelación del uuid	
1003	Sello No Corresponde al RFC Receptor	
1004	Existen más de una petición de cancelación para el mismo uuid	
1005	El uuid es nulo no posee el formato correcto	
1006	Se rebaso el número máximo de solicitudes permitidas	Se cuenta con un límite 500 solicitudes pendientes por petición. Estás 500 solicitudes deben pertenecer al mismo Receptor.