



Documentación para la implementación del Servicio Web de Descarga Masiva de CFDI y retenciones.

Servicio de Verificación de
Descarga de Solicitudes Exitosas.

Agosto 2018
Versión 1.1



Tabla de contenido

1. Introducción	3
2. Prerrequisitos	3
3. Modo de Uso para Servicios	3
4. Autenticación para Servicios	4
5. Servicio Verificación de Descarga Masiva	7
6. Control de cambios	14



1. Introducción

El servicio Descarga Masiva de CFDI y Retenciones está diseñado para que los contribuyentes en su calidad de Emisores o Receptores de CFDI puedan recuperar sus comprobantes que hayan emitido o recibido por las operaciones comerciales realizadas, en este sentido se llevó a cabo la implementación del servicio Web (WS por sus siglas en inglés) que le permite la descarga masiva en sus propios equipos de cómputo, para lo cual deberá desarrollar un mecanismo de comunicación, el cual se diseñó con fin de:

- Generar solicitudes de descarga masiva de CFDI y CFDI de Retenciones.
- Verificar el estatus de las solicitudes realizadas.
- Permitir realizar la descarga de los archivos XML o metadatos generados en archivos compactados mediante las solicitudes que se hayan procesado de manera exitosa.

En la presente documentación se describe la forma en la que el contribuyente realizará la comunicación para verificar el estatus de las solicitudes de descarga realizadas previamente, a través del servicio de solicitud de descarga masiva, cabe mencionar que algunas recomendaciones están enfocadas para realizarse en los equipos de cómputo propios del contribuyente, de no ser así se debe garantizar no poner en riesgo su información almacenándola en un equipo que no sea el propio.

2. Prerrequisitos

El contribuyente debe contar con el Certificado de tipo e.Firma vigente para solicitar la información.

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.

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 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

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 e.Firma vigente.

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 de la e.Firma vigente, se recomienda utilizar el almacén local de llaves criptográficas para almacenar y recuperar una llave para utilizarla posteriormente, es importante mencionar que esto se puede realizar siempre y cuando estés utilizando tu propio equipo de cómputo para establecer la comunicación con el Web Service, de no ser así se debe garantizar que la información referente a la e.Firma no se almacene en el equipo de un tercero, a continuación se muestra un ejemplo de código en C# de cómo obtener un certificado específico.

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 usar el servicio de verificación de descarga masiva, esto se realiza de la siguiente manera:

Ejemplo

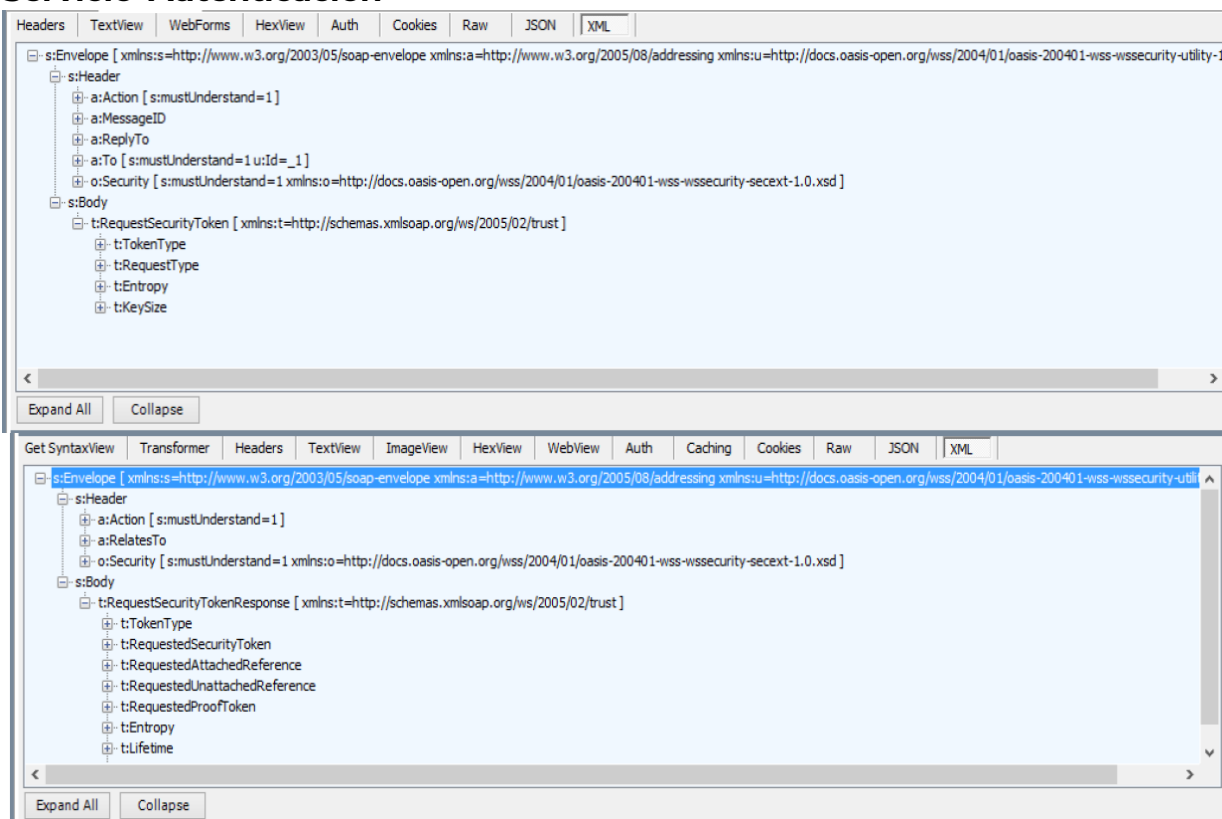
Servicio Autenticación

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

El código mostrado anteriormente es en C#, pero sirve como ejemplo para ilustrar cómo 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



The image shows two screenshots of a SOAP message viewer. The top screenshot displays a SOAP request message. The root element is `s:Envelope` with namespaces for SOAP, addressing, and WSS. The header contains `a:Action`, `a:MessageID`, `a:ReplyTo`, `a:To`, and `o:Security`. The body contains `t:RequestSecurityToken` with sub-elements `t:TokenType`, `t:RequestType`, `t:Entropy`, and `t:KeySize`. The bottom screenshot displays a SOAP response message. The root element is `s:Envelope` with the same namespaces. The header contains `a:Action`, `a:RelatesTo`, and `o:Security`. The body contains `t:RequestSecurityTokenResponse` with sub-elements `t:TokenType`, `t:RequestedSecurityToken`, `t:RequestedAttachedReference`, `t:RequestedUnattachedReference`, `t:RequestedProofToken`, `t:Entropy`, and `t:Lifetime`.

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<s:Header>
<o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
<u:Timestamp u:id="_0">
<u:Created>2018-05-09T21:21:42.953Z</u:Created>
<u:Expires>2018-05-09T21:26:42.953Z</u:Expires>
</u:Timestamp>
```




```
T3LYruwpGXq4jW4hbTELUuMg/+c3hxXdFyvmU5sajRYbVm+Vqya4IJQ+aZfR4d9ZfWgW2t7S
vv9WL4ikaizyWbTGN5LLasr69AzS2g87JfHq7mbmycl+BL/Enu5EZdf/K/r/UykmDvN9sdUMdU
CRcT3A2M66VHDcOZYnVxUkR7yV8NC8MLP2Hz3wlrKPRUQm4qjFQOi4fpqtlnXwwKpMg==
</SignatureValue>
  <KeyInfo>
    <o:SecurityTokenReference>
      <o:Reference Value="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3" URI="#uuid-572bbc7a-287d-4233-bdcb-75f92418becd-1" />
    </o:SecurityTokenReference>
  </KeyInfo>
</Signature>
</o:Security>
<To s:mustUnderstand="1"
xmlns="http://schemas.microsoft.com/ws/2005/05/addressing/none">https://desktop-
3fi24u7:444/Autenticacion/Autenticacion.svc</To>
  <Action s:mustUnderstand="1"
xmlns="http://schemas.microsoft.com/ws/2005/05/addressing/none">http://DescargaMasiva
Terceros.gob.mx/IAutenticacion/Autentica</Action>
</s:Header>
<s:Body>
  <Autentica xmlns="http://DescargaMasivaTerceros.gob.mx" />
</s:Body>
</s:Envelope>
```

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 validará el token enviado si este es válido se podrá hacer uso de los métodos expuestos de cada uno, en caso contrario se mandará una excepción de autenticación y no se podrá hacer uso del Web Service.

Nota: El servicio de autenticación descrito en esta sección, es el mismo a utilizar para los servicios de Solicitud de Descarga Masiva, Verificación Descarga Masiva y Descarga Masiva.

5. Servicio Verificación de Descarga Masiva

Es un servicio web que permite verificar el estatus de las solicitudes de descarga realizadas previamente a través del servicio de solicitud de descarga masiva, en caso de que la solicitud de descarga haya sido aceptada y se encuentre con estatus de terminado, este servicio de verificación devolverá los identificadores de los paquetes que conforman la solicitud de descarga. Este WS está compuesto por la siguiente operación:

VerificaSolicitudDescarga

Esta operación permite verificar el estatus de la solicitud de descarga masiva realizada previamente.

Los parámetros que requiere esta operación son los siguientes:



Parámetro	Tipo de Dato	Descripción	Tipo Parámetro
Authorization	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 - Obligatorio
IdSolicitud	String	Contiene el Identificador de la solicitud que se pretende consultar.	Entrada - Obligatorio
RfcSolicitante	String	Contiene el RFC del solicitante que genero la petición de solicitud de descarga masiva.	Entrada - Obligatorio
Signature	SignatureType	Firma de la petición realizada con el certificado de tipo e.Firma vigente.	Entrada - Obligatorio
IdsPaquetes	Lista o secuencia con datos de tipo String	Contiene los identificadores de los paquetes que componen la solicitud de descarga masiva. Solo se devuelve cuando la solicitud posee un estatus de finalizado.	Salida - Opcional
EstadoSolicitud	Int	Contiene el número correspondiente al estado de la solicitud de descarga, Estados de la solicitud: Aceptada=1 EnProceso=2 Terminada=3 Error=4 Rechazada=5 Vencida=6	Salida - Obligatorio
CodigoEstadoSolicitud	String	Contiene el código de estado de la solicitud de descarga, los cuales pueden ser 5000,5002,5003,5004 o 5005 para más información revisar la tabla "Códigos Solicitud Descarga Masiva".	Salida - Obligatorio



Content-Length: 4641

Host: srvsolicituddescargamaster.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:des="http://DescargaMasivaTerceros.sat.gob.mx"
xmlns:xd="http://www.w3.org/2000/09/xmldsig#">
  <soapenv:Header/>
  <soapenv:Body>
    <des:VerificaSolicitudDescarga>
      <!--Optional:-->
      <des:solicitud IdSolicitud="4E80345D-917F-40BB-A98F-4A73939343C5"
RfcSolicitante="AXT940727FP8">
        <!--Optional:-->
        <Signature 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/2000/09/xmldsig#rsa-sha1"/>
            <Reference URI="">
              <Transforms>
                <Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
              </Transforms>
              <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <DigestValue>leZ4dK/Q/RNbckYkY7WOOncjK5Q=</DigestValue>
              </Reference>
            </SignedInfo>
```

```
<SignatureValue>BuuRjPmgk4QwI2ER7vjL7+57WiqNZMRD12Hjfh65irE1lCu8biQSqeHHiaZ7Nn
mB/LsjyGaHQmZMW50mfnDtNzowAadytB6FS0RNUNLoajAZAdii8bYHYoW0BqrLaXSIImwbZYa
Hgi4TIPch1OpXZHmUOqfS1qnEEsRXVBN2DvEh1RbAYupmQxBMW75eo4HZZm/IRug44mb47
Evm9428ejTzTnu6LDPEAZEmHV4jOwRzqmM4GgiW7aEptqHOhdSxV+QzPSQ2/H5s8AZZ4ILC
K+3gSdCq3Kmf9S2H5R3BRS6VSAM5J9xa0I2CvzJf/REwrxHsc7Xk9uXwXWOofjeTIIbW==</Signa
tureValue>
```

```
<KeyInfo>
  <X509Data>
    <X509IssuerSerial>
      <X509IssuerName>OID.1.2.840.113549.1.9.2=Responsable: ACDMA,
OID.2.5.4.45=SAT970701NN3, L=Coyoacán, S=Distrito Federal, C=MX, PostalCode=06300,
STREET="Av. Hidalgo 77, Col. Guerrero", E=asisnet@pruebas.sat.gob.mx, OU=Administración
de Seguridad de la Información, O=Servicio de Administración Tributaria, CN=A.C. 2 de
pruebas(4096)</X509IssuerName>
```




- 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 VerificaSolicitudDescarga del servicio de Verificación descarga masiva

```

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: Thu, 10 May 2018 16:38:15 GMT
Content-Length: 430

<?xml version="1.0" encoding="utf-8" ?>
<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">
    <VerificaSolicitudDescargaResponse xmlns="http://DescargaMasivaTerceros.sat.gob.mx">
      <VerificaSolicitudDescargaResult CodEstatus="5000" EstadoSolicitud="3"CodigoEstadoSolicitud="5000" NumeroCFDIs="0" Mensaje="Solicitud Aceptada">
        <IdsPaquetes>4e80345d-917f-40bb-a98f-4a73939343c5_01</IdsPaquetes>
        <IdsPaquetes>4e80345d-917f-40bb-a98f-4a73939343c5_02</IdsPaquetes>
        <IdsPaquetes>4e80345d-917f-40bb-a98f-4a73939343c5_03</IdsPaquetes>
        <IdsPaquetes>4e80345d-917f-40bb-a98f-4a73939343c5_04</IdsPaquetes>
        <IdsPaquetes>4e80345d-917f-40bb-a98f-4a73939343c5_05</IdsPaquetes>
        <IdsPaquetes>4e80345d-917f-40bb-a98f-4a73939343c5_06</IdsPaquetes>
      </VerificaSolicitudDescargaResult>
    </VerificaSolicitudDescargaResponse>
  </s:Body>
</s:Envelope>

```

```

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: Thu, 10 May 2018 16:38:15 GMT
Content-Length: 430
<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">
    <VerificaSolicitudDescargaResponse xmlns="http://DescargaMasivaTerceros.sat.gob.mx">
      <VerificaSolicitudDescargaResult CodEstatus="5000" EstadoSolicitud="3"CodigoEstadoSolicitud="5000" NumeroCFDIs="0" Mensaje="Solicitud Aceptada">
        <IdsPaquetes>4e80345d-917f-40bb-a98f-4a73939343c5_01</IdsPaquetes>
        <IdsPaquetes>4e80345d-917f-40bb-a98f-4a73939343c5_02</IdsPaquetes>
        <IdsPaquetes>4e80345d-917f-40bb-a98f-4a73939343c5_03</IdsPaquetes>

```



```

<IdsPaquetes>4e80345d-917f-40bb-a98f-4a73939343c5_04</IdsPaquetes>
<IdsPaquetes>4e80345d-917f-40bb-a98f-4a73939343c5_05</IdsPaquetes>
<IdsPaquetes>4e80345d-917f-40bb-a98f-4a73939343c5_06</IdsPaquetes>
</VerificaSolicitudDescargaResult>
</VerificaSolicitudDescargaResponse>
</s:Body>
</s:Envelope>

```

En el ejemplo mostrado en la imagen anterior se puede ver que la respuesta contiene los parámetros de salida mencionados anteriormente.

Nota importante: Las direcciones electrónicas (URL) que se integran en esta documentación, son solo referencia para la correcta interpretación de los ejemplos contenidos, por lo que las URL válidas para la implementación del Web Service, están publicadas en la sección Consulta y Recuperación de Comprobantes, del apartado de Factura Electrónica en el Portal del SAT.

Mensajes recibidos desde la operación VerificaSolicitudDescarga del servicio de Verificación descarga masiva

Evento	Mensaje	Observaciones
300	Usuario No Válido	
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	
303	Sello no corresponde con RfcSolicitante	
304	Certificado Revocado o Caduco	El certificado fue revocado o bien la fecha de vigencia expiró.
305	Certificado Inválido	El certificado puede ser invalido por múltiples razones como son el tipo, codificación incorrecta, etc.
5000	Solicitud recibida con éxito	La petición de verificación fue recibida con éxito.
5004	No se encontró la información	No se encontró la solicitud con el identificador enviado.



Códigos Solicitud Descarga Masiva

Evento	Mensaje	Observaciones
5000	Solicitud recibida con éxito	Indica que la solicitud de descarga que se está verificando fue aceptada.
5002	Se agotó las solicitudes de por vida	Para el caso de descarga de tipo CFDI, se tiene un límite máximo para solicitudes con los mismos parámetros (Fecha Inicial, Fecha Final, RfcEmisor, RfcReceptor).
5003	Tope máximo	Indica que en base a los parámetros de consulta se está superando el tope máximo de CFDI o Metadata, por solicitud de descarga masiva.
5004	No se encontró la información	Indica que la solicitud de descarga que se está verificando no generó paquetes por falta de información.
5005	Solicitud duplicada	En caso de que exista una solicitud vigente con los mismos parámetros (Fecha Inicial, Fecha Final, RfcEmisor, RfcReceptor, TipoSolicitud), no se permitirá generar una nueva solicitud.
404	Error no Controlado	Error genérico, en caso de presentarse realizar nuevamente la petición y si persiste el error levantar un RMA.

6. Control de cambios

En la siguiente sección se muestra un resumen de los cambios realizados al documento para brindar mayor entendimiento al contribuyente.

Cambio realizado	Fecha del cambio
1. Introducción: se precisa que la documentación contiene recomendaciones que pueden aplicarse siempre y cuando se utilice un equipo propio que no comprometa la información.	14/08/2018
4. Autenticación para Servicios. Servicio de autenticación: Se precisa que la e.firma no debe almacenarse en el repositorio de llaves criptográficas si no se está utilizando un equipo propio, a fin de no comprometer la información.	14/08/2018