Documento Técnico Informático para certificadores del Régimen FEL

Acuerdo de Directorio 13-2018 – Régimen de Factura Electrónica en Línea

Versión 1.2

Tabla de contenido

I. Presentación 4
- **A. Objetivo y alcance** 4
- **B. Síntesis del proceso** 5

II. Documento Tributario Electrónico 7
- **A. Definición del esquema** 7
- **B. Elementos requeridos en la emisión** 8
- **C. Incorporación de firma electrónica de emisión** 8
- **D. Complementos** 9
- **E. Utilización del elemento Adenda** 9
- **F. Elementos requeridos al certificar** 10
- **G. Incorporación de firma electrónica de certificación** 11
- **H. Esquema y catálogos** 12
- **I. Información técnica de incorporación de firma** 13

III. Servicio de recepción de DTE 15
- **A. API de recepción** 15
- **B. Autenticación del API** 15
- **C. Envío de un DTE al API** 16

IV. Servicio de Anulación de DTE 19
- **A. Descripción** 19
- **B. Esquema de la operación de anulación** 19
- **C. Incorporación de firma electrónica de emisión** 19
- **D. API de Anulación** 20
- **E. Autenticación del API** 20
- **F. Envío de una Anulación al API** 21

V. Modelo de publicación/suscripción de catálogos 24
- **A. Catálogo base (mini-RTU)** 24
- **B. Esquema de funcionamiento** 25
- **C. Suscripción** 25
- **D. API de recepción de notificaciones** 25
- **E. Estructura JSON** 26

VI. Anexo A: Catálogos Publicados 27

Índice de ilustraciones

Ilustración 1 Proceso de emisión, certificación y envío a SAT 5
Ilustración 2 Elementos mínimos incorporados por el EMISOR 8
Ilustración 3 Elementos principales de un DTE Certificado 10
Ilustración 4 Catálogos del Sistema 12
Ilustración 5 - Ejemplo de estructura de firma electrónica Xades-Bes 14
Ilustración 6 Proceso de Generación de Token 16
Ilustración 7 Header con la Llave Access_Token 17
Ilustración 8 DTE incorporado en el POST 17
Ilustración 9 Acuse de recibo de SAT 18
Ilustración 10 Proceso de Generación de Token 21
Ilustración 11 Header con la Llave Access_Token 22
Ilustración 12 Anulación incorporada en el POST 22
Ilustración 13 Acuse de recibo de SAT 23
Ilustración 14 Modelo de publicación/suscripción 25

Nota de la versión 1.2: Se actualizaron URL hacia el nuevo ambiente para desarrollo y pruebas.

El documento técnico informático está orientado está sujeto a cambios sin aviso previo aviso, debidamente versionados y comunicados a las personas que se encuentren en el proceso de autorización como certificador coordinado por la Intendencia de Recaudación.

I. Presentación

A. Objetivo y alcance

Este documento describe los aspectos técnicos-informáticos de los servicios desarrollados por la SAT para nuevo sistema de factura electrónica en línea, que deben ser empleados por los CERTIFICADORES De acuerdo con los lineamientos técnicos y condiciones acá establecidas.

Los principales que se requiere sean utilizados y se describen son los siguientes:

- Servicios y mecanismo de propagación para el modelo de Proveedor/Subscriptor (P/S) que se utilizará para realizar la sincronización de información con cada uno de los CERTIFICADORES.
- Servicio para la recepción de información, el cual realiza la función de recibir cada DTE que sean enviado por el CERTIFICADOR.

Este documento no tiene por si solo toda la información necesaria para el desarrollo informático de un CERTIFICADOR, solo complementa aspectos técnicos informáticos de los diferentes documentos que conforman las disposiciones del Régimen FEL conforme con lo establecido en el Acuerdo de Directorio 13-2018, las cuales deben ser leídas y comprendidas por los interesados previamente a este documento.

Dentro del presente documento tiene información general del funcionamiento de los servicios electrónicos del Régimen FEL, así como también el funcionamiento de la autenticación para poder consumir los servicios que se están proporcionando por parte de SAT. El documento requiere de conocimiento y experiencia informática.

Características generales requeridas

El Régimen FEL requiere un sistema que debe desarrollarse e implementar para la recepción de grandes volúmenes de información, en el caso de certificadores por cuenta propia para soportar adecuadamente las operaciones propias del contribuyente y para los certificadores que ofrecerán los el servicio a terceros debe considerar las características siguientes:

- ✓ **Capacidad elástica:** Los contribuyentes con alto volumen de operaciones y quienes presten el servicio a terceros, requieren la capacidad de cargar grandes volúmenes de datos en pocos segundos.
- ✓ **Respuesta inmediata:** El proceso de certificación ocurre previo a la entrega de los documentos, por lo que la respuesta del certificador debe ser inmediata.

- ✓ **Información en tiempo real:** Quienes presten el servicio a terceros, deben brindar a sus usuarios y a la SAT acceso a en tiempo real a información que permita verificar del cumplimiento del acuerdo de nivel de servicio.
- ✓ **Monitoreo interno del sistema:** Quienes presten el servicio a terceros, deben contar con un monitoreo y proceso de control de todos los componentes del sistema con la finalidad de garantizar el cumplimiento del acuerdo de niveles de servicio con sus clientes y de las obligaciones con la SAT.
- ✓ **Cumplimiento:** Por su naturaleza, el diseño, desarrollo, implementación y mantenimiento del sistema debe siempre cumplir con la legislación aplicable, reglamentos y disposiciones que regulan, el Régimen FEL y cada uno de los tipos de documentos tributarios electrónicos a ser emitidos.
- ✓ **Seguridad informática:** Deben implementar de los controles de seguridad en la gestión de la información y de seguridad de la infraestructura y plataforma que sean necesarios bajo la premisa que el certificador maneja información que confidencial e incorpora firma electrónica de emisión y de certificación.

Estos requisitos son más relevantes cuando el servicio se presta a terceros porque se gestiona información confidencial propiedad de terceros; si el certificador además brinda el sistema o componente para construcción del XML con firma de emisión deberá considerar los controles específicos para el correcto uso y protección del certificado digital para la firma de emisión del contribuyente.

B. Síntesis del proceso

El sistema del CERTIFICADOR debe tener la capacidad de envió de información en línea, para garantizar que la información se encuentre registrada en SAT de forma inmediata, a manera de síntesis, se describe el proceso de la forma en que opera el Régimen FEL, el cual se puede visualizar de la siguiente forma:

Ilustración 1 Proceso de emisión, certificación y envío a SAT

1. Cada emisor o contribuyente construye un XML con firma de emisión y lo envía al CERTIFICADOR, quien debe aplicar todas las reglas de validación proporcionadas por la SAT, debiendo retornar al emisor un mensaje de error cuando no se cumplan las validaciones.

2. Una vez validado el mensaje satisfactoriamente por parte del CERTIFICADOR, este asigna número de autorización de forma automatizada y e incorpora la firma electrónica avanzada a la certificación.

3. El mensaje es enviado en formato XML por medio del API de recepción para que SAT proceda a realizar las verificaciones correspondientes, para determinar si el documento es válido o invalido.

4. La SAT devuelve un acuse de recibo con un código de mensaje de respuesta de acuerdo conl catálogo definido y confirmará si el mensaje se rechazó y si se recibió sin errores o con errores.

5. El CERTIFICADOR está obligado a almacenar el acuse de recibo de cada DTE enviado, el cual irá firmado por parte de la SAT.

Cuando un documento es rechazado o recibido con errores no imputables al certificador, el certificador tiene la obligación de informar al emisor para su conocimiento y las acciones necesarias; si el rechazo o error es imputable al certificador, este debe corregirlo y enviar de nuevo el documento.

Considerando que este documento únicamente se refiere a la implementación técnica de los servicios en la nube, se invita a los certificadores a revisar el Procedimiento de Autorización del Certificador. Este documento contiene secciones relacionadas con áreas de tecnología:

- ✓ B) Requisitos de desempeño
- ✓ C) Funcionalidad general del sistema del certificador
- ✓ D) Funcionalidad del sistema del certificador para el emisor
- ✓ E) Requisitos de tecnología

Adicionalmente, contiene la lista de revisión de seguridad del certificador necesaria porque contiene:

- ✓ Controles mínimos requeridos y estándares de seguridad requeridos.
- ✓ A verificar por una entidad auditora de seguridad de la información.
- ✓ Contempla normas sobre el uso de centros de datos, servicios de colocación y servicios en la nube.

II. Documento Tributario Electrónico

A. Definición del esquema

El formato en que se generarán los documentos tributarios electrónicos XML o Lenguaje Extensible de "Etiquetado", EXtensible Markup Language. Este metalenguaje proporciona una forma de aplicar etiquetas para describir las partes que componen un documento, permitiendo además el intercambio de documentos entre diferentes plataformas.

Este formato cumple con el esquema definido y proporcionado por SAT, los DTE deben construirse de acuerdo con el esquema de definición del XML que la SAT publicará de forma oficial por medio de Internet y que se describe por medio de un XSD en el cual se define la estructura de XML, es decir los elementos que contiene y sus tipos de datos, atributos, formatos, valores permitidos, entre otras características que deben cumplirse.

La observancia del cumplimiento del XSD aplica para la emisión, certificación y recepción de los DTE. Para este efecto el emisor, certificador, receptor y la SAT tienen disponible los archivos XSD oficiales que facilitan la validación del esquema del documento.

El esquema se define a partir de un XSD principal para la generación de DTE y otros XSD adicionales que se requieren en casos especiales y se listan a continuación:

Archivo XSD	Propósito
GT_documento.xsd	Esquema principal de los Documentos Tributarios Electrónicos para FEL.
GT_Complemento_Referencia_Nota.xsd	Complemento utilizado para incorporar en notas de crédito, débito o abono la información del documento original (factura) al cual aplica.
GT_Complemento_Fac_Especial.xsd	Complemento requerido para las facturas especiales.
GT_Complemento_Exportaciones.xsd	Complemento requerido para facturas que tengan como destino la exportación.
GT_Complementos_Cambiaria.xsd	Complemento aplicable para elementos específicos de la factura cambiaria.

El esquema principal adicionalmente refiere al XSD que implementa la firma electrónica por medio del estándar creado por W3C y que se amplía más adelante. Los archivos XSD se encuentran publicados en la dirección siguiente:

- https://cat.desa.sat.gob.gt/xsd/alfa/
    - https://cat.desa.sat.gob.gt/xsd/alfa/GT_Documento-0.1.0.xsd
    - https://cat.desa.sat.gob.gt/xsd/alfa/GT_Complemento_Referencia_Nota-0.1.0.xsd
    - https://cat.desa.sat.gob.gt/xsd/alfa/GT_Complemento_Fac_Especial-0.1.0.xsd
    - https://cat.desa.sat.gob.gt/xsd/alfa/GT_Complemento_Exportaciones-0.1.0.xsd
    - https://cat.desa.sat.gob.gt/xsd/alfa/GT_Complemento_Cambiaria-0.1.0.xsd

B. Elementos requeridos en la emisión

La primera construcción del DTE ocurre al momento en que el EMISOR debe crear la estructura del DTE con los datos de emisión e incorporar la firma electrónica de emisión. Los elementos mínimos requeridos se visualizan en siguiente ilustración:

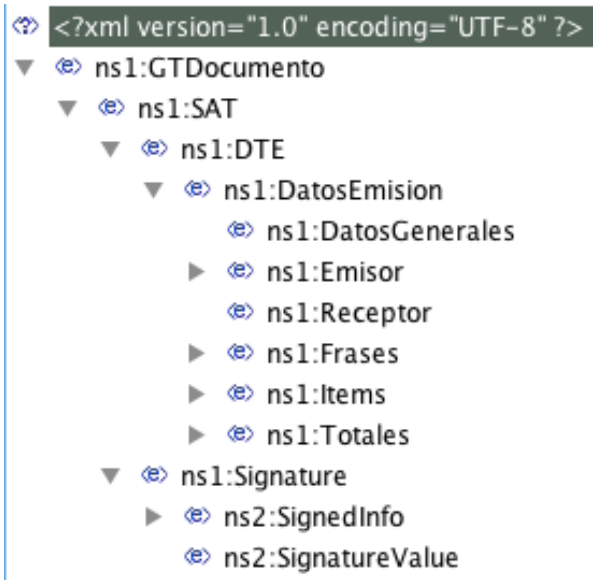

Ilustración 2 Elementos mínimos incorporados por el EMISOR

En el elemento DatosEmisión el EMISOR consignará los datos de acuerdo con lo establecido en el documento de reglas y validaciones (**Documento Reglas y Validaciones**). Adicionalmente a los elementos mínimos requeridos por el XSD el nodo DatosEmision puede tener un elemento Complementos, por ejemplo, en el caso de notas de débito y crédito.

Es el EMISOR el responsable de los datos de emisión, independiente del proceso o sistema empleado la incorporación de la firma electrónica de emisión vincula a la persona que emite el DTE hacia los datos contenidos en el elemento DatosEmision.

C. Incorporación de firma electrónica de emisión

En el nodo Signature, el EMISOR incorporará un nodo conteniendo la firma de emisión, la cual se realiza sobre el elemento DatosEmision, de acuerdo con los lineamientos técnicos descritos más adelante.

Para la firma el EMISOR debe emplear el certificado digital que la SAT le entregará por medio de los mecanismos que para tal efecto de establezcan. El certificado digital que SAT otorgue es de uso exclusivo

del emisor, para tal efecto deberá implementar mecanismos de seguridad bajo su exclusiva responsabilidad.

El CERTIFICADOR y la SAT deben validar la firma de emisión siempre que reciban un DTE y están obligados a rechazar cualquier DTE que no cumpla con la firma. Un receptor también puede validar la firma de emisión, ya que sin una firma de emisión valida el DTE tampoco tiene validez porque esto significa que existe una alteración de los datos.

En el proceso de validación de la firma electrónica, la vigencia del certificado digital se verifica respecto a la fecha emisión del documento.

> *Para las pruebas de firma de emisión en ambiente de desarollo pueden emplear un certificado generado por ustedes (Certificados RSA con llaves de 2048) en el servicio: https://www.pkicloud.com/*

D. Complementos

Los complementos deben incorporarse conforme con las disposiciones del Régimen FEL y forman parte de los nodos firmados por el EMISOR.

Cuando existan, los complementos deben ser enviado a la SAT, la SAT verificará y puede rechazar o informar error si un complemento requerido no es enviado.

E. Utilización del elemento Adenda

El elemento Adenda existe para que se pueda incorporar el XML del DTE información que sea de interés propio del EMISOR o bien a requerimiento del RECEPTOR de común acuerdo el EMISOR.

El elemento Adenda no forma parte de los elementos DatosEmision ni DTE, motivo por el cual no se encuentra firmado por el EMISOR ni por el RECEPTOR y no altera la validez de un DTE.

El elemento Adenda no debe ser enviado a la SAT, si un DTE es enviado a la SAT conteniendo el elemento Adenda la SAT rechazará el mismo y deberá enviarse de nuevo sin el mismo.

F. Elementos requeridos al certificar

Luego de validar el documento que el EMISOR ha firmado, el CERTIFICADOR genera un nuevo XML donde incorpora los datos de certificación y la firma electrónica de emisión. El documento resultante contiene los nodos siguientes:

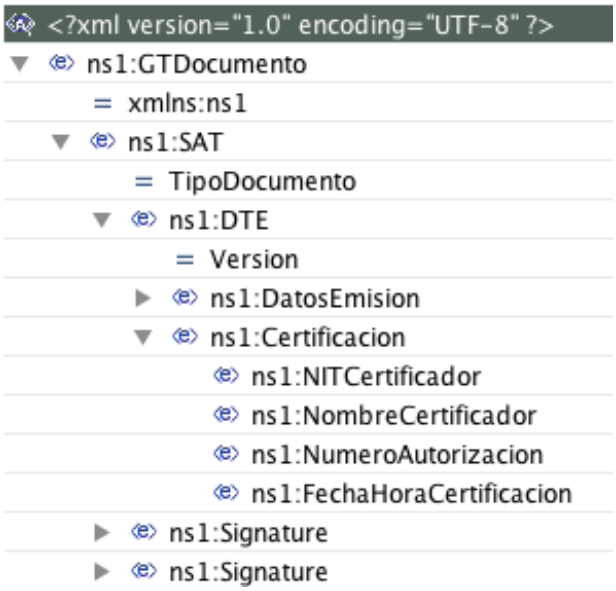

Ilustración 3 Elementos principales de un DTE Certificado

Los elementos DatosEmision y el primer elemento Signature corresponden a los creados originalmente por el EMISOR y deben mantener la validez de la firma.

El elemento Certificación incorpora NIT, Nombre del CERTIFICADOR, Número de autorización y la fecha y hora en la que el certificador está firmando el DTE.

El elemento NumeroAutorización contiene el identificador único que el CERTIFICADOR debe asignar cuando el documento se ha validado es de tipo aleatorio, es decir, versión 4 de acuerdo con la especificación de UUID[1]. Cada CERTIFICADOR es responsable verificar que no exista en su sistema duplicidad de UUID, si existe colisión al generar un UUID se debe generar uno nuevo.

[1] Ver referencia: https://es.wikipedia.org/wiki/Identificador_%C3%BAnico_universal

G. Incorporación de firma electrónica de certificación

El certificador agrega un segundo elemento Signature, el cual firma los datos del nodo DTE. Ambas firmas deben ser válidas para que el DTE sea válido.

La firma electrónica de certificación debe ser generada con un certificado de firma electrónica del CERTIFICADOR emitido por un prestador de servicios de certificación autorizado por el Registro de Prestadores de Servicios de Certificación.

La firma electrónica de emisión se aplica sobre el nodo de DTE, SAT debe validarla siempre que reciba un DTE y está obligada a rechazar cualquier DTE que no cumpla con la firma. En el proceso de validación de la firma electrónica, la vigencia del certificado digital del emisor y del certificador se verifica respecto a la fecha emisión del documento.

H. Esquema y catálogos

Como en todo sistema existen varios catálogos que son de utilidad para las personas que utilizaran el sistema, para mantener la certeza de los catálogos vigentes, se encuentran clasificados en los grupos siguientes:

Ilustración 4 Catálogos del Sistema

Catálogos dentro del XSD → Algunos catálogos se encuentran explícitos dentro del XSD proporcionado si en algún momento se realiza algún cambio, estos variarán dentro del mismo XSD y serán publicados en la misma dirección que se proporcionó.

Catálogos publicados en un repositorio → Otros catálogos no van explícitos en el XSD y se encontrarán publicados en formato JSON[2] en un repositorio publicado en la dirección[3] siguiente: https://cat.desa.sat.gob.gt/catalogos/

Modelo de publicación / suscripción → Catálogos con cambio de información tributaria constante, este permitirá tener actualizada la información del RTU que se comparte con cada uno de los CERTIFICADORES.

[2] Referencia: https://es.wikipedia.org/wiki/JSON
[3] En esta carpeta se publicarán las versiones de catálogos bajo la misma lógica explicada para las versiones de XSD (alfa/prod).

I. Información técnica de incorporación de firma

El DTE cuenta con dos firmas electrónicas, una firma electrónica de emisión y una firma electrónica de certificación. Conceptualmente y en congruencia con la ley de la materia, la primera es una firma electrónica simple realizada con un certificado digital que la SAT brindará al contribuyente emisor y la segunda es una firma electrónica avanzada realizada con un certificado digital que el Certificador adquiere con un prestador de servicios autorizado; sin embargo, técnicamente, ambas son incorporadas al XML por medio de un elemento Signature con un ID diferente para la firma de emisión y para la firma electrónica avanzada del certificador, ambas empleando las extensiones **Xades-Bes y firmas tipo RSA con algoritmo SHA-256.**

A continuación, se muestra un ejemplo:


```
– <ds:Signature Id="xmldsig-a66e3aa9-fd76-472f-8f48-af88fafa0c12">
  – <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    – <ds:Reference Id="xmldsig-a66e3aa9-fd76-472f-8f48-af88fafa0c12-ref0" URI="">
      – <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>FJ0fd8NjJDIUi4AiGSoyKRQaJlX226BFEb3/UEEN/M8=</ds:DigestValue>
      </ds:Reference>
    – <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#xmldsig-a66e3aa9-fd76-472f-8f48-af88fafa0c12-signedprops">
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>vKqq4EWOTvcSHG4yZjd8xcSngK+sdtK0Rh/zErK2Ulk=</ds:DigestValue>
      </ds:Reference>
  </ds:SignedInfo>
  – <ds:SignatureValue Id="xmldsig-a66e3aa9-fd76-472f-8f48-af88fafa0c12-sigvalue">
      THBuJe0So5CoeyuCa+IzaPch4RZ7oPGVDhvjqBK/VU/Hlgw9hAISwQmK9RgjGH9AmqqXBM6U2usw
      iXATSAcqSlQPYl1G2vKeQUNswUBOjqqBi/pO2LlThUHdYR3fHRvbK3b2D2EDbznQ/mmvbqWYWuEP
      ++EAnnYOc0dPCvKdIrFwjPHB7pruQptFy7YjOdDYNP5gMpPE14i02lQxBenx9J0NFzGZ0iD4kqF8
      eeoqo1aYJa//hvKKueIs0ZR8bYQ8jKPwwF7YwCostFdfdj4YLqkKA5gQRjrfsPDsRKBSsdg04MkQ Mlu57V9QszoVVHX7WznTSdsgzbDC
  </ds:SignatureValue>
  – <ds:KeyInfo>
    – <ds:X509Data>
      – <ds:X509Certificate>
          MIIEFDCCAvygAwIBAgIIUxC/w+Zng7gwDQYJKoZIhvcNAQELBQAwSTELMAkGA1UEBhMCR1QxJDAi
          BgNVBAoMG1NBVCBBbWJpZW50ZSBkZSBwcnVlYmFzIEZFTDEUMBIGA1UEAwwLVGVzdCBGRUxERVYw
```

```
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
- <ds:Object>
  - <xades:QualifyingProperties Target="#xmldsig-a66e3aa9-fd76-472f-8f48-af88fafa0c12">
    - <xades:SignedProperties Id="xmldsig-a66e3aa9-fd76-472f-8f48-af88fafa0c12-signedprops">
      - <xades:SignedSignatureProperties>
          <xades:SigningTime>2018-05-30T18:07:19.391Z</xades:SigningTime>
        - <xades:SigningCertificate>
          - <xades:Cert>
            - <xades:CertDigest>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>DIb/JT5iA9WqUiOLdVNou4aBZbtOPrsOH2wy/9cRYQI=</ds:DigestValue>
              </xades:CertDigest>
            - <xades:IssuerSerial>
                <ds:X509IssuerName>CN=Test FELDEV,O=SAT Ambiente de pruebas FEL,C=GT</ds:X509IssuerName>
                <ds:X509SerialNumber>5985494752880460728</ds:X509SerialNumber>
              </xades:IssuerSerial>
            </xades:Cert>
          - <xades:Cert>
            - <xades:CertDigest>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>yAVTZ0ZGhQvm3pO4XjcEfg0jBX9FhmXSr9MqJOBs8ns=</ds:DigestValue>
              </xades:CertDigest>
            - <xades:IssuerSerial>
                <ds:X509IssuerName>CN=Test FELDEV,O=SAT Ambiente de pruebas FEL,C=GT</ds:X509IssuerName>
                <ds:X509SerialNumber>202440495352962062</ds:X509SerialNumber>
              </xades:IssuerSerial>
            </xades:Cert>
          </xades:SigningCertificate>
        </xades:SignedSignatureProperties>


        - <xades:SignedDataObjectProperties>
          - <xades:CommitmentTypeIndication>
            - <xades:CommitmentTypeId>
                <xades:Identifier>http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin</xades:Identifier>
              - <xades:Description>
                  Indicates that the signer recognizes to have created, approved and sent the signed data object
                </xades:Description>
              </xades:CommitmentTypeId>
              <xades:AllSignedDataObjects/>
            </xades:CommitmentTypeIndication>
          </xades:SignedDataObjectProperties>
        </xades:SignedProperties>
      </xades:QualifyingProperties>
    </ds:Object>
  </ds:Signature>
```

Ilustración 5 - Ejemplo de estructura de firma electrónica Xades-Bes

III. Servicio de recepción de DTE

A. API de recepción

Se habilitó un servicio de recepción en un ambiente con controles de autenticación; para verificar disponibilidad y acceso básico al ambiente puede abrir en un navegador el URL siguiente: https://api.desa.sat.gob.gt/test

En conexión exitosa la página devolverá un "OK". La disponibilidad del servicio es regular en horario laboral[4], en horario fuera de oficina el servicio puede ser interrumpido con previo aviso.

B. Autenticación del API

El servicio de recepción de información está basado en una autenticación, dicha autenticación se le denomina "Autenticación Básica" y se realiza por medio de un usuario y clave, para lo cual se devolverá un Token[5] de acceso con tiempo de expiración de acuerdo con los pasos descritos a continuación.

1. Se solicita la autenticación a través de la invocación del servicio, enviando el usuario y clave proporcionado por SAT, utilizando la configuración de envío de servicio REST con autenticación.

2. El servicio se encuentra en la dirección siguiente: https://api.desa.sat.gob.gt/getToken

3. El usuario y clave de pruebas deberá ser solicitado a SAT para que pueda ser dado de alta en el ambiente correspondiente.

[4] Horario de atención para ambiente de desarrollo: 7:00a 16:00 horas, lunes a viernes.
[5] Es una cadena de caracteres que tiene un significado coherente en cierto lenguaje de programación, los cuales son identificadores con palabras claves.

Como ejemplo, para realizar una prueba se puede hacer uso de la herramienta PostMan (https://chrome.google.com/webstore/detail/postman/).

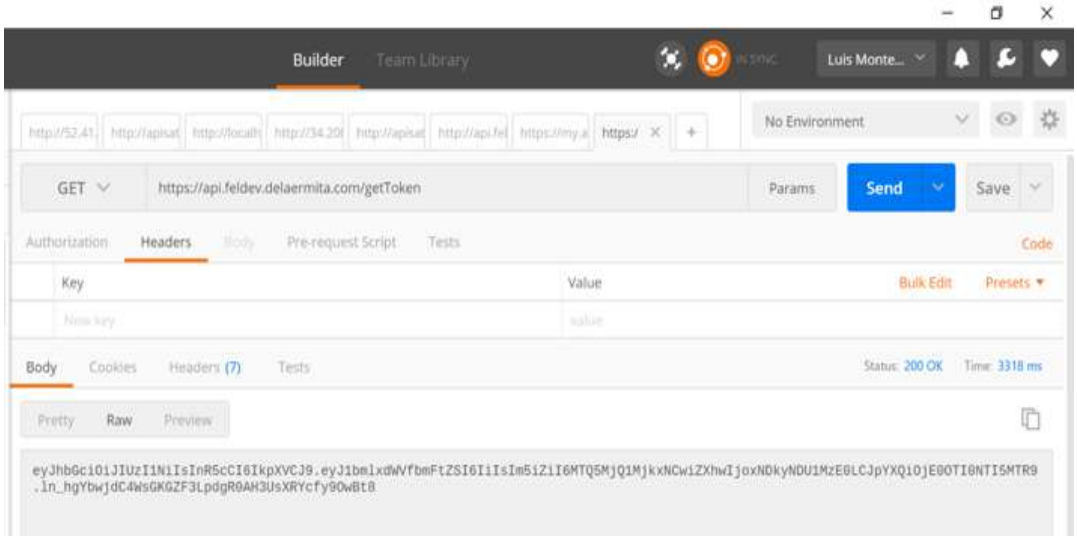

Ilustración 6 Proceso de Generación de Token

El método que invoca vía GET, necesita que se le envié una autenticación, la cual sería con el Usuario y Password que se le proporcionara, este método le devuelve un token el cual tiene un tiempo de vida (60 minutos), al vencer el token se debe de volver a generar uno nuevo.

C. Envío de un DTE al API

El API de recepción de DTE se encuentra publicado en la dirección siguiente: https://api.desa.sat.gob.gt/postFactura

Se envía la información a través de un método POST el cual viene conformado de la siguiente forma, en el Header se debe de incluir el token proporcionado en el paso anterior el cual debe definirse con el nombre de "Access _Token" para que la transacción pueda ser autorizada, y en el body el XML generado con la información de la factura generada.

Se debe de incluir dentro del Header una llave la cual tiene como valor el token devuelto en el método GET, se debe de garantizar que el nombre de la llave sea el indicado tomando en cuenta la sensibilidad al contexto para que pueda ser validado por el método de recepción, esto quedaría de la siguiente forma:

Ilustración 7 Header con la Llave Access_Token

Dentro del Body del mensaje debe de colocar el XML generado con la información de la factura emitida.

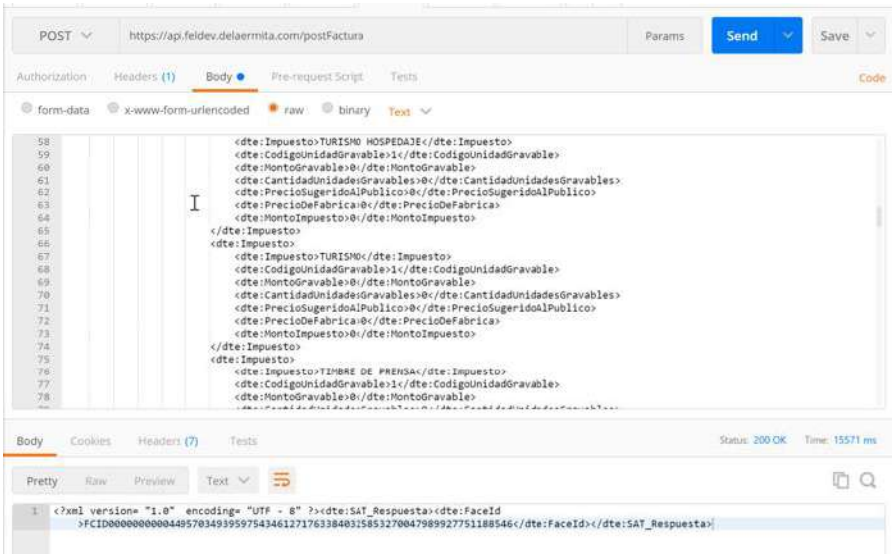

Ilustración 8 DTE incorporado en el POST.

Luego de enviar el DTE por medio del método POST, el API de SAT devolverá un mensaje con un código de éxito si todo salió correctamente o fallo si no paso las validaciones; dichos códigos se encuentran detallados en el catálogo de Errores, para que puedan ser interpretados de mejor manera.

Si el mensaje es exitoso, se devolverá un acuse de recibo el cual le garantiza que el mensaje fue registrado dentro del sistema de SAT, esto sirve para evidenciar que las transacciones están en el lugar, el mensaje seria de la forma[6] siguiente:

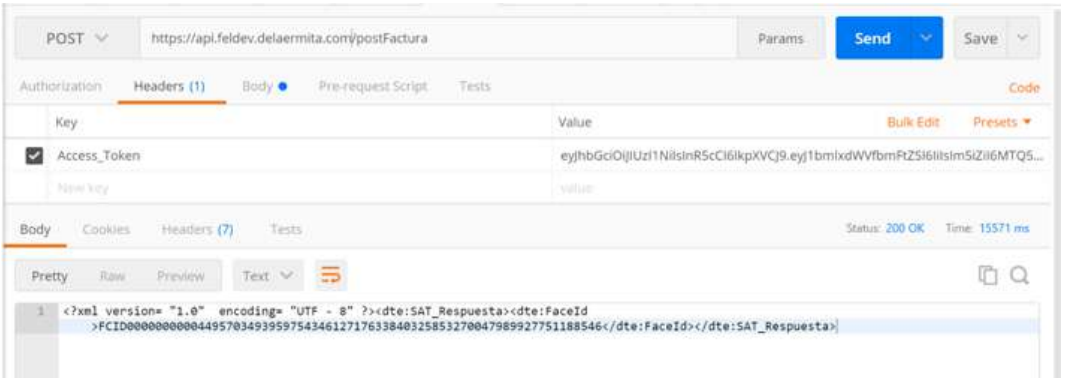

Ilustración 9 Acuse de recibo de SAT

[6] En una siguiente versión este mensaje de acuse de recibo incorporará una firma electrónica simple.

IV. Servicio de Anulación de DTE

A. Descripción

La anulación de DTE es una operación que el EMISOR puede, de acuerdo con las normativas y procedimientos, realizar ante el CERTIFICADOR del documento a anular para garantizar la integridad en los DTE y las anotaciones correspondientes.
Cada certificador es responsable de poner a disposición de sus EMISORES una aplicación o servicio para este efecto, la cual deberá cumplir las reglas y validaciones correspondientes.
La anulación se realiza por una operación externa al DTE y no modificará en ningún caso un DTE ya certificado, únicamente consiste en una anotación lógica vinculada al DTE que sea anulado.
La anulación del DTE debe ser informada de forma inmediata a la SAT por medio de la API de anulación que la SAT pondrá a disposición de los CERTIFICADORES.

B. Esquema de la operación de anulación

La operación de anulación se realiza por medio de una operación que debe ser firmada por el EMISOR que requiere la anulación y también debe ser firmada por el CERTIFICADOR para su validez.
El esquema de la operación de anulación, también definido por medio de un XSD, se encuentra publicado en conjunto con los demás esquemas, en la dirección siguiente:

- https://cat.desa.sat.gob.gt/xsd/alfa/GT_AnulacionDocumento-0.1.0.xsd

C. Incorporación de firma electrónica de emisión

En el nodo Signature, el EMISOR incorporará un nodo conteniendo la firma de emisión. Esta firma se realiza sobre el elemento DatosGenerales.

La firma electrónica de emisión es incorporada por el EMISOR de acuerdo con los lineamientos técnicos descritos. Para la firma el EMISOR debe emplear el certificado digital que la SAT le entregará por medio de los mecanismos que para tal efecto de establezcan.

El certificado digital que SAT otorgue es de uso exclusivo del emisor, para tal efecto deberá implementar mecanismos de seguridad bajo su exclusiva responsabilidad, la firma electrónica de emisión se aplica sobre el nodo de DatosGenerales.

El CERTIFICADOR y la SAT deben validarla siempre que reciban DTE y están obligados a rechazar cualquier DTE que no cumpla con la firma.

D. API de Anulación

Se habilitó un servicio de recepción en un ambiente con controles de autenticación. La disponibilidad del servicio es regular en horario laboral[7], en horario fuera de oficina el servicio puede ser interrumpido con previo aviso. Para verificar acceso básico al ambiente puede abrir en un navegador el URL siguiente: https://api.desa.sat.gob.gt/test. En conexión exitosa la página devolverá un "OK".

E. Autenticación del API

El servicio de recepción de información está basado en una autenticación, dicha autenticación se le denomina "Autenticación Básica" y se realiza por medio de un usuario y clave, para lo cual se devolverá un Token[8] de acceso con tiempo de expiración de acuerdo con los pasos descritos a continuación.

- El usuario y clave de pruebas deberá ser solicitado a SAT para que pueda ser dado de alta en el ambiente correspondiente.
- Se solicita la autenticación a través de la invocación del servicio, enviando el usuario y clave proporcionado por SAT, utilizando la configuración de envío de servicio REST con autenticación.
- El servicio se encuentra en la dirección siguiente: https://api.desa.sat.gob.gt/getToken

[7] Horario de atención para ambiente de desarrollo: 7:00a 16:00 horas, lunes a viernes.
[8] Es una cadena de caracteres que tiene un significado coherente en cierto lenguaje de programación, los cuales son identificadores con palabras claves.

Como ejemplo, para realizar una prueba se puede hacer uso de la herramienta PostMan (https://chrome.google.com/webstore/detail/postman/).

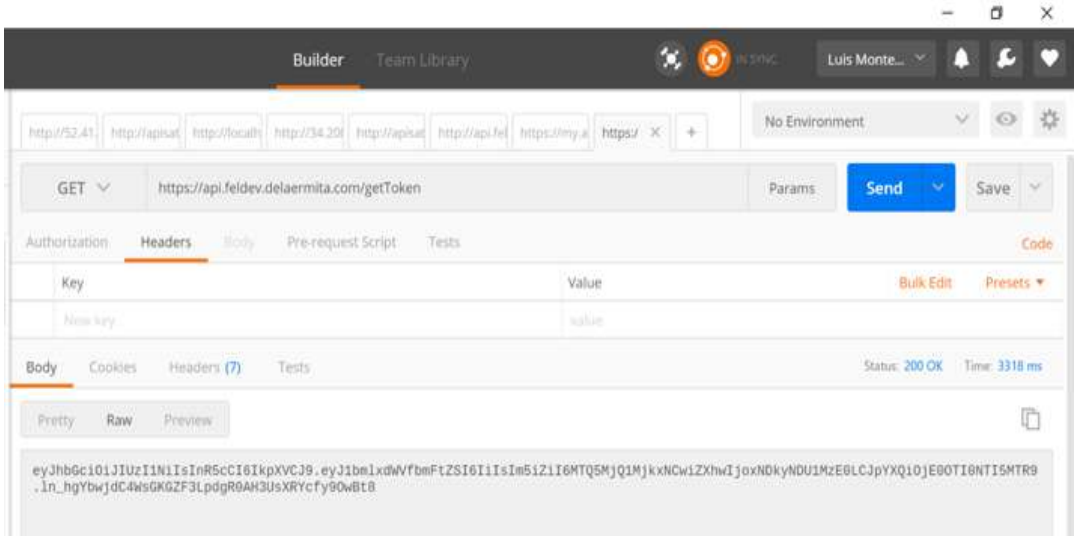

Ilustración 10 Proceso de Generación de Token

El método que invoca vía GET, necesita que se le envié una autenticación, la cual requiere un usuario y password que se le proporcionado a las personas que se encuentren en el proceso de autorización como certificador, este método le devuelve un token el cual tiene un tiempo de vida (60 minutos), al vencer el token se debe de volver a generar uno nuevo.

F. Envío de una Anulación al API

El API de recepción de DTE se encuentra publicado en la dirección siguiente:

- https://api.desa.sat.gob.gt /postAnulacionDTE

Se envía la información a través de un método POST el cual viene conformado de la siguiente forma, en el Header se debe de incluir el token proporcionado en el paso anterior el cual debe definirse con el nombre de "Access _Token" para que la transacción pueda ser autorizada, y en el body el XML generado con la información de la anulación de la factura previamente enviada.

Se debe de incluir dentro del header una llave la cual tiene como valor el token devuelto en el método GET, se debe de garantizar que el nombre de la llave sea el indicado tomando en cuenta la sensibilidad al contexto para que pueda ser validado por el método de recepción, esto quedaría de la siguiente forma:

Ilustración 11 Header con la Llave Access_Token

Dentro del Body del mensaje debe de colocar el XML generado con la información de la factura emitida.

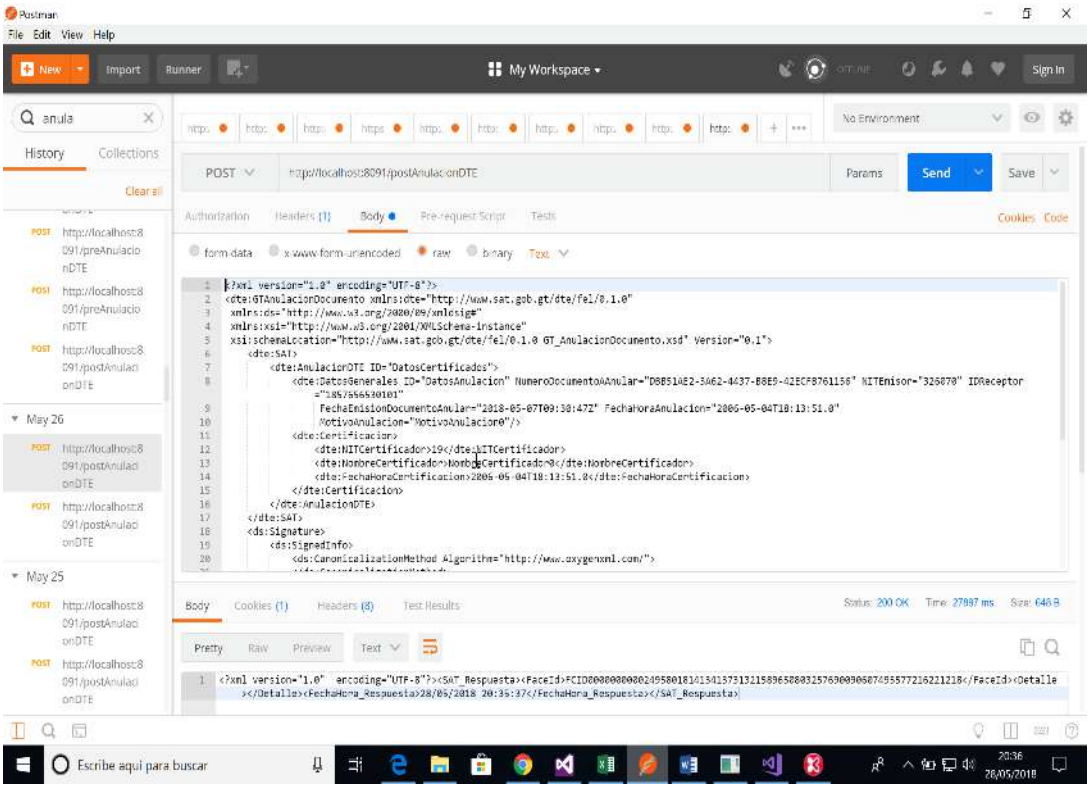

Ilustración 12 Anulación incorporada en el POST

Luego de enviar el DTE por medio del método POST, el API de SAT devolverá un mensaje con un código de éxito si todo salió correctamente o fallo si no paso las validaciones; dichos códigos se encuentran detallados en el catálogo de Errores, para que puedan ser interpretados de mejor manera.

Si el mensaje es exitoso, se devolverá un acuse de recibo el cual le garantiza que el mensaje fue registrado dentro del sistema de SAT, esto sirve para evidenciar que las transacciones están en el lugar, el mensaje seria de la forma[9] siguiente:

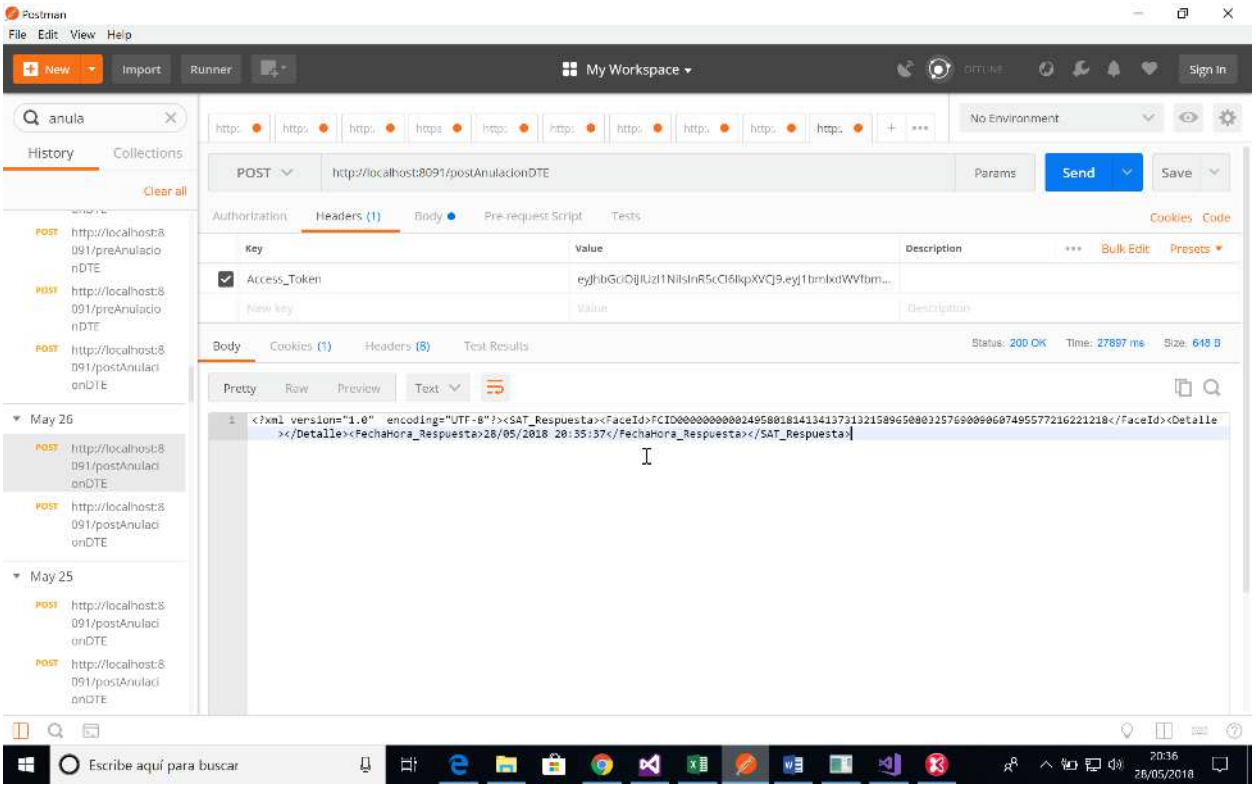

Ilustración 13 Acuse de recibo de SAT

[9] En una siguiente versión este mensaje de acuse de recibo incorporará una firma electrónica simple.

V. Modelo de publicación/suscripción de catálogos

A. Catálogo base (mini-RTU)

La SAT comparte con los Certificadores la información necesaria para que éstos puedan realizar los procesos informáticos propios del Régimen de Factura Electrónica en Línea, siendo la siguiente:

1. Datos del Registro Tributario Unificado de los Emisores de DTE habilitados:
    - Nombre del EMISOR (o razón o denominación social)
    - Nodo ESTABLECIMIENTOS
        - Número de establecimiento
        - Nombre del establecimiento (nombre comercial)
        - Dirección del establecimiento (dirección comercial)
            - Calle o Avenida
            - Letra de la dirección
            - Número de Casa
            - Apartamento
            - Zona
            - Colonia
            - Descripción del Municipio
            - Descripción del Departamento
        - Estatus (activo o no activo)
    - Nodo AFILIACIONES
        - Impuesto
        - Régimen
    - Nodo MARCAS
        - Código
        - Fecha
        - Valor

2. Datos generales de los contribuyentes. La SAT pondrá a disposición de los Certificadores la información de NIT, nombre o razón social y CUI cuando corresponda, de todos los contribuyentes registrados.

Durante la primera etapa del desarrollo por parte de certificadores y el proceso de autorización, este catálogo se publica a través del foro de desarrollo disponible para las personas interesadas en ser certificadores que la Intendencia de Recaudación tenga registrados.

En una segunda etapa, posterior a que el API de recepción se haya probado satisfactoriamente, se estarán proporcionando las credenciales y los repositorios que contendrán toda la información

B. Esquema de funcionamiento

El modelo de publicación/suscripción de catálogos se describe en la ilustración siguiente:

Ilustración 14 Modelo de publicación/suscripción

C. Suscripción

Los suscriptores deberán cumplir todos los requisitos que son solicitados en el procedimiento de autorización del certificador, si cumple con todos los requisitos se solicitara información que será registrada en un módulo interno de la SAT, para ellos deberán proporcionar la información de sus servicios restfull a los cuales les enviara la información de los deltas de cambios para la información (mini-rtu) que se compartirá, una vez quede registrado quedara suscrito al modelo.

D. API de recepción de notificaciones

Para el Api de recepción de información de los deltas de los contribuyentes que estén suscritos con cada uno de los certificadores, el certificador debe de contar con un Uri (identificador uniforme de recursos, sirve para identificar recursos web) que debe de proporcionar a la Superintendencia de Administración Tributaria, al momento de darse de alta esto permitirá realizar los envíos de información de cambios de los contribuyentes, este proceso se realiza por parte de SAT en base a la dirección proporcionada, en su defecto si no cuenta con un servicio se debe de registrar un correo electrónico donde estará llegándole la información de los delta de cambios en un formato especifico.

E. Estructura JSON

JSON (JavaScript Object Notation - Notación de Objetos de JavaScript) es un formato ligero de intercambio de datos. La estructura del archivo que contiene la información del Mini-Rtu se define en el ejemplo que se presenta, esta información es la que se estará enviando en cada uno de los deltas, para la carga inicial de pruebas se publicó en el foro dicho documento con la información, al momento de que el certificador pase todo el proceso de certificación se estarán proporcionando las credenciales y repositorio donde estará ubicada la información de producción.


```
{
   "Cabecera": {
   "minirtu": [
                {"Nit":"800000000011"
                ,"afiliacionIVA":"PEQ","marcas":[],"establecimientos":[{"zona":"8","estado":"A","nu
                mero":4,"municipio":"Mixco","numeroCasa":"12-
                85","apto":null,"departamento":"GUATEMALA","letra":null,"nombre":"EL
                AGAVE","calleAvenida":"3A. CALLE","colonia":"LOCAL 9 CIUDAD SAN
                CRISTOBAL"}],"nombre":" Juan Pequeno Perez
                800000000011","frases":[{"escenario":1,"tipo":3,"fechaResolucion":null,"numeroR
                esolucion":null}]},
                .
                .
                .
                .
                ]
 }
```

VI. Anexo A: Catálogos Publicados

Para la adecuada comprensión de los catálogos utilizados para el uso de Factura Electrónica en Línea, estos se encuentran publicados en el siguiente url:

https://cat.desa.sat.gob.gt/catalogos/alfa

Dentro de este url se encuentra dividido en dos secciones en las cuales encontraremos lo siguiente:

Dentro de la carpeta de catálogos encontramos la información de los catálogos que se publican y que se mencionan en apartados anteriores, este tiene los siguientes archivos.

1. **Catálogo de Frases** → Contiene la información de las frases que pueden ser utilizadas en cada escenario definido en el documento de Reglas y Validaciones.

2. **Catálogo de Unidades Gravables** → Contiene la información de las unidades gravables que se utilizan en cada escenario definido en el documento de Reglas y Validaciones.

3. **Catálogo de Mensajes** → Contiene la información de los errores tanto de rechazo, como informativos y secundarios que pueden generarse cuando se está emitiendo un DTE, estos mensajes están descritos en cada una de las validaciones que están contenidas dentro del documento de Reglas y Validaciones. Adicional a esto se tienen mensajes definidos para autenticación, anulaciones, éxito y errores genéricos definidos.