GUÍA PARA EL USO DEL SERVICIO DE VALIDACIÓN DE CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA (e.Firma)

Mayo, 2017

Administración General de Comunicaciones y Tecnologías de la Información
Administración Central de Seguridad, Monitoreo y Control
Administración de Manejo de Identidades y FEA

CONTENIDO

I. INTRODUCCIÓN 3
II. ALCANCE 7
III. OBJETIVO 7
IV. GLOSARIO DE TÉRMINOS Y ACRÓNIMOS 8
V. EL PROCESO DE FIRMADO ELECTRÓNICO 9
VI. EJEMPLO DE PROCESO DE FIRMADO 11
VII. VALIDACIÓN DEL ESTADO DEL CERTIFICADO (OCSP) 12
VIII. LENGUAJES DE PROGRAMACIÓN A UTILIZAR 14
IX. PREGUNTAS FRECUENTES 15
X. ANEXO I – AMBIENTE DE PRUEBAS 19
XI. ANEXO II – CERTIFICADOS DIGITALES 24

I. INTRODUCCIÓN

La Estrategia Digital Nacional establece como objetivo I, la transformación gubernamental y dentro de sus líneas de acción, la utilización de la Firma Electrónica Avanzada (e.Firma) como medio de autenticación para trámites y servicios, esta medida provoca en el corto plazo que gran cantidad de Entidades Externas al SAT o Terceros como son Entidades Federativas, Entidades Gubernamentales de los tres niveles de Gobierno e Instituciones Privadas requieran utilizar el certificado de Firma Electrónica Avanzada, emitido por el Servicio de Administración Tributaria, en sus procesos institucionales, para dar cabal cumplimiento a la línea de acción mencionada.

La e.Firma es un conjunto de datos que se incluyen a un mensaje electrónico, cuyo propósito es identificar al emisor del mensaje como autor legítimo de éste, tal y como si se tratara de una firma autógrafa, pero permite hacerlo en medios electrónicos con seguridad técnica y jurídica.

	Firma Autógrafa	Firma Electrónica	Firma Electrónica Avanzada
Identificación	✓	✓	✓
Autenticación	✓	✓	✓
Confidencialidad		✓	✓
Integridad			✓
No repudio			✓

Como ya se ha mencionado su diseño se basa en estándares internacionales de infraestructura de claves públicas o "Public Key Infraestructure" (PKI por sus siglas en inglés) en donde se utilizan dos claves o llaves para el envío de mensajes:

1. La "llave o clave privada" que únicamente es conocida por el titular de la e.Firma, que sirve para cifrar datos; y
2. La "llave o clave pública", disponible en Internet para consulta de todos los usuarios de servicios electrónicos, con la que se descifran datos.

Asimismo la e.Firma es un habilitador de Interoperabilidad de los documentos de identificación con el objetivo de hacer más eficientes los procesos de gestión al interior de la administración pública.

Dos de los escenarios más comunes donde se utiliza la e.Firma son los siguientes:

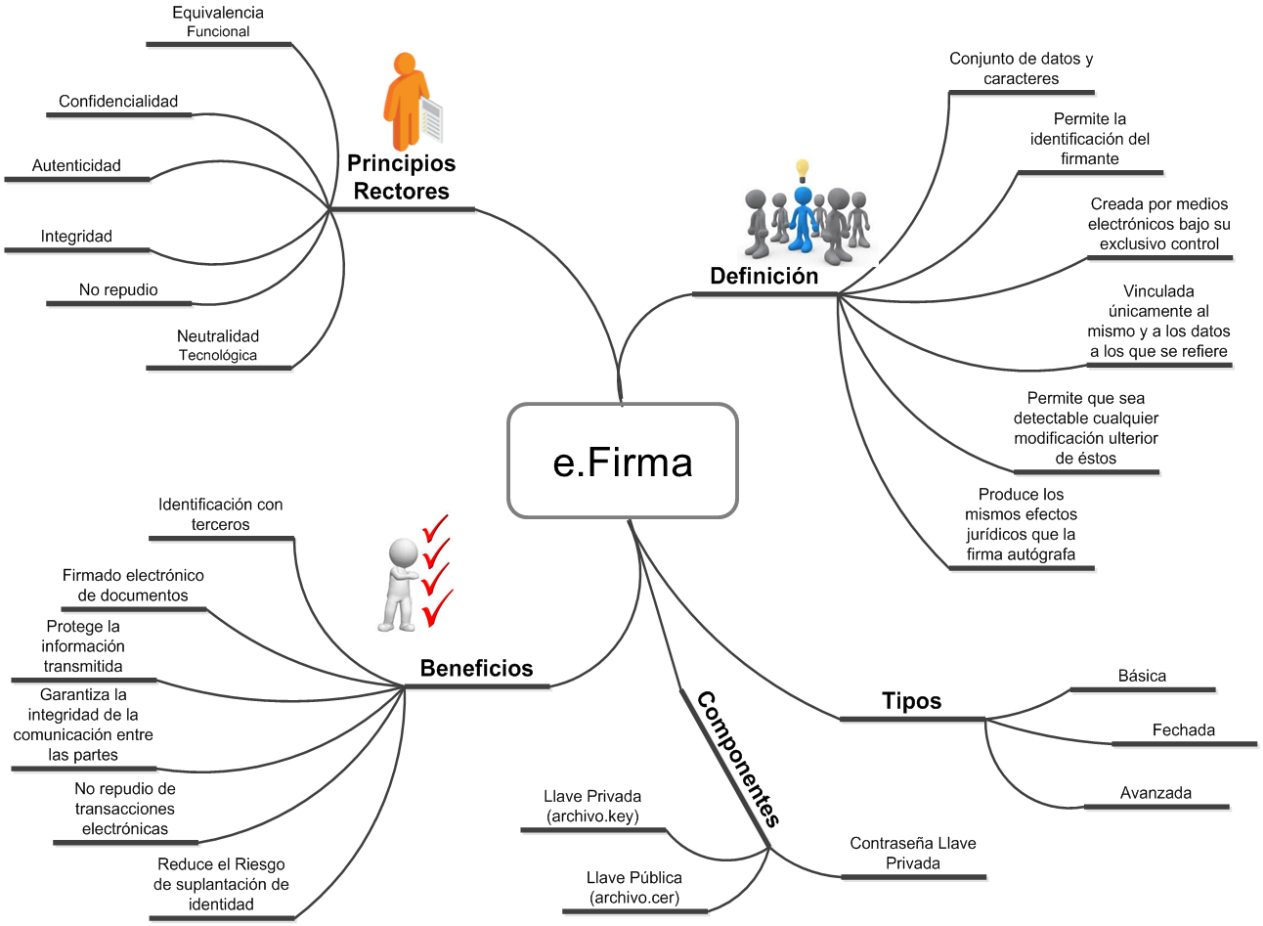
(i) En los procesos de autenticación, como por ejemplo los utilizados en algunos de los sistemas de declaraciones y pagos del SAT,

(ii) En los procesos de firmado electrónico de documentos, como por ejemplo el caso de la Oficina Postal Electrónica (OPE) o bien en el proceso de firmado electrónico de la Declaración anual de impuestos que realizan los contribuyentes ante el SAT, así como la Declaración anual de modificación patrimonial que los servidores públicos deben realizar año con año.

Asimismo los juicios en línea del Tribunal Federal de Justicia Fiscal y Administrativa utilizan la e.Firma para firma electrónica de documentos.

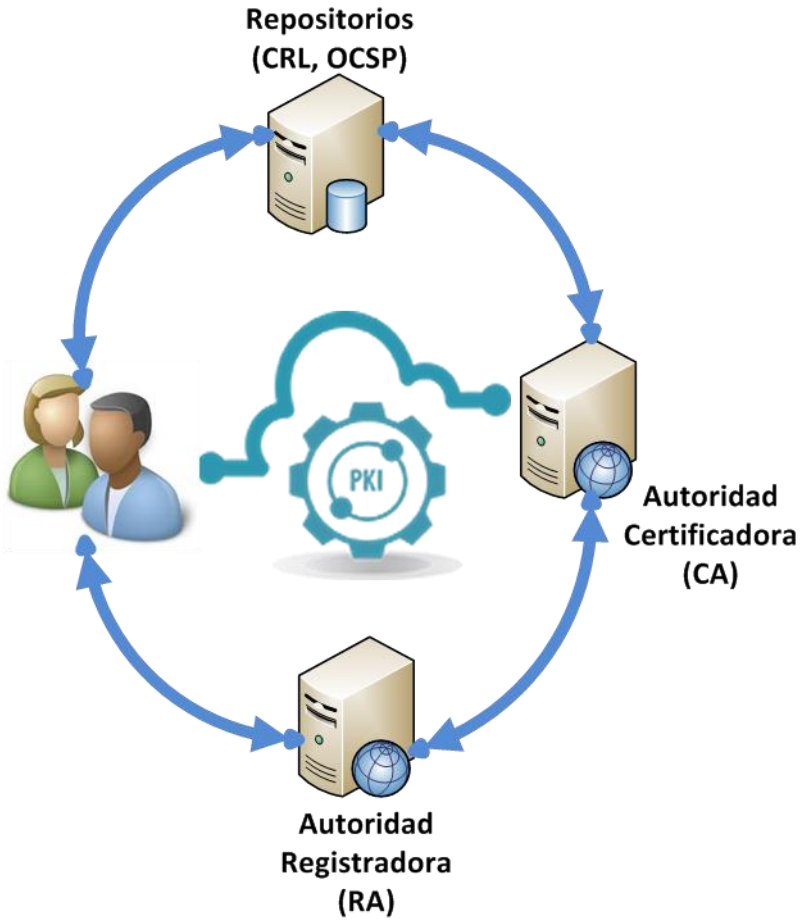
Es decir, en los servicios donde se pretende endurecer los mecanismos de control de acceso y brindar un nivel de seguridad mayor en las transacciones realizadas que requieran ser autenticadas y firmadas.

El siguiente mapa mental resume la e.Firma:



Con la finalidad de facilitar el uso y adopción de la e.Firma se ha diseñado el presente documento para garantizar, que los sistemas de dichas organizaciones estén preparados para hacer uso del servicio de "On-Line Certificate Status Protocol" (OCSP por sus siglas en Inglés) ofrecido por el SAT para validación de los certificados de Firma Electrónica Avanzada (e.Firma) emitida por el SAT.

La e.Firma está basada en PKI, Infraestructura de clave pública.



La Infraestructura de Clave Pública (Public Key Infraestructure o PKI por sus siglas en inglés) está compuesta principalmente por una Autoridad Certificadora (AC), una Autoridad Registradora (AR) y se complementa con las combinaciones de hardware y software, tecnologías criptográficas, servicios, políticas y procedimientos orientadas a la gestión, emisión, generación y validación de certificados digitales.

En los servicios de PKI del SAT se incluyen:

- Identificación de los solicitantes de certificados digitales
- Gestión de certificados digitales

- Generación de certificados digitales
- Emisión de certificados digitales
- Validación de certificados digitales

II. ALCANCE

El presente documento es una guía para todas las Entidades Externas o Terceros ajenos a la infraestructura del SAT que necesitan validar que el certificado de e.Firma con el que dichas Entidades Externas o Terceros, están tratando de autenticar la identificación de una persona, es decir, que realmente fue emitido por el SAT y no ha sido revocado.

III. OBJETIVO

Identificar y/o describir el conjunto de actividades que una Entidad Externa o Tercero deberá seguir para lograr la validación de los certificados de Firma Electrónica Avanzada del SAT así como las recomendaciones básicas que deberán atender en el proceso de validación de los certificados.

Asegurar mediante la integración de los servicios de OCSP del SAT y los sistemas desarrollados por las Entidades Externas o Terceros que los usuarios de dichos sistemas sean identificados, autenticados y autorizados de manera segura, garantizando también la autenticidad y el "No repudio" sobre las transacciones realizadas en los sistemas mencionados.

Es importante acotar que el desarrollo de los aplicativos para firmado electrónico y/o autenticación deben de ser desarrollados e implementados por cada Entidad Externa o Tercero, preferentemente alineados a las estrategias e infraestructura tecnológica con la que cuentan.

IV. GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

TÉRMINOS	SIGNIFICADO
Autenticación	Proceso mediante el cual el usuario de un sistema informático es identificado como válido al momento de proporcionar sus credenciales para acceder a dicho sistema de información.
Autoridad Certificadora (AC)	En criptografía una autoridad de certificación, certificadora o certificante es una entidad de confianza, responsable de emitir y revocar los certificados digitales, utilizados en la Firma Electrónica. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.
Autorización	Proceso mediante el cual un aplicativo certifica que la identidad que hace uso del mismo tenga el conjunto de permisos requeridos para acceder o ejecutar una función.
Clave Pública y Clave Privada	El certificado de e.Firma emitido por el SAT consta de dos elementos basados en un modelo de criptografía asimétrica. Esos elementos son una clave pública que puede ser conocida por otras personas distintas al dueño del certificado y una clave privada asociada a la clave pública y que solo debe ser conocida por el dueño del certificado.
Directorio	Repositorio Jerárquico de información en el cual se encuentran concentradas las identidades autorizadas por parte del SAT para hacer uso de los servicios de información.
e.Firma (antes FIEL)	Firma Electrónica Avanzada es un certificado Digital emitido por el Servicio de Administración Tributaria.
Identidad	Cualquier persona o usuario que requiere poseer una cuenta para hacer uso de los servicios de información.
IETF	“The Internet Engineering Task Force” (por sus siglas en inglés) es una organización internacional abierta de estandarización, que tiene como objetivos el contribuir a que la Internet funcione mejor, actuando en diversas áreas, como transporte, encaminamiento, seguridad, etc.
OCSP	“Online Certificate Status Protocol” por sus siglas en inglés, es un método (protocolo) para conocer el estado de los certificados de e.Firma, la finalidad es conocer si ha sido revocado o aún continúa siendo válido.
PKCS	En el tema de la criptografía, el acrónimo PKCS (“Public-Key Cryptography Standards” por sus siglas en inglés) se refiere a un grupo de estándares de criptografía de clave pública concebidos entre otras cosas para intercambio de claves, sintaxis de mensajes, sintaxis de la información de las claves y que son publicados por los laboratorios de RSA en California, USA.

V. EL PROCESO DE FIRMADO ELECTRÓNICO

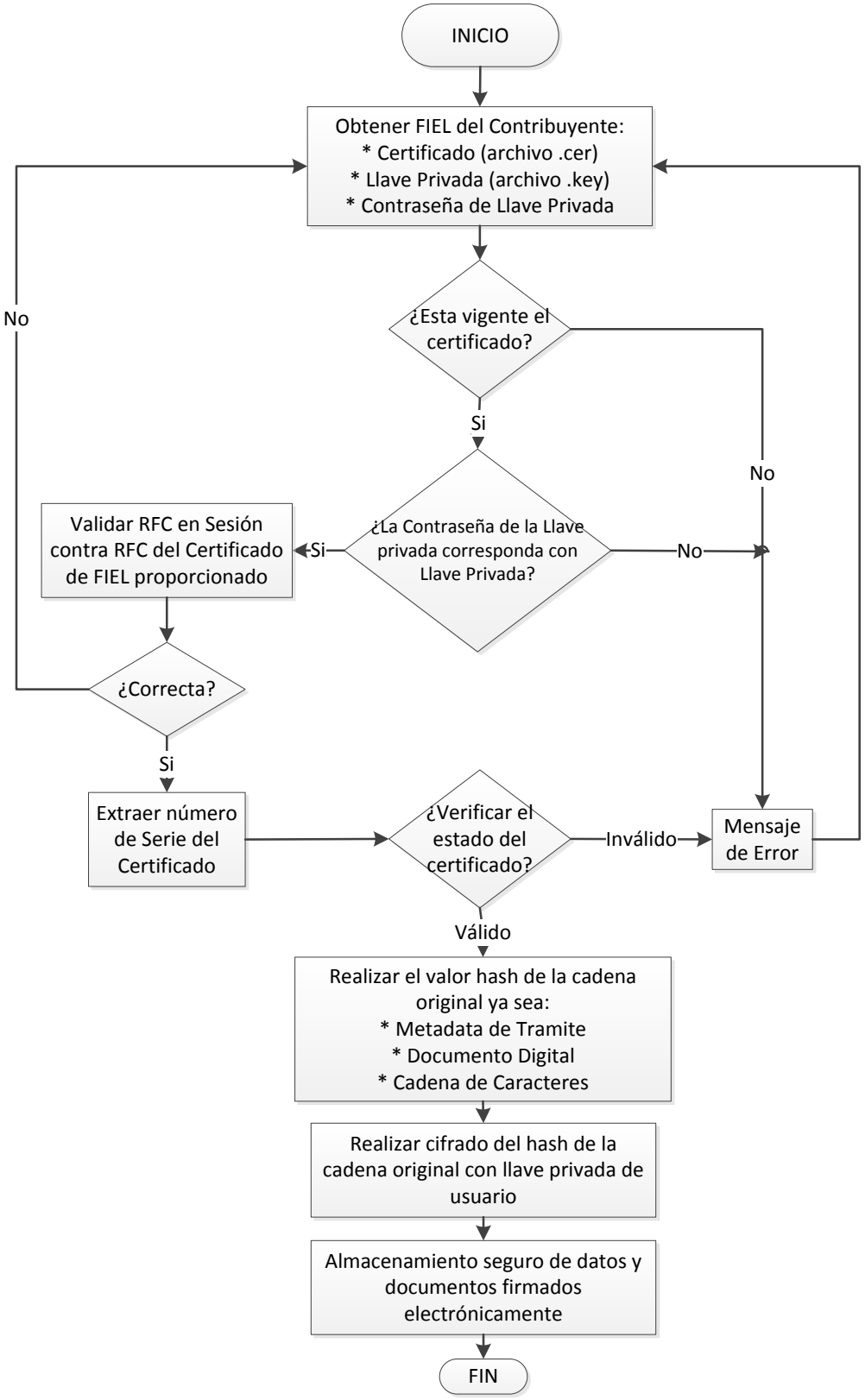
En base a diferentes experiencias de distintas Entidades Externas o Terceros que consumen el servicio de validación de certificados digitales del SAT, se han establecido los lineamientos siguientes:

1. Para la firma de un documento o cadena digital es conveniente realizar las siguientes validaciones antes de proceder al firmado electrónico:
    a. Los documentos generados por los sistemas que operan transacciones que requieren garantizar la autenticidad, integridad, confidencialidad y no-repudio deben contener al menos los siguientes elementos que lo hagan único:
        i. Nombre de a quién se emite el documento.
        ii. Identificador de a quién se emite el documento (ej. RFC o CURP).
        iii. Estampado de tiempo (Fecha y hora) de emisión del documento.
        iv. Número de folio único por documento.
        v. Datos particulares del trámite o servicio por el cual se emite el documento con firma electrónica.
        vi. Datos de quien emite el documento, como por ejemplo: nombre, puesto, número de empleado, etc.
        vii. Datos de la dependencia firmante (en su caso): nombre, clave de dependencia, etc.
        viii. Número de serie del certificado correspondiente al firmante.
        ix. Fechas de vigencia del certificado con el que se está firmando.
2. Se deberán realizar localmente (en el equipo del usuario) las siguientes validaciones antes de utilizar la clave privada del firmante para aplicarla al documento:
    a. Que la ejecución de la firma ocurra en la computadora local del usuario que firmará el documento.
    b. Que el programa de firmado solicite para la firma el certificado (archivo.cer), la clave privada del certificado (archivo.key) y la frase de seguridad para abrir la clave privada. Por ejemplo, algunos aplicativos en el portal del SAT lo hacen de esta manera.
    c. En los campos donde solicitan los datos del certificado no se debiera permitir la edición del campo que contiene el RFC. El valor de dicho campo debe ser obtenido del certificado.
    d. Abrir la clave privada con la contraseña proporcionada.
    e. Verificar que el certificado este vigente.
    f. Verificar la clave privada con la contraseña proporcionada.
    g. Verificar la correspondencia entre el certificado y la clave privada asociada al certificado.

3. Hacer las validaciones propias del sistema de la Entidad o Tercero, de acuerdo a sus propias reglas de negocio definidas o las adicionales que se consideren pertinentes.
4. Verificar el estado del certificado, utilizando el servicio OCSP. (Ver sección VII de este documento)

   Una vez realizadas las validaciones mencionadas, la siguiente acción es el firmado electrónico con la e.Firma del documento generado por la transacción del sistema.
5. El aplicativo que pretende hacer uso del sistema OCSP debe considerar la validación del algoritmo de cifrado que incluya SHA1 y SHA2 para los certificados y una longitud de 1024 y 2048 bits para sus claves.
6. Adicional al sistema de firmado se debe de considerar la construcción de otro componente que permita la subsecuente verificación del documento firmado, con el objetivo de comprobar su validez, en cualquier punto del tiempo. Por ello también es recomendado, que a todo documento firmado, agregarle el certificado del firmante, esto es posible utilizando el estándar PKCS7 (Estándar de la sintaxis para mensajes criptográficos).
7. El almacenamiento de los documentos firmados digitalmente y su resguardo seguro, también se vuelven parte esencial de todo el proceso de documentos donde existe el uso de firmas digitales, ya que probablemente se espera que dichos documentos y su firma tengan una validez en el futuro, donde surgirán nuevos retos sobre temas de criptografía y la potencial violación a esquemas criptográficos digitales.
8. Previo a la utilización del sistema desarrollado por la Entidad Externa o Tercero, los usuarios deberán de contar con el certificado digital de e.Firma emitido por el SAT.

VI. EJEMPLO DE PROCESO DE FIRMADO



VII. VALIDACIÓN DEL ESTADO DEL CERTIFICADO (OCSP)

El Servicio de Administración Tributaria ofrece a las Entidades Externas o Terceros un servicio en línea para validación de estatus de certificados de Firma Electrónica Avanzada. Este servicio como ya hemos mencionado es conocido como OCSP y su objetivo es ofrecer el estatus que guardan los certificados digitales de firma electrónica avanzada emitidos por el SAT.

Los lineamientos generales para la utilización del servicio OCSP son los siguientes:

1. La Entidad Externa o Tercero, deberá celebrar un convenio de colaboración administrativa con el Servicio de Administración Tributaria cuyo envío se realizará a petición de los interesados.
2. La Entidad Externa decide la tecnología a utilizar para el desarrollo tanto de su sistema o aplicación como las peticiones o llamados para el consumo del servicio OCSP.
3. La petición al servicio OCSP deberá construirse de acuerdo al estándar publicado por la IETF (Internet Engineering Task Force) en http://www.ietf.org/rfc/rfc6960.txt
4. El Protocolo de estado de certificados en línea (OCSP) del SAT solo permite que las aplicaciones puedan determinar el estado de un certificado digital de e.Firma emitido por el SAT, para satisfacer algunos de los requisitos operativos de proporcionar información de revocación y/o vigencia más oportuna.
5. El cliente de OCSP desarrollado por las Entidades Externas o Terceros, envía una solicitud de estado de certificado de e.Firma al servicio OCSP del SAT y suspende la aceptación del certificado de e.Firma hasta que la respuesta sea recibida de parte del SAT.
6. El servicio responderá de manera general a la petición de validación del certificado, con los siguientes valores:
    i. Estatus correcto, que indica que el certificado de e.Firma tiene un estatus válido y puede ser aceptado.
    ii. Estatus incorrecto, que indica que el certificado de e.Firma tiene un estatus que no debiera permitir ser aceptado.
    iii. Estatus desconocido, que indica que el certificado posiblemente no fue emitido por el SAT.

    Para interpretar detalladamente la respuesta del servicio OCSP del SAT deberá de consultar el estándar publicado por la IETF en http://www.ietf.org/rfc/rfc6960.txt
7. Cada Entidad Externa o Tercero deberá definir sus propias reglas de negocio que definan la aceptación o rechazo de un certificado digital de FIEL con que se pretenda realizar el firmado electrónico de documentos.
8. Antes de aceptar un certificado para el firmado electrónico, el aplicativo debe comprobar si el certificado procede de una fuente confiable y que existe una

asociación válida entre el nombre del subscriptor y su clave pública. Este proceso de comprobación se llama validación de ruta. La validación de ruta implica el procesamiento de certificados emisores de clave pública, donde el emisor certifica de forma jerárquica hasta que la ruta de certificación termina en un certificado autofirmado de confianza. Normalmente, se trata de un certificado de AC raíz. En el caso del SAT, la Autoridad Registradora Certificadora raíz (ARC) es Banco de México. En un nivel siguiente encontramos la Autoridad Certificadora (AC) del SAT. Finalmente se debe comprobar el certificado del OCSP. Si hay un problema con uno de los certificados de la ruta o si no se encuentra un certificado, se considera que la ruta de certificación no es de confianza.

IMPORTANTE: Si no se hace correctamente la validación de la ruta de certificación, existe el riesgo de que un certificado apócrifo no emitido por la AC del SAT sea utilizado.

9. Las liga en la cual el Servicio de Administración Tributaria expone los servicios del OCSP para fines de pruebas y desarrollo es:

   https://cfdit.sat.gob.mx/edofiel

10. Para la realización de pruebas del servicio de OCSP, deberá de solicitar a la Administración Central de Seguridad, Monitoreo y Control adscrita a la Administración General de Comunicaciones y Tecnologías de la Información del SAT, un conjunto de certificados de pruebas. Esto debido a que el servicio de OCSP NO PRODUCTIVO no reconoce los certificados del ambiente de producción. Para validar la ruta de certificación se deben usar los certificados de pruebas anexos al presente documento.

11. Para conocer detalladamente las estructuras de las peticiones y de las respuestas del servicio OCSP, deberá consultar el estándar publicado por la Internet Engineering Task Force en el sitio http://www.ietf.org/rfc/rfc6960.txt

12. Para cualquier duda o requerimiento de información adicional, los contactos definidos por el Servicio de Administración Tributaria son los siguientes:

    - Enrique Francisco Arochi Alfaro (enrique.arochi@sat.gob.mx)
    - Israel Becerril Sierra (Israel.becerril@sat.gob.mx)
    - Javier Mendieta González (javier.mendieta@sat.gob.mx)

VIII. LENGUAJES DE PROGRAMACIÓN A UTILIZAR

Las Entidades Externas o Terceros que consumirán el servicio de OCSP del SAT, deberán definir las tecnologías de información así como los lenguajes de programación y/o librerías criptográficas que más se adecuen a sus propias estrategias tecnológicas y capital humano con el que cuenten para el desarrollo del módulo de peticiones al servicio de OCSP.

Usualmente para evitar dependencias de fabricantes o marcas específicas, se han utilizado lenguajes estándar de programación como Java o .NET, así como librerías criptográficas de código abierto ("Open Source").

La decisión para definir qué librerías criptográficas utilizar, depende del lenguaje de programación definido para el desarrollo del sistema de la Entidad Externa, por ejemplo:

- Si el lenguaje de desarrollo seleccionado es .NET (Lenguaje C) la librería criptográfica seleccionada podría ser "openssl", ya que está desarrollada en dicho lenguaje. Esta librería criptográfica puede ser consultada en http://www.openssl.org/.

  La librería criptográfica "Openssl" es más completa, tiene más funciones, pero es más pesada. Adicionalmente cuenta con una función de verificación del estado del certificado con OCSP, la cual puede ser utilizada para la verificación con el servicio correspondiente del SAT.

  En el Anexo I, se incluye un pequeño laboratorio que utiliza un cliente de OCSP para demostrar cómo se puede consumir el servicio de OCSP, esto solamente con fines demostrativos.

- Si por el contrario, el lenguaje de desarrollo seleccionado es JAVA, la librería criptográfica definida podría ser "bouncy castle", ya que está desarrollada en el mismo lenguaje de programación. Esta librería criptográfica puede ser consultada en http://www.bouncycastle.org/ y proporciona ejemplos de utilización y códigos fuente

  "Bouncy castle" y es más ligera que "OpenSSL".

Al final, la decisión de cual lenguaje de programación y cual librería criptográfica utilizar, es totalmente decisión de la Entidad Externa o Tercero que consumirá el servicio de validación de estado de certificados de FIEL, y que los mencionados previamente en éste apartado no son los únicos, es decir, existen otros lenguajes y/o librerías criptográficas que también podrían permitir el consumo del servicio del OCSP del SAT.

No se debe de olvidar que el objetivo al consumir el servicio de OCSP del SAT es la validación del certificado digital de e.Firma, NO es utilizar los mismos lenguajes de programación y librerías criptográficas que usa el SAT.

IX. PREGUNTAS FRECUENTES

¿Qué no es una Firma Electrónica?

Las firmas digitalizadas o escaneadas

¿Para qué sirve la Firma Electrónica Avanzada?

Sirve para brindar seguridad a las operaciones electrónicas y la identificación del firmante ya que ha sido creada bajo su estricto control y garantiza la vinculación única con los datos al que se adjunta posibilitando la detección de cualquier alteración o modificación posterior a la emisión o firma del documento o mensaje evitando su repudio.

¿Qué garantiza la Firma Electrónica Avanzada?

Autenticidad: La información del documento y su firma electrónica se corresponden indubitablemente con la persona que ha firmado.

Integridad: La información contenida en texto electrónico, no ha sido modificada luego de su firma.

No repudio: La persona que ha firmado electrónicamente no puede decir que no lo ha hecho.

Confidencialidad: La información contenida ha sido cifrada y por voluntad del emisor, solo permite que el receptor pueda descifrarla.

¿Qué es el Certificado de Firma Electrónica?

Es un certificado firmado electrónicamente por la Autoridad de Certificación del SAT asegurando la vinculación con la identidad del usuario y que ha sido creado por medios electrónicos bajo su exclusivo control.

¿Qué contiene un Certificado Digital?

a) Identificación de la Autoridad de Certificación que lo emitió

b) Los datos del titular del certificado que permitan su identificación

c) Las fechas de emisión y expiración del certificado;

d) El número único de serie que identifica el certificado

e) Clave pública del certificado

f) La Clave Única de Registro de Población

g) Algoritmo de Firma del certificado

¿Existe riesgo de falsificación de la Firma Electrónica?

El riesgo es prácticamente nulo.

¿Alguien puede firmar información sin mi consentimiento?

No, los responsables del sistema de Firma Electrónica Avanzada, las Entidades y Dependencias no conservan las claves privadas ni las contraseñas que resguardan el uso de los certificados digitales para realizar el proceso de firma, además cada sistema cuenta con contraseñas de acceso propias mismas que restringen el acceso a los sistemas de firmado en línea.

¿Cómo puedo comprobar si la e.Firma es válida y está vigente?

Actualmente el SAT tiene el servicio llamado CERTISAT donde los contribuyentes pueden verificar el estado de su certificado de e.Firma. El sitio está en la página:

https://paic.plataforma.sat.gob.mx/nidp/idff/sso?id=FormGenCont&sid=0&option=credential&sid=0

¿Qué es el servicio de validación OCSP?

Es un servicio que ofrecen las Autoridades Certificadoras emisoras de certificados digitales para consultar el estado actual de sus certificados emitidos.

¿Qué estados puede tener un certificado digital?

Vigente, el certificado es válido y no ha sido revocado

Revocado, el certificado ha sido invalidado por el usuario o por la Autoridad Certificadora

Caducado, la vigencia del certificado ha expirado

¿La firma electrónica protege el contenido del documento digital?

Así es, cualquier cambio realizado a los datos del documento, incluso alterando una sola letra, invalidará la firma electrónica, después de cualquier cambio. El receptor del documento digital al validar la firma electrónica puede verificar que la firma es inválida.

¿Qué debo hacer si olvidé la contraseña de la clave privada o perdí la clave privada?

Desafortunadamente no hay forma de recuperar la contraseña de la clave privada. Tampoco es posible recuperar la clave privada (archivo.key). Si usted se encuentra en cualquiera de estos dos supuestos, deberá acudir a las oficinas del SAT para solicitar la revocación del certificado de e.Firma actual y solicitar la emisión de uno nuevo.

¿Cómo obtener el certificado digital de FIEL?

El ciudadano deberá acudir a cualquiera de las oficinas del SAT y:

1. Presentar original o copia certificada de una identificación oficial vigente.
2. Verificar si tu CURP está certificada en el Registro Nacional de Población; en caso contrario, debes presentar acta de nacimiento en original.
3. Original de comprobante de domicilio, no mayor a cuatro meses.

   En el caso de los asalariados y contribuyentes sin actividad económica será aceptada la credencial para votar expedida por el Instituto Nacional Electoral (antes Instituto Federal Electoral), para acreditar su domicilio, siempre y cuando este contenido en la misma.

   En caso de personas morales, el representante legal debe contar con e.Firma (activa) y presentar el poder general para actos de dominio o de administración, así como el acta constitutiva de la persona moral.
4. Para que tu visita sea más rápida solicita una cita.
5. Sugerencias para agilizar el trámite.
   a. Para que puedas obtener tu certificado de e.Firma más rápido opcionalmente podrás generar tus archivos de clave privada y requerimiento; es muy sencillo, para eso necesitas:
      i. Descargar el programa Certifica antes Solcedi (Solicitud de certificado digital) de e.Firma. En la liga: https://portalsat.plataforma.sat.gob.mx/solcedi/
      ii. Ejecutar el programa, y proporcionar tu RFC, CURP y una cuenta de correo electrónico.
      iii. Crear una contraseña de acceso.
      iv. Opcionalmente también podrá llenar e imprimir la Solicitud de certificado de Firma Electrónica Avanzada
   b. El programa genera dos archivos, la clave privada (key) y tu requerimiento (req)

6. Al concluir el trámite obtendrás el certificado digital de tu e.Firma (.cer) y tu solicitud sellada.
7. Es importante que resguardes tus archivos en un medio digital seguro, son exclusivamente tuyos. Si compartes esos documentos electrónicos, facilitarías a terceros que firmen documentos oficiales electrónicos a tu nombre.

Para información adicional sobre más preguntas frecuentes, puede consultarlas directamente en la siguiente dirección de internet:

http://www.sat.gob.mx/informacion_fiscal/preguntas_frecuentes/Paginas/firma_electronica_preguntas.aspx

X. ANEXO I – AMBIENTE DE PRUEBAS

El SAT pone a disposición un ambiente de pruebas en el que se pueda verificar el comportamiento del esquema implementado y puedan realizar consultas al OCSP.

A manera descriptiva, para probar que algún certificado X, haya sido emitido por el SAT, es necesario verificar que la firma del certificado emisor o padre, coincida con la que contiene el certificado X, el SAT les provee los certificados emisores o padres mediante los cuales se han emitido a lo largo del tiempo los certificados de los ciudadanos y personas morales, con la finalidad de que puedan realizar esta comprobación.

Por otra parte, para aceptar un certificado digital de un usuario en alguna aplicación de firmado electrónico o autenticación para acceso a aplicativos, además de verificar que este sea vigente, es necesario validar que no haya sido revocado, ya que si es el caso no debe de aceptarse este certificado para cualquiera que sea el trámite o uso.

El proceso de validación de estado se realiza a través del servicio de OCSP[1] (Online Certificate Status Protocol), este servicio verifica que los certificados emitidos por el SAT estén activos e informa en su respuesta el estado de estos, es decir si está activo o si ha sido revocado. En el servicio de OCSP del SAT sólo se pueden 'testar' certificados emitidos por el SAT, en caso de acceder a él para tratar de verificar algún certificado no emitido por el SAT, se obtendrá una respuesta de error. El servicio de OCSP es un protocolo, por lo que las peticiones al mismo deberán de cumplir con los requisitos establecidos para este protocolo.

Antes de aceptar un certificado para el firmado electrónico, el aplicativo debe comprobar si el certificado procede de una fuente confiable y que existe una asociación válida entre el nombre del subscriptor y su clave pública. Si no se hace correctamente la validación de la ruta de certificación, existe el riesgo de que un certificado apócrifo no emitido por la AC del SAT sea utilizado [2].

Para poder realizar pruebas del servicio, el SAT cuenta con un ambiente de pruebas al cual pueden acceder en la URL https://cfdit.sat.gob.mx/edofiel, requieren contar con el 'set' de certificados para la realización de pruebas y reconocer las respuesta y comportamiento del servicio, asimismo es conveniente mencionar que los certificados de pruebas, incluyen certificados a 1024 y 2048 con SHA1 y SHA2-256 de conformidad a lo siguiente:

- Certificados de prueba emitidos por el SAT para ambiente de pruebas, permiten realizar el firmado, archivos "1024-v2.zip y 2048.zip"
- Certificado de AC y OCSP de respuesta, para prueba en el SAT, archivo "ocsp_3_uat.zip"

Es importante contar con la IP de pruebas, de esta manera, en caso de presentar algún problema será más eficiente la atención y eventual resolución.

Otro aspecto de suma importancia, es contar con la volumetría estimada de los servicios, para lo cual se cuenta con un archivo en formato Excel, de esta manera el SAT puede proyectar la actualización y robustecimiento de la infraestructura de la PKI en la que se opera la FIEL. El único objetivo es garantizar que la infraestructura tenga la capacidad de respuesta para proporcionarles el mejor servicio posible.

1) *Para interpretar detalladamente la respuesta del servicio OCSP del SAT deberá de consultar el estándar publicado por la IETF en http://www.ietf.org/rfc/rfc6960.txt*
2) *Para revisar el tema de validación de ruta, se deberá consultar el estándar publicado por la IETF en http://www.ietf.org/rfc/rfc5280.txt en su capítulo 6 en particular.*

Como se ha mencionado en la "GUÍA PARA EL USO DEL SERVICIO DE VALIDACIÓN DE CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA (FIEL)", es posible utilizar OpenSSL para realizar consultas al OCSP, para los siguientes ejemplos, se utiliza un cliente de OpenSSL para Windows versión 1.0.1j.

Los certificados de AC, de OCSP y de prueba que se suministran, para estos ejemplos se encuentran en el subdirectorio C:/Test.

Para realizar una consulta al servicio del OCSP, es necesario que el certificado a probar se encuentre en formato PEM, los certificados de prueba que se distribuyen, por lo general se encuentran en formato .CER, por lo que será necesario hacer esta conversión.

La siguiente instrucción toma el archivo gava730717ae1.cer que previamente ha sido descomprimido en el directorio c:/Test y crea un archivo gava730717ae1.pem con la codificación PEM que se necesita para realizar la consulta.

```
OpenSSL>x509 -in c:/Test/gava730717ae1.cer -inform der -outform pem -out
c:/Test/gava730717ae1.pem
```

Para realizar la consulta del estado de este certificado se utiliza la siguiente instrucción:

```
OpenSSL> ocsp -issuer c:/Test/ac2_4096.crt -cert c:/Test/gava730717ae1.pem -
text -url https://cfdit.sat.gob.mx/edofiel -VAfile
c:/Test/OCSP_AC_4096_SHA256.crt -header host cfdit.sat.gob.mx

Response verify OK
gava730717ae1.pem: good
        This Update: Jul 20 21:55:32 2015 GMT
```

Donde:

- ocsp indica que se trata de una sentencia de OCSP
- -issuer es para indicarle que a continuación habrá un certificado de AC o raíz
- -url antecede a la dirección del sitio que alberga el servicio de OCSP
- -cert es para indicarle que a continuación habrá el certificado del cual se desea conocer su estado
- -VAfile indica que se verificara por el OCSP y se incluye el certificado de respuesta OCSP

Vale la pena mencionar que: Openssl resuelve el nombre del dominio a su dirección IP, se está recibiendo esta dirección IP desde un servidor Proxy e intenta acceder al directorio /edofiel. Por supuesto este directorio no lo encuentra y se emite el error 403 – Forbidden por parte del servidor proxy.

Para solucionar esta situación, es necesario enviar el parámetro –header dentro del comando OpenSSL. El encabezado a enviar es "HOST".

Por lo anterior es que añadimos –header host cfdit.sat.gob.mx

Los certificados con terminación CRT son archivos PEM.

Al realizar la consulta de los 9 restantes certificados de prueba, se obtienen los siguientes resultados:

```
OpenSSL> ocsp -issuer c:/Test/ac2_4096.crt -cert c:/Test/aimr770903ri4.pem -
text -url https://cfdit.sat.gob.mx/edofiel -VAfile
c:/Test/OCSP_AC_4096_SHA256.crt -header host cfdit.sat.gob.mx

Response verify OK
aimr770903ri4.pem: good
        This Update: Jul 20 22:08:24 2015 GMT
```

```
OpenSSL> ocsp -issuer c:/Test/ac2_4096.crt -cert c:/Test/aacf670505np1.pem -
text -url https://cfdit.sat.gob.mx/edofiel -VAfile
c:/Test/OCSP_AC_4096_SHA256.crt -header host cfdit.sat.gob.mx

Response verify OK
aacf670505np1.pem: revoked
        This Update: Jul 20 22:11:29 2015 GMT
        Next Update: Jul 20 22:16:29 2015 GMT
        Reason: unspecified
        Revocation Time: Jun 12 21:53:29 2014 GMT
```

```
OpenSSL> ocsp -issuer c:/Test/ac2_4096.crt -cert c:/Test/cesj550110p99.pem -
text -url https://cfdit.sat.gob.mx/edofiel -VAfile
c:/Test/OCSP_AC_4096_SHA256.crt -header host cfdit.sat.gob.mx

Response verify OK
cesj550110p99.pem: good
        This Update: Jul 20 22:14:39 2015 GMT
```

```
OpenSSL> ocsp -issuer c:/Test/ac2_4096.crt -cert c:/Test/cms941215jf7.pem -
text -url https://cfdit.sat.gob.mx/edofiel -VAfile
c:/Test/OCSP_AC_4096_SHA256.crt -header host cfdit.sat.gob.mx

Response verify OK
cms941215jf7.pem: good
        This Update: Jul 20 22:15:56 2015 GMT
```

```
OpenSSL> ocsp -issuer c:/Test/ac2_4096.crt -cert c:/Test/con010716a98.pem -
text -url https://cfdit.sat.gob.mx/edofiel -VAfile
c:/Test/OCSP_AC_4096_SHA256.crt -header host cfdit.sat.gob.mx

Response verify OK
con010716a98.pem: good
        This Update: Jul 20 22:18:10 2015 GMT
```

```
OpenSSL> ocsp -issuer c:/Test/ac2_4096.crt -cert c:/Test/eugs6203281q9.pem -
text -url https://cfdit.sat.gob.mx/edofiel -VAfile
c:/Test/OCSP_AC_4096_SHA256.crt -header host cfdit.sat.gob.mx

Response verify OK
eugs6203281q9.pem: good
        This Update: Jul 20 22:21:03 2015 GMT
```

```
OpenSSL> ocsp -issuer c:/Test/ac2_4096.crt -cert c:/Test/gama600504jp1.pem -
text -url https://cfdit.sat.gob.mx/edofiel -VAfile
c:/Test/OCSP_AC_4096_SHA256.crt -header host cfdit.sat.gob.mx

Response verify OK
gama600504jp1.pem: good
        This Update: Jul 20 22:23:00 2015 GMT
```

```
OpenSSL> ocsp -issuer c:/Test/ac2_4096.crt -cert c:/Test/guph751126m88.pem -
text -url https://cfdit.sat.gob.mx/edofiel -VAfile
c:/Test/OCSP_AC_4096_SHA256.crt -header host cfdit.sat.gob.mx

Response verify OK
guph751126m88.pem: good
        This Update: Jul 20 22:25:39 2015 GMT
```

```
OpenSSL> ocsp -issuer c:/Test/ac2_4096.crt -cert c:/Test/hehf7712015z2.pem -
text -url https://cfdit.sat.gob.mx/edofiel -VAfile
c:/Test/OCSP_AC_4096_SHA256.crt -header host cfdit.sat.gob.mx

Response verify OK
hehf7712015z2.pem: good
        This Update: Jul 20 22:28:08 2015 GMT
```

También es posible realizar la consulta sin validación del certificado de OCSP, de la siguiente manera, con respuesta similar, indica que no hay verificación, como se muestra a continuación y continúa reportando el estado del certificado:

```
OpenSSL> ocsp -issuer c:/Test/ac2_4096.crt -cert c:/Test/ac2_4096.crt -url
https://cfdit.sat.gob.mx/edofiel -noverify -header host cfdit.sat.gob.mx

guph751126m88.pem: good
        This Update: Jul 20 22:33:19 2015 GMT
```

XI. ANEXO II – CERTIFICADOS DIGITALES

Un certificado digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Si bien existen variados formatos para certificados digitales, los más comúnmente empleados se rigen por el estándar UIT-T X.509. El certificado contiene usualmente el nombre de la entidad certificada, número de serie, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital) y la firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación.

Formato de certificado digital
Un certificado emitido por una entidad de certificación autorizada como el SAT, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente (Art. 17 Ley de Firma Electrónica Avanzada):

I. Número de serie;
II. Autoridad certificadora que lo emitió;
III. Algoritmo de firma;
IV. Vigencia;
V. Nombre del titular del certificado digital;
VI. Dirección de correo electrónico del titular del certificado digital;
VII. Clave Única del Registro de Población (CURP) del titular del certificado digital;
VIII. Clave pública, y
IX. Los demás requisitos que, en su caso, se establezcan en las disposiciones generales que se emitan en términos de esta Ley.

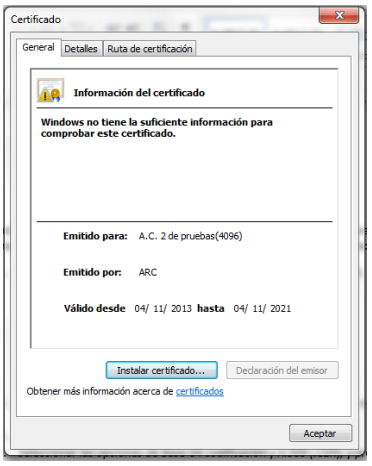
Los Certificados y sus Juegos de Caracteres (codificación)

En esencia un certificado X.509 es un documento digital que ha sido codificado y/o digitalizado conforme al RFC5280 de la IETF.

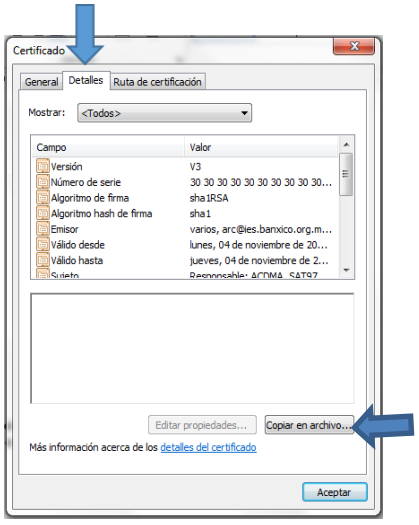
El término certificado X.509 usualmente se refiere al certificado PKIX de la IETF y al perfil de la CRL del certificado estándar X.509 v3, tal y como se especifica en el RFC5280, comúnmente referido como PKIX (Infraestructura de llave pública - X.509).

Los archivos con extensiones .CRT y .CER son intercambiables. Si se requiere el uso del archivo con extensión .CER, puede ser cambiada su extensión considerando lo siguiente:

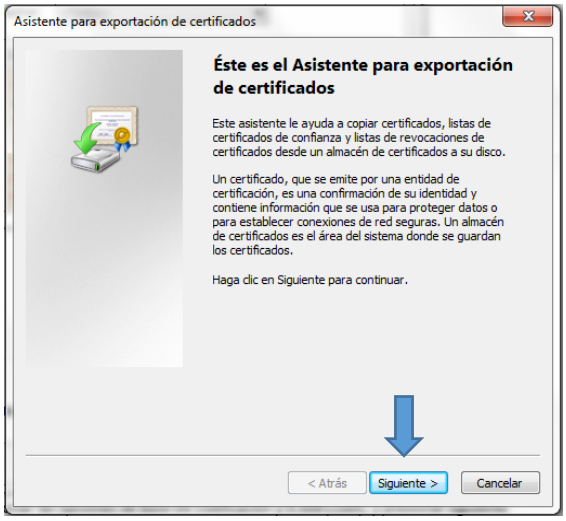
1. Abrir el certificado (ac2_4096.crt) presionando doble click sobre él.



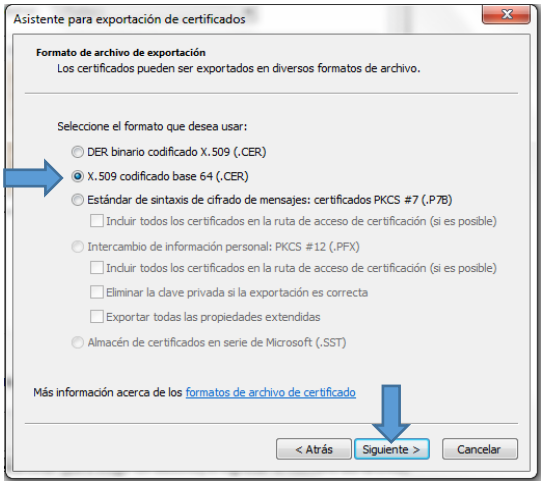
2. Seleccionar la pestaña de detalles, posteriormente seleccionar la opción de copiar que se despliega.



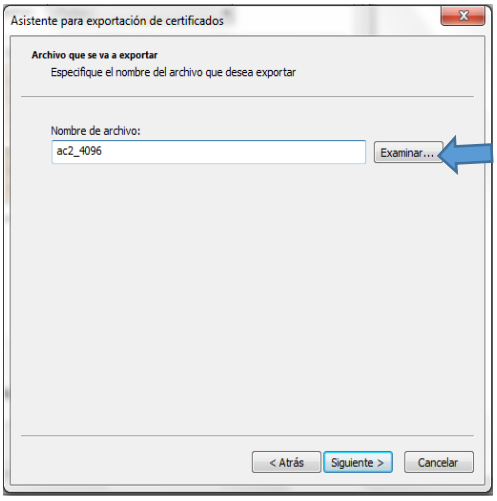
3. Presionar siguiente en el "wizard" que aparece.



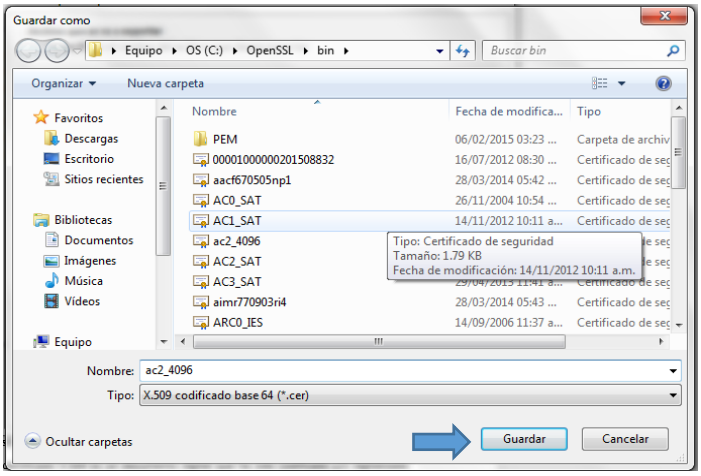
4. Seleccionar las opciones de X.509 (.CER) y Base-64 codificación, y presionar siguiente



5. Seleccionar examinar (para elegir un destino) e ingresar el nombre del archivo "certificado"



6. Salvar. Ahora se cuenta con un certificado .cer (ac2_4096.cer)



Las Extensiones de archivos X509

Lo primero que se debe identificar es el tipo de extensión del archivo. Existe gran confusión acerca del significado de DER, PEM, CRT y CER además de que se maneja incorrectamente que todos ellos son intercambiables.

Sólo en ciertos casos pueden ser intercambiables, las mejores prácticas establecen que se debe de identificar su codificación y etiquetarlo apropiadamente.

Los certificados correctamente etiquetados facilitan el manejo de su codificación (también mencionado como extensiones)

DER → La extensión DER es utilizada para certificados DER codificados binariamente. Siendo ortodoxos en la semántica, es correcto decir "Tengo un certificado codificado en DER" e incorrecto "tengo un certificado DER"

PEM → La extensión PEM es empleada en diferentes tipos de archivos X509 v3 que están construidos en ASCII (Base64) con el prefijo al inicio de línea donde comienza la información "----- BEGIN ....."

Extensiones Comunes

.CRT → La extensión CRT es empleada para certificados. Los certificados podrían estar codificados como binario DER o como ASCII PEM. Las extensiones CER y CRT son casi sinónimos, ya se ha visto un ejemplo al inicio de este anexo. Esto es más común entre sistemas *nix.

.CER → Forma alternativa de los certificados .CRT (Convención Microsoft). Puede emplearse el ambiente Microsoft para convertir .CRT a .CER (Ambos codificación DER -.CER-, o codificación base64 [PEM] -.CER-).

Los archivos con extensión .CER son reconocidos también por IE como un comando ejecutable para correr un comando MS cryptoAPI (Específicamente rundll32.exe cryptex.dll, CryptExtOpenCER) el cual despliega un diálogo para importar o visualizar el contenido de certificados.

.KEY → La extensión KEY es empleada como llave (PKCS8) pública y privada. Estas llaves pueden ser codificadas como DER -binario- o como PEM -ASCII-

Las extensiones CRT y CER pueden ser intercambiadas solamente cuando su codificación es la misma (i.e. CRT Codificación PEM = CER codificación PEM)

Operaciones OpenSSL más comunes sobre Certificados

Existen 4 tipos principales de operaciones sobre Certificados: Abrir, Transformar, Combinar y Extraer

Abrir

Aún y cuando los certificados PEM están codificados en ASCII, no son legibles para el ser humano. Hay varios comandos que permiten obtener el contenido de un certificado en formato legible para el Humano,

Apertura de un certificado

Utilizar el comando de openssl conforme a la extensión del certificado a consultar.

Con el siguiente comando se obtiene la información del certificado con codificación PEM:

```
OpenSSL> x509 -inform pem -in c:/Test/OCSP_AC_4096_SHA256.crt -noout -text

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            30:30:30:30:31:30:38:38:38:38:38:38:31:30:30:30:30:30:30:37
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=A.C. 2 de pruebas(4096), O=Servicio de
Administraci\xC3\xB3n Tributaria, OU=Admi
istraci\xC3\xB3n de Seguridad de la
Informaci\xC3\xB3n/emailAddress=asisnet@pruebas.sat.gob.mx/stre
t=Av. Hidalgo 77, Col. Guerrero/postalCode=06300, C=MX, ST=Distrito Federal,
L=Coyoac\xC3\xA1n/x500
niqueIdentifier=SAT970701NN3/unstructuredName=Responsable: ACDMA
        Validity
            Not Before: Jun 27 06:25:12 2015 GMT
            Not After : Jun 26 06:25:12 2023 GMT
        Subject: O=Servicio de Administracion Tributaria, OU=Seguridad de la
Informacion, C=MX, ST=
istrito Federal, L=Coyoacan, CN=AVL - PKI/unstructuredName=SAT
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b6:bf:07:18:43:26:47:03:cb:d4:4d:bc:7f:f2:
                    3f:f6:3c:69:f0:64:ee:9d:17:5b:17:21:e6:a3:2c:
                    d3:39:1e:76:ba:45:ba:a5:ae:4e:5c:60:9d:4e:e3:
                    76:e9:89:cf:7e:c4:ab:09:3d:0f:96:74:a2:67:a2:
                    fd:24:b5:ab:ec:cb:bb:82:19:75:cb:c4:f8:fc:aa:
                    04:a5:3d:ae:f4:44:9b:35:d1:05:a2:3b:23:b6:f9:
                    a7:73:e2:6b:f3:b0:5c:ae:8a:b4:f5:56:ac:de:0c:
                    fb:18:32:71:d8:1e:23:fa:1f:de:d0:c7:f7:22:56:
                    a2:ea:ea:ab:36:db:cf:a9:94:b2:a8:5b:96:d1:7c:
                    a2:9a:bb:c7:7a:69:cb:f8:f3:b6:4e:22:5c:b2:25:
                    7a:b4:f3:12:3d:b4:95:92:6c:16:0e:ce:e5:d5:92:
                    20:da:33:75:b9:33:43:d8:fb:5a:a6:76:ca:f5:c6:
                    59:de:23:19:7f:d2:d5:c5:d8:ad:0a:fc:63:41:ce:
                    4b:bf:52:da:24:e7:01:17:73:d7:92:85:ea:32:ac:
                    57:f4:5f:12:3c:e2:34:29:9f:73:9e:09:37:e3:a0:
                    6f:54:10:f1:57:87:45:1e:d8:f7:3a:74:af:76:26:
                    9d:21:d5:87:ce:3e:7b:05:e7:85:26:d5:ff:0e:96:
                    26:ef
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Extended Key Usage:
                OCSP Signing
            Authority Information Access:
                OCSP - URI:https://cfdit.sat.gob.mx/edofiel

            X509v3 Subject Key Identifier:
                A8:20:16:E4:AA:1B:C7:4C:3E:65:A5:B0:87:75:4E:02:7C:F7:A6:FA
            X509v3 Authority Key Identifier:

keyid:EB:66:6A:95:50:0C:E5:31:BB:EE:38:89:ED:CD:B7:B2:53:0D:69:16
```

```
    Signature Algorithm: sha256WithRSAEncryption
         5b:89:a1:df:fc:1e:15:ce:22:36:6f:ef:c6:24:fb:f9:6b:61:
         10:c8:14:ad:99:6d:55:a8:1d:ab:a0:e3:b4:d7:d9:29:f1:9a:
         a7:5e:7a:83:a5:38:57:69:d8:88:7e:63:7d:7e:94:73:bd:28:
         b6:14:58:4b:05:d4:d0:b5:e7:2a:fb:e2:42:18:37:fc:3c:e5:
         f9:d0:5b:3e:0a:2c:c2:9a:e2:5e:f1:37:50:1f:7a:dd:f8:29:
         b5:a5:e5:f0:39:8d:58:5f:eb:45:8b:91:cb:b3:75:ac:7b:03:
         49:22:21:4c:9d:22:9e:12:e8:4b:9e:be:a1:94:05:5b:41:78:
         3a:e1:bb:bb:0e:0a:07:59:67:68:8c:b7:ef:41:d5:b2:d4:a2:
         f0:ed:a1:b3:4a:62:2d:00:ad:1d:c6:04:d0:28:89:8c:b9:a0:
         fd:e5:d6:32:98:88:1c:75:ce:95:30:c7:87:59:52:8c:e8:67:
         fb:59:07:d5:1f:6a:f1:1b:e9:c5:21:3d:ed:56:20:64:64:7e:
         f9:c9:ae:08:5a:f4:f7:a4:2c:6d:92:8d:86:84:39:41:c3:c0:
         6b:b8:b6:55:47:85:3f:05:99:de:5e:12:7b:70:d4:a4:7e:f4:
         7f:b7:d7:65:d5:c1:25:85:b6:63:5c:a7:1d:5a:eb:cd:15:5d:
         8f:09:9c:14:a0:8b:61:9a:38:9d:42:11:2a:49:d8:c2:7c:2a:
         a6:3f:93:e1:98:9e:89:89:a7:92:f6:70:6c:49:a1:68:c8:48:
         6d:c9:09:7a:c6:d1:5a:46:14:15:16:e3:7d:f8:77:ce:f7:59:
         96:72:14:5a:6a:18:d3:78:34:b9:2b:ee:16:b0:d7:e4:f4:e0:
         6c:19:00:22:32:80:1d:7a:cb:25:13:17:05:8c:46:2e:db:48:
         d1:06:c3:35:fb:71:95:50:23:d7:fc:4a:ea:a0:d9:97:26:ef:
         5a:49:0c:6f:f9:bf:6c:77:c2:98:51:9e:ee:aa:6e:93:d3:14:
         72:2a:a5:b6:78:f9:a6:52:d8:41:c7:72:41:d7:76:97:8f:13:
         22:80:9f:fc:5a:1f:12:e4:f5:e7:7a:a0:1b:34:12:f7:78:1a:
         dc:8a:d3:e5:2b:17:d1:88:58:72:bc:77:c2:74:2d:0f:b8:94:
         4c:cd:b7:d4:76:3c:ca:df:ab:b7:99:5f:e7:00:03:6d:43:53:
         1d:ee:60:79:0d:8c:f3:1e:7d:26:db:81:2b:7d:e5:9f:f9:9d:
         5a:26:c1:86:ec:0f:fe:0d:6e:41:5b:df:45:c5:bc:3b:22:25:
         a5:17:ad:ff:55:f0:d8:07:2b:40:cf:33:9e:35:ef:0a:fd:48:
         b1:1d:a9:80:1b:1b:a6:25
```

El mismo certificado en codificación CER requiere del siguiente comando:

```
OpenSSL> x509 -inform der -in c:/Test/ac2_4096.cer -noout -text
```

En caso de realizar la consulta del certificado CER indicando codificación PEM se obtiene el siguiente error:

```
unable to load certificate
12626:error:0906D06C:PEM routines:PEM_read_bio:no start
line:pem_lib.c:647:Expecting: TRUSTED CERTIFICATE
```

Esto se da porque está tratando de visualizar un certificado con codificación DER y requiere utilizar el comando para visualizar certificados con codificación DER que se mostró con antelación.

Si por el contrario intenta una consulta de un certificado PEM indicando codificación CER se obtiene el siguiente error:

```
unable to load certificate
3580:error:0D0680A8:asn1 encoding
routines:ASN1_CHECK_TLEN:wrongtag:.\crypto\asn1\tasn_dec.c:1319:
3580:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:.\crypto\asn1\tasn_dec.c:381:Type=X509
error in x509
```

Si se obtiene el error, entonces está tratando de visualizar un certificado con codificación PEM con un comando para certificados con codificación DER. Requiere utilizar el comando ejemplificado al inicio de esta sección.

Transformar

Es posible transformar la codificación de un certificado a otra codificación.

PEM to DER

```
openssl> x509 -in c:/Test/ac2_4096.crt -outform der -out
c:/Test/ac2_4096.der
```

DER to PEM

```
openssl x509 -in c:/Test/ac2_4096.crt -inform der -outform pem -out
C:/Test/cert.pem
```

Combinar

En algunos casos tiene ventaja combinar múltiples piezas de la infraestructura X509 en un solo archivo. Un ejemplo es la combinación de ambas llaves, la pública y la privada en un mismo certificado.

La manera más fácil de combinar certificados y cadenas es convertirlos cada uno de ellos certificados codificados PEM para posteriormente simplemente copiar el contenido de cada archivo en un nuevo archivo. Esto es empleado para combinar archivos y usarles en aplicaciones como Apache por ejemplo.

Extraer

Algunos certificados están combinados. Un archivo puede contener cualesquiera de: Certificado, Clave privada, Clave Pública, Certificado firmado, Certificaddo de AC y/o Cadena de autoridad.