Glosario

Términos en México

CIEC

La Clave de Identificación Electrónica Confidencial (CIEC) es un sistema de identificación basado en el RFC y NIP (número de identificación personal).

Agencia certificadora

Entidad responsable de establecer identidades y crear los certificados digitales que forman la asociación entre una identidad y una pareja de claves pública/privada (SAT y agencias prestadoras de servicios de certificación autorizadas por el Banco de México).

Agencia registradora central

Entidad responsable de autorizar a las autoridades certificadoras para que presten servicios en su nombre, siendo ésta la que concentra el directorio de certificados digitales y los movimientos realizados a los mismos (BANXICO).

Agencia registradora

Entidad responsable de identificar y registrar en forma inequívoca al solicitante de un certificado fiscal digital. Solicita a la autoridad certificadora la información verificada del solicitante, para emitirle un certificado digital (SAT).

Autenticidad

Característica intrínseca de la Firma Electrónica Avanzada, gracias a la cual el autor del mensaje queda acreditado puesto que permite verificar la identidad del emisor de un documento.

CERTISAT Sistema de certificación del SAT

Es el sistema encargado de controlar todo lo relacionado con la creación y mantenimiento de certificados digitales expedidos por el SAT.

Clave de RFC

Es la cadena de caracteres que, de tratarse de una persona física, se compone de 4 letras, 6 dígitos numéricos y 3 dígitos alfanuméricos, que el contribuyente obtiene en el

momento de inscribirse ante la Secretaría de Hacienda. Si el contribuyente es persona moral, la cadena se compone de 3 letras, 6 dígitos numéricos y 3 dígitos alfanuméricos.

Clave de Identificación Electrónica Confidencial (CIEC)

Sistema de identificación basado en el RFC y el NIP (número de identificación personal), utilizado para realizar declaraciones provisionales y declaraciones anuales.

CFD Comprobantes Fiscales Digitales

Las personas físicas y las morales que cuenten con un certificado de Firma Electrónica Avanzada vigente, y lleven su contabilidad en sistema electrónico, podrán emitir los comprobantes de las operaciones que realicen mediante documentos digitales, siempre que dichos documentos cuenten con sello digital amparado por un certificado expedido por el Servicio de Administración Tributaria, cuyo titular sea la persona física o la persona moral que expida los comprobantes.

Criptografía

Se define como el arte o ciencia de escribir en código, de tal forma que permita que sólo el destinatario lo descifre y comprenda utilizando una clave.

Criptografía de clave pública

Sistema de encriptación basado en el uso de un par de llaves (pública y privada), el cual opera de tal modo que lo que es cifrado con una de las claves sólo puede ser descifrado con la otra, y viceversa.

Certificado digital

Los certificados digitales tienen como objetivo identificar al dueño de una Firma Electrónica Avanzada. Estos certificados contienen información diversa acerca del firmante, además de los servicios a los que éste tiene acceso para utilizar su firma, la fecha de vigencia del certificado, la Agencia Certificadora que lo emitió, entre otras características.

Confidencialidad

Sólo el receptor y el emisor del mensaje podrán participar en la transacción, ya que la encriptación transforma el mensaje original en caracteres ininteligibles y el acceso al mensaje original es restringido por medio de claves.

Encriptación

Es la acción de codificar información de tal forma que sólo quien conoce la estructura del código pueda descifrarlo. Para efectos de este proyecto, la información del certificado se codificará de tal manera que sólo las aplicaciones emitidas por el SAT podrán descifrarla.

Firma Electrónica Avanzada

Conjunto de datos asociados a un mensaje, que permiten asegurar la identidad del contribuyente y la integridad (imposibilidad de modificarlo posteriormente) del mensaje. Además de contar con un certificado digital expedido por el SAT o por un prestador de servicios de certificación autorizada, esta firma tiene las cualidades de Reconocimiento por el marco legal, y de Fiabilidad técnica basada en infraestructura de llave pública, otorgando las garantías de Integridad, No repudio, Autenticidad y Confidencialidad.

Homoclave

Son los tres últimos caracteres alfanuméricos de cualquier RFC, los cuales evitan duplicidad de información de los contribuyentes, por lo que proporciona una identidad única e irrepetible al contribuyente.

IES

La infraestructura extendida de seguridad es un sistema diseñado y administrado por el Banco de México, con el propósito de fortalecer la seguridad de la información que se transmite tanto en los sistemas de pago como entre el sistema financiero mexicano y el instituto central. La IES está basada en el uso de firmas electrónicas mediante la aplicación de algoritmos criptográficos para garantizar la confidencialidad e integridad de la información que se transmite, y a su vez, acreditar la identidad del remitente.

Integridad

Característica intrínseca de la Firma Electrónica Avanzada. Garantiza que la información contenida en el mensaje queda protegida y no puede ser manipulada o modificada durante el proceso; es decir, confirma la no alteración de los datos desde su origen.

Infraestructura de clave pública (ICP)

También conocida como PKI (Public Key Infrastructure), es un conjunto de protocolos, servicios y estándares, que soportan las aplicaciones basadas en criptografía de clave pública, además de brindar los servicios de creación segura de claves, validaciones de identidades, expedición, renovación y terminación de certificados, validación de certificados, distribución de certificados, generación de firma, establecimiento y administración de relaciones de confianza.

Llave privada (*.key)

Es uno de los documentos electrónicos que genera el uso de algoritmo asimétrico y que sólo debe ser conocido y resguardado por el propietario del par de llaves (pública/privada). Con esta llave privada se realiza el firmado digital, mismo que codifica el contenido de un mensaje.

Llave pública (*.req)

Es uno de los documentos electrónicos que genera el uso de algoritmo asimétrico y que se publica junto con el certificado digital para cifrar información que se desea enviar al propietario de la llave privada. La llave pública se presenta dentro del archivo de requerimiento para presentarlo ante el SAT y obtener un certificado digital.

No repudio

El emisor que firme electrónicamente un documento no podrá negar que envió el mensaje original, ya que éste es imputable al emisor por medio de las claves que sólo conoce él mismo. El no repudio permite comprobar quién participó en una transacción.

Persona Física

Es aquel contribuyente que se constituye de un solo individuo.

Persona Moral

Es el contribuyente que se constituye por una empresa, asociación u organización.

Sello digital

(Artículo 17-E del Código Fiscal de la Federación). Cuando los contribuyentes remitan un documento digital a las autoridades fiscales, recibirán el acuse de recibo que

contenga el sello digital. El sello digital es el mensaje electrónico que acredita que un documento digital fue recibido por la autoridad correspondiente y estará sujeto a la misma regulación aplicable al uso de una Firma Electrónica Avanzada. En este caso, el sello digital identificará a la dependencia que recibió el documento y se presumirá, salvo prueba en contrario, que el documento digital fue recibido en la hora y fecha que se consignen en el acuse de recibo mencionado.

SAT

Servicio de Administración Tributaria.

Certificado de sello digital

Los certificados de sellos digitales son expedidos por el SAT para uso exclusivo de Comprobantes Fiscales Digitales. Por medio de ellos el contribuyente podrá firmar los comprobantes que emita en cada una de sus sucursales; así se tendrá identificado el origen de la factura, junto con todas las demás características que tienen los certificados (Integridad, no repudio, autenticidad y confidencialidad). El contribuyente puede optar por pedir un solo sello digital para todas las sucursales o puntos de facturación, o un sello digital por cada uno.

Sistema Integral de Comprobantes Fiscales (SICOFI)

Este sistema se encarga de asignar folios y recibir reportes mensuales de facturas electrónicas emitidas vía web por parte de aquellos contribuyentes que estén interesados en emitir facturas electrónicas.

Solicitud de Certificados Digitales (SOLCEDI)

La aplicación de la Solicitud del Certificado Digital (SOLCEDI) será utilizada para que el contribuyente (Persona Moral o Persona Física) pueda generar un archivo de requerimiento, con el cual realizará el proceso para obtener un Certificado Digital que ocupará en sus movimientos de tipo fiscal.

Suscribe

Aplicación a través de la cual los contribuyentes dictaminados y los contadores públicos registrados obtienen un certificado digital para presentar ya sea un dictamen o declaraciones electrónicas.

Tu Firm@

Nombre con el cual se dio a conocer la Firma Electrónica Avanzada. Ambos términos se utilizan indistintamente.

Certificado

Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.

Datos de Creación de Firma Electrónica

Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.

Destinatario

La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje.

Emisor

Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.

Firma Electrónica

Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Firmante

La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.

Intermediario

En relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él.

Mensaje de Datos

La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

Parte que Confía

La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.

Prestador de Servicios de Certificación

La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.

Secretaría

Se entenderá la Secretaría de Economía.

Sistema de Información

Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos.

Titular del Certificado: Se entenderá a la persona a cuyo favor fue expedido el Certificado.

CFF

Código Fiscal de la Federación.

Términos en España.

Firma electrónica

Es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente el autor o los autores del documento que la recoge.

Firma electrónica avanzada

Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

Signatario

Es la persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

Datos de creación de firma

Son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica.

Dispositivo de creación de firma

Es un programa o un aparato informático que sirve para aplicar los datos de creación de firma.

Dispositivo seguro de creación de firma

Es un dispositivo de creación de firma que cumple los requisitos establecidos en el artículo 19.

Datos de verificación de firma

Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

Dispositivo de verificación de firma

Es un programa o un aparato informático que sirve para aplicar los datos de verificación de firma.

Certificado

Es la certificación electrónica que vincula unos datos de verificación de firma o un signatario y confirma su identidad.

Certificado reconocido

Es el certificado que contiene la información descrita en el artículo 8 y es expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en el artículo 12.

Prestador de servicios de certificación

Es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

Producto de firma electrónica

Es un programa o un aparato informático o sus componentes específicos, destinados a ser utilizados para la prestación de servicios de firma electrónica por el prestador de servicios de certificación o para la creación o verificación de firma electrónica.

Acreditación voluntaria del prestador de servicios de certificación

Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se dicta, a petición del prestador al que le beneficie, por el organismo público encargado de su supervisión