UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN MODALIDAD PROYECTO DE APLICACIÓN

SISTEMA EMISOR DE FACTURAS ELECTRÓNICAS

PARA OPTAR AL GRADO DE

MAESTRO EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESORA:

DRA. MARÍA DE LOURDES LÓPEZ GARCÍA

PRESENTADO POR:

JORGE MIGUEL ERAZO MELARA

JOSÉ ORLANDO TORRES AGUILUZ

KATYA KAROLYNA RODRÍGUEZ RIVAS

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América.

JUNIO 2015

Agradecimientos

Agradecimientos,

A Dios Padre todopoderoso, por su infinita misericordia y permitirme finalizar este logro profesional.

A mi santísima Madre la Virgen de Guadalupe, quien siempre me ha brindado su protección y cuidados.

A mis padres Ernesto y Ana Josefa, por su apoyo incondicional, amor y confianza en todos los proyectos de mi vida.

A mi hermano Reynaldo, por sus consejos, apoyo y sobre todo, por ser para mí un modelo de perseverancia, dedicación, esfuerzo y lucha por conseguir los propósitos trazados en la vida.

A mis abuelos Frank y Elba, por sus constantes oraciones y apoyo.

A mi familia por apoyarme en este proyecto.

A mis compañeros de tesis Jorge y José, por la oportunidad de trabajar en juntos y compartir conocimientos y experiencias que nos enriquecieron como personas y profesionales.

A la asesora Lourdes, por su dedicación y palabras de aliento para el feliz término del proyecto.

Katya Karolyna Rodríguez Rivas

Agradecimientos.

En primer lugar, agradecer a Dios Padre por medio de mi señor Jesucristo que en su santa voluntad me permitiera alcanzar una nueva meta profesional.

A mi esposa Verónica Mejía de Erazo, por su apoyo incondicional en los momentos de flaqueza, su inigualable compañía y comprensión en todo momento.

A mi madre Mirna Cano, que gracias a su esfuerzo pude alcanzar mi grado universitario y por el cual ahora tengo la oportunidad, por mi cuenta, de alcanzar el grado de maestro.

A mi hermano Ricardo Erazo, por ser un ejemplo de constancia, dedicación y esfuerzo.

A mi asesora y compañeros de tesis por la oportunidad de conocerlos y compartir experiencias.

Jorge Erazo

Agradecimientos.

A Dios todo poderoso que escucho mis oraciones brindándome la oportunidad de iniciar un nuevo reto académico y las fuerzas para culminarlo.

A mis padres y hermanos que siempre me han apoyado y brindado ánimos para seguir adelante y no desfallecer en el camino.

A mis tías y tíos que me han dado aliento y consejos en todo momento para continuar persiguiendo mis sueños y deseos.

A mis abuelos (Q.D.D.G) que con su ejemplo de perseverancia y dedicación me enseñaron a seguir adelante a pesar de las dificultades que la vida nos presenta.

A nuestra asesora Lourdes por su apoyo y consejos que nos permitieron culminar de forma exitosa nuestra tesis, y a mis compañeros Katya y Jorge por tener la oportunidad de trabajar a su lado y gracias a su dedicación y esmero hoy hemos culminado nuestra tesis.

José Torres.

Contenido

Índice de Figuras

1 Introducción

En El Salvador, la emisión de facturas electrónicas es un proyecto que deberá ser implementado a corto plazo por las empresas. Si bien es cierto aún no ha sido aprobado por el estado ya se está estudiando el anteproyecto.

Una factura es el justificante fiscal de la entrega de un producto o de la provisión de un servicio, que afecta al obligado tributario emisor (el vendedor) y al obligado tributario receptor (el comprador). Tradicionalmente, es un documento en papel, cuyo original debe ser archivado por el receptor de la factura. Habitualmente, el emisor de la factura conserva una copia o la matriz en la que se registra su emisión.

La factura electrónica es el equivalente digital y evolución lógica de la tradicional factura en papel. A diferencia de ésta, se emplean soportes informáticos para su almacenamiento en lugar de un soporte físico como es el papel.

En los países en los que la legislación lo admite, la validez de una factura electrónica es exactamente la misma que la de la tradicional factura en papel y gracias a soluciones criptográficas que se incluyen se garantiza su integridad y un alto nivel de trazabilidad, por lo que judicialmente es un documento considerado como vinculante y que no necesita de mayor prueba o confirmación de su propia existencia.

La factura electrónica es un tipo de factura que se diferencia de la factura en papel por la forma de gestión informática y el envío mediante un sistema de comunicaciones que conjuntamente permiten garantizar la autenticidad y la integridad del documento electrónico.

Una factura electrónica se produce fundamentalmente en un proceso que se puede dividir en dos grandes fases:

1. Creación de una factura tal y como se ha hecho siempre y se almacena en un fichero de datos.
2. Generación de una firma digital con un certificado electrónico propiedad del tributario emisor que certifica el contenido de la factura y añade el sello digital a la misma.
3. Verificación de la firma digital

Al terminar se obtiene una factura que garantiza, en primer lugar, que la persona física o jurídica que firmó la factura es quien dice ser (autenticidad) y en segundo lugar, que el contenido de la factura no ha sido alterado (integridad).

El emisor envía la factura al receptor mediante medios electrónicos, como pueden ser CDs, memorias Flash e incluso Internet. Si bien se dedican muchos esfuerzos para unificar los formatos de factura electrónica, actualmente está sometida a distintas normativas y tiene diferentes requisitos legales exigidos por las autoridades tributarias (Ministerio de Hacienda), de forma que no siempre es posible el uso de la factura electrónica, especialmente en las relaciones con empresas extranjeras que tienen normativas distintas a la del país de origen.

Los requisitos legales respecto al contenido mercantil de las facturas electrónicas son exactamente los mismos que regulan las tradicionales facturas en papel. Los requisitos legales en relación con la forma imponen un determinado tratamiento con el fin de garantizar la integridad y la autenticidad y ciertos formatos que faciliten la interoperabilidad.

Hoy día, la organización GS1 (antes EAN/UCC) a nivel mundial ha organizado comités internacionales de usuarios de 108 países miembros, para conformar las guías de facturación electrónica estándar a nivel mundial.

La factura electrónica permite que instituciones, empresas y profesionales dejen atrás las facturas en papel y las reemplacen por la versión electrónica del documento tributario. Tiene exactamente la misma validez y funcionalidad tributaria que la factura tradicional en papel. Todo el ciclo de la facturación puede ser administrado en forma electrónica.

Por tal motivo en este trabajo se propone el desarrollo de un Sistema Emisor de Facturas Electrónicas (SEFE) según las leyes fiscales salvadoreñas.

Como en varios países ya se encuentra establecida la facturación digital, para lograr el objetivo planteado en este trabajo, se usará como base la implementación que realizó el Gobierno de México en su factura digital.

Además, el sistema propuesto brindará al usuario un método útil y de fácil manejo para la transmisión de la factura y su firma a terceros. En este caso, se ha optado por dotar a la aplicación con la funcionalidad de ser capaz de enviar dichos ficheros por correo electrónico.

Los alcances definidos en este trabajo son los siguientes:

- ✓ Crear un protocolo seguro de emisión de facturas que pueda ser la base para la creación de aplicaciones seguras.
- ✓ Elaborar un prototipo funcional en JAVA para realizar pruebas de funcionamiento.
- ✓ Crear una propuesta de Diseño para el formato de la Factura Digital de Crédito Fiscal, esto considerando que serían las empresas las que primero adoptaría la factura digital.

El resto del documento se organiza como sigue. En el capítulo 2 se presenta el contexto o margo legal vigente en El Salvador aplicable a la emisión de facturas. Dicho marco legal es aplicable también a las facturas electrónicas y han sido contempladas en el prototipo de este proyecto.

Las herramientas criptográficas utilizadas en el prototipo de factura electrónica propuesto se describen en el capítulo 3, presentando una breve descripción de cada una de ellas así como su funcionamiento lógico.

En el capítulo 4 se detalla la funcionalidad del sistema de factura electrónica objeto del presente documento. Se contempla desde el análisis de los requerimientos, la generación de la

factura digital, los protocolos entre el emisor y el receptor y finalmente un análisis de la seguridad del prototipo.

Un detalle paso a paso del sistema emisor de factura electrónica se detalla en el capítulo 5, se describe la funcionalidad del sistema con imágenes de cada una de las etapas y pasos para su funcionamiento.

2 Marco Legal

Para la automatización de la facturación en El Salvador, es necesario conocer todos los aspectos legales que la involucran. A continuación se listan los artículos extraídos de las leyes de El Salvador aplicables a materia tributaria [1,2,3,4],:

2.1 Constitución de la República de El Salvador

Art. 101: El orden económico debe responder esencialmente a principios de justicia social, que tiendan a asegurar a todos los habitantes del país una existencia digna del ser humano.

El Estado promoverá el desarrollo económico y social mediante el incremento de la producción, la productividad y la racional utilización de los recursos. Con igual finalidad, fomentará los diversos sectores de la producción y defenderá el interés de los consumidores.

2.2 Código Tributario

Artículo 107: Los contribuyentes del Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios están obligados a emitir y entregar, por cada operación, a otros contribuyentes un documento que, para los efectos de este Código, se denominará "Comprobante de Crédito Fiscal", que podrá ser emitido en forma manual, mecánica o computarizada, tanto por las transferencias de dominio de bienes muebles corporales como por las prestaciones de servicios que ellos realicen, sean operaciones gravadas, exentas o no sujetas, salvo en los casos previstos en los artículos 65 y 65-A de la Ley de Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios, en los que deberán emitir y *entregar Factura*.

Cuando se trate de operaciones realizadas con consumidores finales, deberán emitir y entregar, por cada operación, un documento *que se denominará "Factura"*, la que podrá ser sustituida por otros documentos o comprobantes equivalentes, autorizados por la Administración Tributaria. Los contribuyentes del Impuesto a la Transferencia de Bienes Muebles y a la

Prestación de Servicios, en ningún caso deberán tener en sus establecimientos para documentar las transferencias de bienes o prestaciones de servicios que realicen, Facturas Comerciales u otro documento distinto a los previstos en este Código. Se faculta a la Administración Tributaria para proceder al decomiso y destrucción de los mismos.

2.3 Requisitos Formales de los Documentos

Artículo 114: Los documentos que utilicen los contribuyentes cumplirán, en todo caso, con las siguientes especificaciones y menciones:

a) Facturas u otros documentos a emitir a no contribuyentes del impuesto o consumidores finales:

1. Deben imprimirse en talonarios y estar prenumerados en forma correlativa asimismo podrán imprimirse en talonarios prenumerados por series en forma correlativa e independiente, para cada establecimiento, negocio u oficina;
2. Indicar el nombre, denominación o razón social del contribuyente emisor, giro o actividad, dirección del establecimiento u oficina y de las sucursales, si las hubiere, Número de Identificación Tributaria y Número de Registro de Contribuyente;
3. Fecha de emisión;
4. Se emitirán en duplicado en forma correlativa, debiendo entregarse en caso de las operaciones locales la copia al adquirente del bien o prestatario del servicio y en las operaciones de exportación deberá entregarse el original al cliente y, cumplir con las especificaciones que el tráfico mercantil internacional requiere;
5. Descripción de los bienes y servicios especificando las características que permitan individualizar e identificar plenamente tanto el bien como el servicio comprendido en la operación, el precio unitario, cantidad y monto total de la operación;
6. Separación de las operaciones gravadas, exentas y no sujetas;
7. Inclusión del impuesto respectivo en el precio de las operaciones gravadas;
8. Valor total de la operación;
9. Número y fecha de la nota de remisión cuando hubiere sido emitida con anterioridad;
10. En operaciones cuyo monto total sea igual o superior a doscientos dólares, se deberá hacer constar en el original y copia de la factura el nombre, denominación o razón social, número de identificación tributaria o en su defecto, el número del documento único de identidad del adquirente de los bienes o del prestatario de los servicios. En el caso de adquirentes extranjeros se hará constar el número de pasaporte o el carnet de residencia;
11. Pie de imprenta: nombre, número de identificación tributaria, denominación o razón social, domicilio, número de registro de contribuyente del propietario de la imprenta, número y fecha de autorización de imprenta, rango de numeración correlativa autorizada con su respectivo número y fecha de autorización.

b) Factura de venta simplificada

1. Deben elaborarse por medio de imprenta en talonarios preimpresos y estar prenumerados en forma correlativa; asimismo, podrán imprimirse en talonarios por series en forma correlativa e independiente para cada establecimiento, negocio u oficina;
2. Indicar de manera preimpresa el nombre del contribuyente emisor, giro o actividad económico, dirección del establecimiento u oficina, y de las sucursales si las hubiere, número de identificación tributaria y número de registro de contribuyente;
3. Fecha de emisión del documento;
4. Pie de imprenta; Nombre, Número de Identificación Tributaria, denominación o razón social, domicilio, número de registro de contribuyente del propietario de la imprenta, número y fecha de autorización de imprenta, tiraje de documentos y fecha de impresión.
5. Se emitirá en duplicado en forma correlativa, debiendo entregarse la copia al adquirente del bien o prestatario de los servicios;
6. Valor total de la operación, en el que deberá incluirse el impuesto respectivo de las operaciones gravadas.

Los requisitos de la Factura de Venta Simplificada que deberán ser impresos por la imprenta son los contenidos en los numerales 1, 2 y 4 antes referidos, y los restantes requisitos deberán ser cumplidos por el contribuyente al momento de su emisión y entrega.

Todos los documentos que deban ser impresos por imprenta autorizada, además de los requisitos establecidos en este Artículo deberán contener de manera preimpresa el número de autorización de asignación de numeración correlativo otorgado por la Administración Tributaria. Lo anterior no es aplicable a los tiquetes de máquinas registradoras, los cuales únicamente deberán contener el respectivo número correlativo asignado y autorizado por la Administración Tributaria. *En el caso de documentos electrónicos deberá hacerse constar el número correlativo autorizado en cada documento por medio del sistema que se utiliza para emitirlos, así como el rango autorizado al que corresponden, el número y fecha de autorización de la numeración correlativa*.

Los valores consignados por los contribuyentes en los documentos que emitan y entreguen a los adquirientes de bienes o prestatarios de servicios, deberán coincidir con los que consten en los documentos que dichos contribuyentes conserven para revisión de la Administración Tributaria.

2.4 Emisión de tiquetes en sustitución de Facturas por medio de máquinas registradoras u otros Sistemas computarizados

Artículo 115: Cuando la emisión de facturas resultare impráctica o de difícil aplicación, por la naturaleza propia del negocio o del sistema particular de ventas o servicios, la Administración Tributaria podrá autorizar mediante resolución la utilización de máquinas registradoras u otros sistemas computarizados para la emisión de tiquetes en sustitución de facturas. En todo caso se deberán cumplir los requisitos mínimos siguientes:

a. Los documentos emitidos por tales medios deberán cumplir con los requisitos establecidos en este Código para las facturas, y además, contener el número de máquina registradora con el que se autorice;
b. El cartel de autorización debe ser colocado junto a la máquina registradora en un lugar visible. Asimismo dicho equipo deberá mantenerse accesible en el establecimiento para el cual fue autorizada para verificación de la Administración Tributaria;
c. Las máquinas registradoras que se utilicen para emitir tiquetes en sustitución de facturas deberán llevar cintas o rollos de auditoría con el registro de las transferencias o servicios que constituirán una copia fiel de los tiquetes emitidos, las cuales se archivarán en orden cronológico, para su examen y comprobación por parte de la Administración Tributaria. En el caso que los contribuyentes utilicen Sistemas computarizados para la emisión de tiquetes en sustitución de facturas, la Administración Tributaria podrá autorizar que el respaldo de dichos tiquetes se lleve por medios magnéticos o electrónicos, siempre que se garantice el interés fiscal; y,
d. Asimismo deberá emitirse un tiquete que resuma el total de operaciones diarias realizadas.
e. La autorización de las máquinas registradoras o sistemas computarizados estará condicionada a que la información correspondiente a cada operación sea remitida a la Administración Tributaria, cuando ésta lo requiera en el ejercicio de sus facultades legales, ya sea por medios físicos, electrónicos o tecnológicos, de acuerdo a los sistemas de información del sujeto pasivo. La Administración Tributaria, podrá establecer que la información referida en este inciso, se transmita en línea a sus servidores en la forma, plazo y bajo los alcances que ésta disponga, en la medida que los recursos tecnológicos del sujeto pasivo y de la Administración Tributaria lo permitan.

2.5 Reglamento de Aplicación del Código Tributario

Artículo 44: Para los efectos de lo dispuesto en el artículo 115 del Código Tributario, las máquinas registradoras o sistemas computarizados a través de los cuales los contribuyentes pretendan emitir tiquetes en sustitución de facturas, deberán contener las especificaciones de identificación siguientes: número de la máquina registradora o sistema computarizado, marca,

modelo y serie, dichas características deben constar en forma visible en el referido equipo. En los sistemas computarizados estos datos serán los correspondientes a la Unidad Central de Procesamiento, si el sistema está en red, los datos corresponderán tanto a las terminales que se autorizarán como al servidor central. En caso que los sistemas computarizados adquiridos por el contribuyente no sean originales de fábrica, sino armado por piezas de diferentes fabricantes, generarán la serie por cada equipo, fijando en ellos la identificación de tal manera que garantice el interés fiscal.

El número de máquina o sistema computarizado propuesto por el contribuyente no podrá ser asignado a otra máquina o sistema computarizado respecto del cual posteriormente solicite autorización, salvo que el propuesto no hubiese sido autorizado por la Administración.

Las máquinas registradoras o sistemas computarizados mencionados, deberán ser capaces de generar como mínimo cuatro dígitos por capacidad de emisión para el registro de la operación correlativa y una capacidad mínima de registro del valor unitario de venta de cuatro dígitos además de las dos cifras decimales; poseer un contador automático inviolable que registre e imprima la cantidad de tiquetes emitidos y el total de las ventas acumuladas en el día sin perder el acumulado de las ventas efectuadas.

Artículo 87: Cuando con posterioridad a la emisión de la factura o documento equivalente autorizados ocurran ajustes que disminuyan, anulen o rescindan operaciones que modifiquen las contenidas en los documentos expedidos inicialmente de acuerdo al artículo 111 del Código Tributario, los contribuyentes deberán anotarlos en el libro de ventas a consumidores en el mes en que ello ocurra, restando los valores que correspondan a tales ajustes de las demás operaciones relativas a dicho mes y registrar la factura que modifica la operación inicial. Los referidos ajustes al débito fiscal deberán realizarse dentro del plazo establecido en el Código Tributario.

2.6 Ley Régimen Especial de las facturas cambiarias y los recibos de las mismas

Art. 1: La factura cambiaria es el títulovalor que, en la compraventa de mercancías, y la prestación de servicios, el vendedor o prestador podrá librar y entregar o remitir al comprador y que incorpora un derecho de crédito sobre la totalidad o la parte insoluta del precio. El comprador o adquirente de los servicios estará obligado a devolver al vendedor o prestador, debidamente aceptada, la factura cambiaria original en las condiciones establecidas en la presente ley. No se podrá librar factura cambiaria que no corresponda a una entrega real o simbólica de mercaderías vendidas o a un servicio efectivamente prestado.

Art. 4: La Factura Cambiaria deberá contener:

1. El nombre de la Factura Cambiaria;
2. La fecha y el lugar de la emisión;
3. Las prestaciones y derechos que incorpora, entre otros: plazo para su pago e intereses por falta de pago;
4. El lugar de cumplimiento o ejercicio de los mismos;
5. La firma del emisor;
6. El número de orden del título librado;
7. El nombre y domicilio del comprador;
8. La denominación y características principales de las mercaderías vendidas o los servicios prestados;
9. El precio unitario y el precio total de las mismas;
10. La fecha o número de días en que se efectuara el pago.

La omisión de cualquiera de los requisitos de los ordinales anteriores, no afectará la validez del negocio jurídico que dio origen a la factura cambiaria, pero ésta perderá su calidad de títulovalor.

La falta de plazo o de fecha de pago estipulada en el numera X de éste artículo, se presumirá que ha sido emitido a 30 días plazo a partir de la fecha de emisión.

Art. 5: Cuando el pago se haya pactado en abonos, la factura deberá contener, en adición a los requisitos expuestos en el artículo anterior:

1. El número de abonos;
2. La fecha de vencimiento de los mismos;
3. El monto de cada uno.

Los pagos parciales se harán constar en la misma factura, indicando, asimismo, la fecha en que fueron hechos. Si el interesado lo pide, se le podrá extender constancia por separado.

Art. 6: La factura podrá ser enviada por el emisor al comprador o adquirente, directamente, o por intermedio de bancos, financieras o tercera persona. De utilizarse intermediarios, éstos deberán presentar la factura al comprador o adquirente para su aceptación y devolverla, una vez firmada por éste, o conservarla en su poder hasta el momento de la presentación para el pago, según las instrucciones que reciban del vendedor o prestador de los servicios. Si la factura no acompañare las mercancías o documentos representativos de éstas, deberá ser enviada por el vendedor en un término no mayor de tres días al de su libramiento, que nunca podrá exceder en cuarenta y ocho horas al de la entrega o despacho de las mercancías o prestación de los servicios, cualquiera que sea primero.

Art. 7: Si el vendedor o prestador de los servicios enviare la factura cambiaría por correo, deberá hacerlo por correo certificado con aviso de recepción, en el cual se indicará:

1. Que el envío contiene facturas;
2. Que el aviso de recepción deberá ser devuelto por correo.

Art. 8: Si el vendedor o prestador enviare la factura por otra vía y el comprador no la aceptare inmediatamente, éste queda obligado a firmar en el mismo acto un recibo o "quedan" que utilizará el vendedor o prestador como comprobante de entrega de la factura cambiaria. En el mencionado recibo o "quedan" deberá constar la fecha de la recepción, el nombre del comprador o adquirente de los servicios, el monto de las facturas entregadas y el nombre y empleo o cargo de la persona facultada para recibirlas y la firma autógrafa de dicha persona.

La firma del receptor de las facturas se presume auténtica a menos de probarse por el comprador o adquirente de los servicios, que la firma es falsa o que la persona suscriptora, en la fecha que consta en el recibo o "quedan", no trabajaba a sus órdenes.

Art. 9: El comprador o adquirente deberá devolver al vendedor o prestador la factura cambiaria, aceptada:

1. Al día siguiente de su recibo, si la operación se ejecuta en la misma plaza;
2. Dentro de un término de cinco días a contar de la fecha de su recibo, si la operación se realiza en diferente plaza.

Art. 15: Los comerciantes deberán conservar ordenadamente, por el término que la ley señale, las facturas cambiarias que hubieren librado o copias de las mismas, o bien conservarlas mediante copias hechas en microfotografía o en cualquier otro sistema tecnológico apropiado.

3 Herramientas criptográficas

En el presente capítulo se muestra una descripción general de algoritmos y herramientas criptográficas, con el propósito de sentar bases conceptuales que permitan entender el funcionamiento del protocolo para facturas electrónicas propuesto.

3.1 Criptografía

El termino Criptografía proviene de los vocablos griegos: κρύπτος (criptos), que significa "oculto" (también podría interpretarse como "escondido"), y el termino γραφη (grafé), que significa "escritura", lo que nos lleva a una traducción de forma literal de: "escritura oculta".

Profundizando un poco más en su significado, se describe a la Criptografía como la ciencia o el arte de escribir en un lenguaje previamente convenido o acordado mediante el uso de claves.

En un primer plano pareciera que el propósito de esta ciencia es la protección de los datos de personas no autorizadas a tener acceso a éstos. Sin embargo, la Criptografía es más allá que solo "ocultar" información ya que está relacionada con procesos que permiten conservar la integridad, confidencialidad y autenticación de la información y a su vez, garantizar la identidad de quienes intervienen en el proceso de la comunicación o intercambio de información. En resumen, la criptografía es fundamental para garantizar los 5 principios de la seguridad de la información [5, 6]:

a. ***Integridad:*** Avala que la información recibida no ha sido alterada y por lo tanto es idéntica a la que fue enviada por el emisor. Si este principio es violentado se puede identificar la manipulación y/o modificación del documento,
b. ***Confidencialidad:*** Un documento o mensaje es confidencial si y solo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada,
c. ***Autenticación:*** Permite verificar el contenido, así como la identidad del emisor y del receptor,
d. ***No repudio:*** El emisor no podrá negar la generación o envío de la información,
e. ***Control de Acceso:*** Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran.

3.2 Criptosistema

Un criptosistema está compuesto por 5 elementos que se describen a continuación [6]:

- ***m****:* Representa el conjunto de todos los mensajes sin cifrar o texto claro que desean enviarse,
- ***C****:* Representa el conjunto de todos los posibles mensajes cifrados, o criptogramas,
- ***k*****:** Representa el conjunto de claves que se pueden emplear en el criptosistema,
- ***E****:* Es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de m para obtener un elemento de C. Existe una transformación diferente E_k para cada valor posible de la clave *k*,
- ***D****:* Es el conjunto de transformaciones de descifrado, análogo a *E*.

Todo criptosistema ha de cumplir la siguiente condición:

$$D_k(E_k(m)) = m$$

Es decir, que si tenemos un mensaje ***m***, lo ciframos empleando la clave ***k*** y luego lo desciframos empleando la misma clave, obtenemos de nuevo el mensaje original ***m.*** Existen dos tipos fundamentales de criptosistemas:

1. Criptosistema simétrico o de llave privada,

2. Criptosistema asimétrico o de llave pública.

3.3 Criptosistema simétrico o de llave privada

Se definen de esta manera a aquellos sistemas que tanto en su algoritmo de cifrado como el algoritmo de descifrado utilizan la misma clave *k*. Debido a su funcionamiento presentan el inconveniente de que para ser utilizados, la clave *k* debe ser conocida tanto por el emisor como por el receptor. Por lo anterior es importante que la clave sea transmitida de manera segura [6]. La Figura 1 muestra de forma general el funcionamiento de los criptosistemas de llave privada.

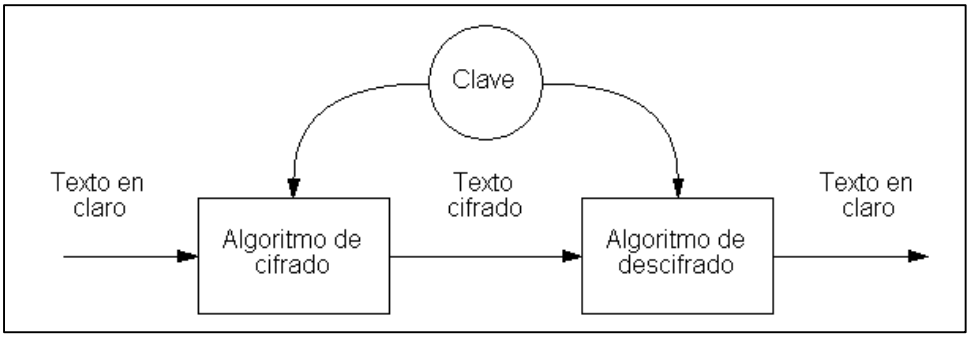


Figura 1: Criptosistema de Llave privada

3.4 Criptosistema asimétrico o de llave pública

En el artículo denominado "New Directions in Cryptography", publicado en Noviembre de 1976 por Whitfield Diffie y Martin E. Hellman, desarrollan el concepto de Criptografía de Llave Pública, en el contexto de un criptosistema, el cual consiste básicamente en un sistema que emplea una pareja de llaves que pertenecen a la misma persona. Una de las llaves es de dominio público y cualquiera puede tenerla y la otra llave es privada [7,8].

La Figura 2 muestra el funcionamiento de este sistema. El remitente usa la llave pública del destinatario y sólo con la clave privada se podrá descifrar el mensaje. De esta forma se consigue que sólo el destinatario pueda acceder a la información. De la misma forma si el propietario usa su clave privada para cifrar un mensaje sólo se podrá descifrar con la clave pública. Al usar la llave privada se comprueba y garantiza la identidad ya que pertenece y es conocida solo por su dueño.

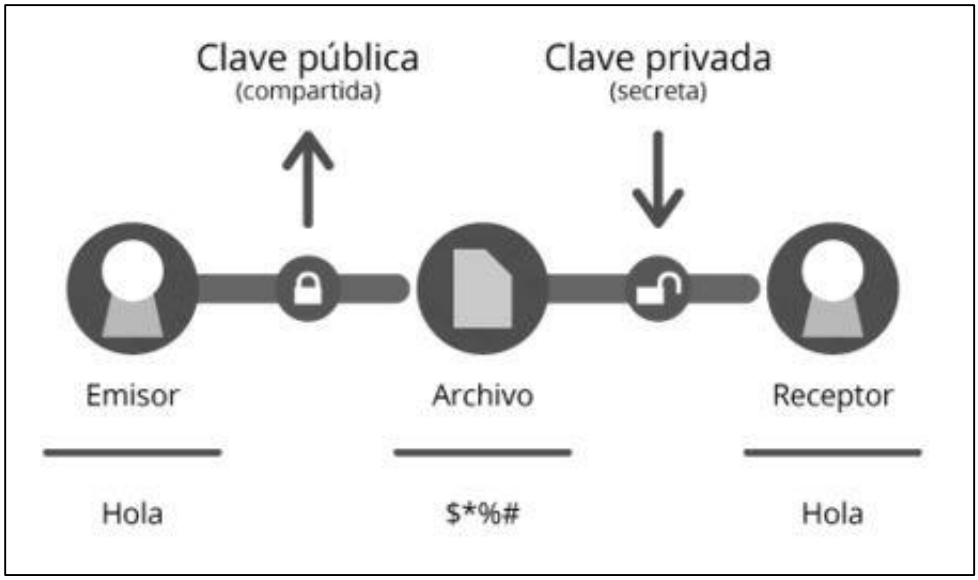


Figura 2: Criptosistema de Llave pública

3.4.1 Función Hash o picadillo

Las funciones hash o también conocidas como funciones de resumen o picadillo son algoritmos que tomando como entrada un texto, una contraseña o un archivo la función genera una salida alfanumérica de longitud fija que representa un resumen de toda la información que se le ha dado. A partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos [9, 10].

Estas funciones se utilizan para muchos propósitos, entre ellos está asegurar que no se ha modificado un archivo en una transmisión, hacer ilegible una contraseña o firmar digitalmente un documento. En el sistema presentado en este documento se utiliza la función Hash SHA256 y MD5.

Una función Hash SHA256 es un hash de 64 dígitos hexadecimales casi único, de un tamaño fijo de 256 bits (32 bytes). Y el MD5 es un algoritmo que toma como entrada un mensaje de longitud arbitraria y sin importar cuál sea esta longitud siempre produce una salida de 128 bits que representa un mensaje resumen o extracto del original.

3.4.2 Firma digital

Es una herramienta criptográfica que por medio de la función Hash, permite garantizar el origen o autoría e integridad de los documentos digitales, permitiendo así que dichos documentos posean una característica que, hasta el surgimiento de esta firma, era exclusiva de documentos físicos [11, 12, 13].

La firma digital relaciona el documento firmado con información propia del firmante, y permiten que terceras partes puedan reconocer la identidad del firmante y asegurarse de que los contenidos no han sido modificados.

El firmante genera, mediante una función matemática, una huella digital del mensaje, la cual se cifra con la clave privada del firmante. El resultado es lo que se denomina firma digital, que se enviará adjunta al mensaje original. De esta manera el firmante adjuntará al documento una marca que es única para dicho documento y que sólo él es capaz de producir.

Para realizar la verificación del mensaje, en primer término el receptor generará la huella digital del mensaje recibido, luego descifrará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que no hubo alteración y que el firmante es quien dice ser.

No se debe pensar entonces que la firma digital permite garantizar la confidencialidad del mensaje; un documento firmado digitalmente puede ser visualizado por otras personas.

3.4.3 Certificado Digital

Consiste en un documento digital que garantiza la relación entre una clave pública y un individuo o entidad. De este modo, permite verificar que una clave pública pertenece a un individuo determinado. Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona [14, 15].

El certificado contiene una clave pública y un nombre. Generalmente también cuenta con una fecha de expiración, el nombre de la Autoridad Certificante que la emitió. Pero lo más importante es que el certificado propiamente dicho está firmado digitalmente por el emisor del mismo.

4 Funcionalidad del sistema

Una factura es el comprobante mercantil que toda empresa o persona está obligada a entregar al momento de hacer entrega de un producto, bien, o servicio, siendo la persona natural o jurídica el emisor o receptor. En El Salvador el Código Tributario es la ley que especifica lo campos que toda factura emitida por empresas o personas dentro del territorio salvadoreño deben entregar como constancia de un producto, bien, o servicios cobrados a las personas naturales o jurídicas. Dentro de este documento llamada factura se deben detallar montos, cantidades, impuestos y demás campos requeridos por dicho código.

4.1 Análisis de requerimientos

El Articulo 114 detalla los campos mínimos que toda factura debe poseer, para que sea considerada válida en el marco de la ley de El Salvador. Por lo tanto, la información que debe contener la factura electrónica son los siguientes.

Datos de la Factura

a) Número de la factura: número identificador único para cada factura,
b) Fecha de Expedición: fecha en que se emitió la factura,
c) Fecha de operación: fecha en que se entregan los bienes o servicios cuando sea posterior a la emisión de la factura,
d) Número Correlativo de documento: números correlativos autorizados por la administración tributaria así como la serie cuando corresponda,
e) Resolución de autorización: número de la resolución otorgado por la administración tributaria donde se autoriza la serie de documentos a ser emitidos junto a la fecha de autorización. Estos datos deben ir impresos dentro de la factura.

Datos del Emisor

En este apartado deben incluirse los datos del contribuyente emisor de la factura, sea persona Natural o Jurídica, la información que debe estar presente es:

a) Nombre,
b) Denominación,
c) Razón social,
d) Giro o actividad comercial,
e) Dirección del establecimiento, oficinas y de las sucursales de existir,
f) Número de Identificación Tributaria (NIT),
g) Número de Registro de contribuyente (NRC).

Datos del Adquiriente

Es la información de la persona natural o jurídica que adquiere los bienes o servicios, para el caso de la factura:

a) Nombre del adquiriente,
b) Denominación (para factura con crédito fiscal),
c) Razón Social (para factura con crédito fiscal),
d) Giro o actividad comercial (para factura con crédito fiscal),
e) Dirección,
f) Número de Identificación Tributaria (NIT) (para factura con crédito fiscal),
g) Número de Registro de Contribuyente (NRC) (para factura con crédito fiscal).

Importes

Detalles de los cargos en impuesto y/o retenciones que se hacen, en cumplimiento del Código Tributario, como son:

a) 13% en concepto de IVA, sobre el monto de la venta,
b) 1% de retención de renta.

Conceptos de la factura

Apartado en donde se debe describir los bienes y/o servicios, las características que permitan individualizarlos e identificarlos plenamente. La información a ser colocada en este apartado es:

a) Cantidad,
b) Descripción,
c) Precio Unitario,
d) Monto total,
e) Operaciones grabadas,
f) Ventas exentas,
g) Ventas no sujetas,
h) Condiciones de las operaciones (al contado, al crédito, puesto en bodega, etc.).

Cuando las operaciones superan los $200 en venta se debe detallar lo siguiente:

a) Nombre, DUI y NIT persona que entrega,
b) Nombre, DUI y NIT persona que recibe.

Facturas para consumidores finales son documentos a emitir a no contribuyentes del impuesto o consumidores finales. Estos documentos deben cumplir con los siguientes requisitos:

1. Datos del Emisor

En este apartado deben incluirse los datos del contribuyente emisor de la factura, sea persona Natural o Jurídica, la información que debe estar presentes son:

a) Nombre,
b) Denominación,
c) Razón Social,
d) Giro o actividad comercial,
e) Dirección del establecimiento, oficinas y de las sucursales de existir,
f) Número de Identificación Tributaria (NIT),
g) Número de Registro de Contribuyente (NRC).

2. Datos del Adquiriente

Es la información de la persona natural o jurídica que adquiere los bienes o servicios, para el caso de la factura se requiere el Nombre y la dirección del adquiriente.

3. Importes

Detalles de los cargos en impuesto y/o retenciones que se hacen, en cumplimiento del Código Tributario, como son:

a) 13% en concepto de IVA, sobre el monto de la venta,
b) 1% de retención de renta.

4. Conceptos de la factura

Apartado en donde se debe describir los bienes y/o servicios, las características que permitan individualizarlos e identificarlos plenamente. Información a ser colocada en este apartado.

a) Cantidad,
b) Descripción,
c) Precio unitario,
d) Monto total,
e) Operaciones grabadas,
f) Ventas exentas,
g) Ventas no sujetas,
h) Condiciones de las operaciones (al contado, al Crédito, puesto en bodega, etc.).

Cuando las operaciones superan los $200 en venta se debe detallar lo siguiente:

a) Nombre, DUI o NIT persona que entrega, denominación o razón social,
b) Para Extranjeros número de Pasaporte o Carnet de Residencia.

La Figura 3, muestra el modelo de la factura electrónica.

4.2 Generación de la factura digital

A continuación se describe la secuencia para generar una factura digital, de acuerdo a la Figura 4.

1. El Emisor ingresa datos que serán procesados por SEFE: Emisor, Receptor y detalle de facturación.
2. SEFE crea una cadena de caracteres con la información mínima que toda factura debe llevar para crear un sello y será agregado como contenido en la factura
3. SEFE crea una factura digital sin firmar y se coloca en un medio de almacenamiento con formato PDF.
4. El emisor firmar una factura seleccionando el archivo PDF desde un medio de almacenamiento.
5. SEFE estampa una firma digital en el documento utilizando una llave privada ubicada en un almacén de llaves.
6. SEFE almacena la factura en un medio compartido.
7. El Receptor de la factura, accede a un medio compartido para obtener la factura firmada.
8. El Receptor valida la firma utilizando un certificado digital del Emisor.

Empresa S.A de C.V
Servicios de Consultorías y Asesoramiento
Av Las Capillas, # 120, San Salvador, San Salvador, El Salvador.
Telf: 22500000, Telf Fax: 22505050

Comprobante de Crédito Fiscal Digital
N° 000001
Correlativo autorizado N° 15DS000-10000 hasta 15DS000-99999
NIT: 1111-111111-111-1
NRC:10000-1

Crédito Fiscal.

Cliente:_____
Dirección:_____
_____
Departamento:_____
_____

Fecha:_____
N° Registro:_____
NIT:_____
Giro:_____
Condiciones de Pago:_____

Cantidad	Descripción	Precio Unitario	Ventas Exentas	Ventas Afectadas
Cuando monto excede $11,428.58		Sumas		
Firma Digital Entrega Producto	Firma Digital Recibe Producto	IVA		
		Sub-Total		
		(-) IVA Retenido		
		Ventas Excentas		
		Venta Total		

Cadena Original

Cadena Original: en este apartado se colocara todos los datos que forman el cuerpo de la factura, los campos que se rellena y la información que por ley debe ser contenida, estos datos pasaran a formar la Cadena Original para el cálculo del Hash

Sello Digital

Hash, que se obtendrá con los datos de la cadena Original más el certificado

Figura 3: Modelo de factura digital

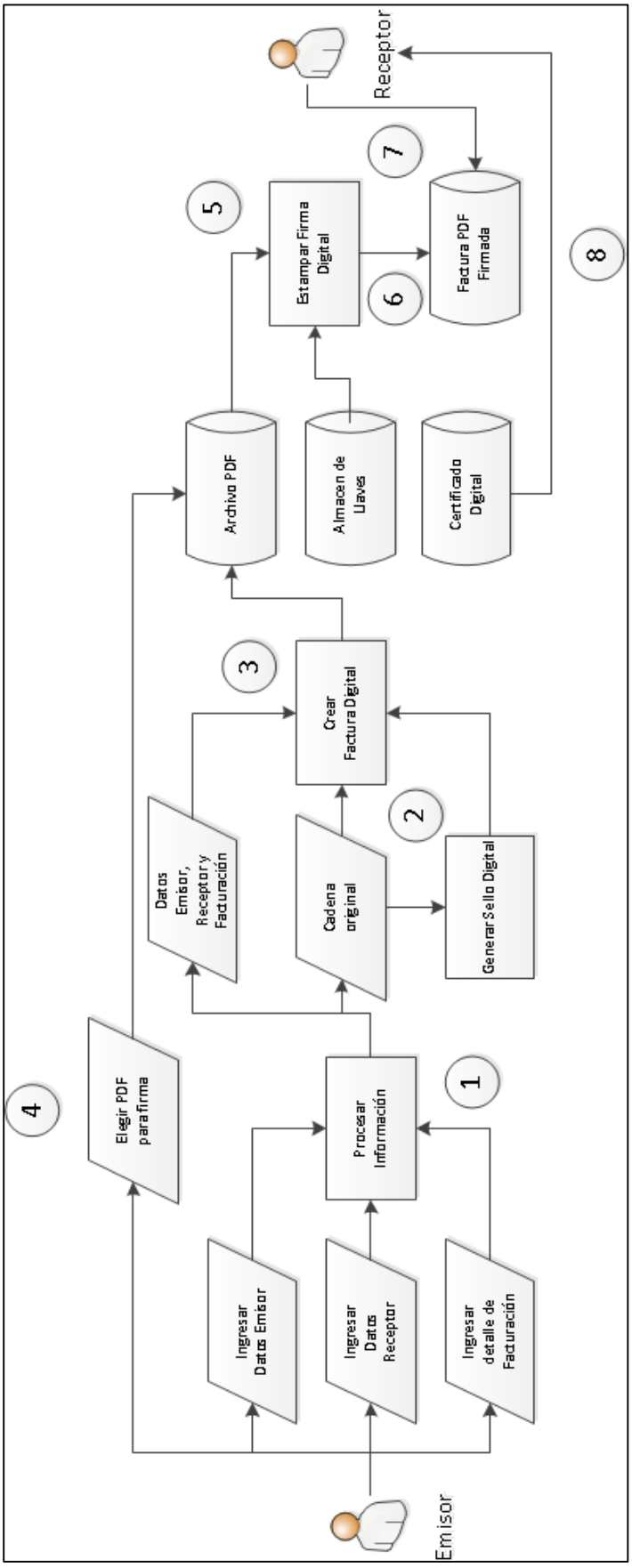


Figura 4: Proceso de generación de factura digital

El proceso de firma digital y verificación de la firma de presentan en la Figura 5.

Proceso de generación de factura electrónica:
Entidades: emisor, sistema, factura

1. A través de un formulario, el emisor ingresa datos del emisor, los datos del receptor y los detalles de facturación.
2. Cuando el emisor termine el ingreso de datos, el sistema realizará lo siguiente:
    a. Extraer la información del formulario:
        i. Datos del Emisor
        ii. Datos de Receptor
        iii. Detalle de facturación
    b. Los datos del literal (a) serán concatenados en una cadena separadas por pipes (|).
    c. Con la cadena generada en el literal (b), creará un digesto utilizando funciones hash y será agregado como parte del contenido de la factura.
    d. Con el digesto generado en el literal (c), será adicionado como parte del contenido de la factura.
    e. La información de los literales (c) y (d) serán visible en la versión de impresión de la factura.
    f. Se creará un archivo digital en formatos PDF con el contenido de los literales anteriores.
3. Con el archivo digital PDF generado en el literal 2, se creará un digesto de todo el archivo PDF y en conjunto con la llave privada del emisor se firma el documento.

Verificación de factura electrónica
Entidades: receptor, sistema, factura.

1. El receptor carga al sistema con un archivo PDF.
2. El sistema carga el archivo PDF firmado, y realizará los procesos siguientes:
    a. Extraer el contenido de la factura.
    b. Generar el digesto de la cadena del literal (a)
    c. Extraer la firma digital del documento.
    d. Extraer el digesto de la firma usando certificado digital del emisor.
    e. Comparar los digestos de los literales (a) y (d)

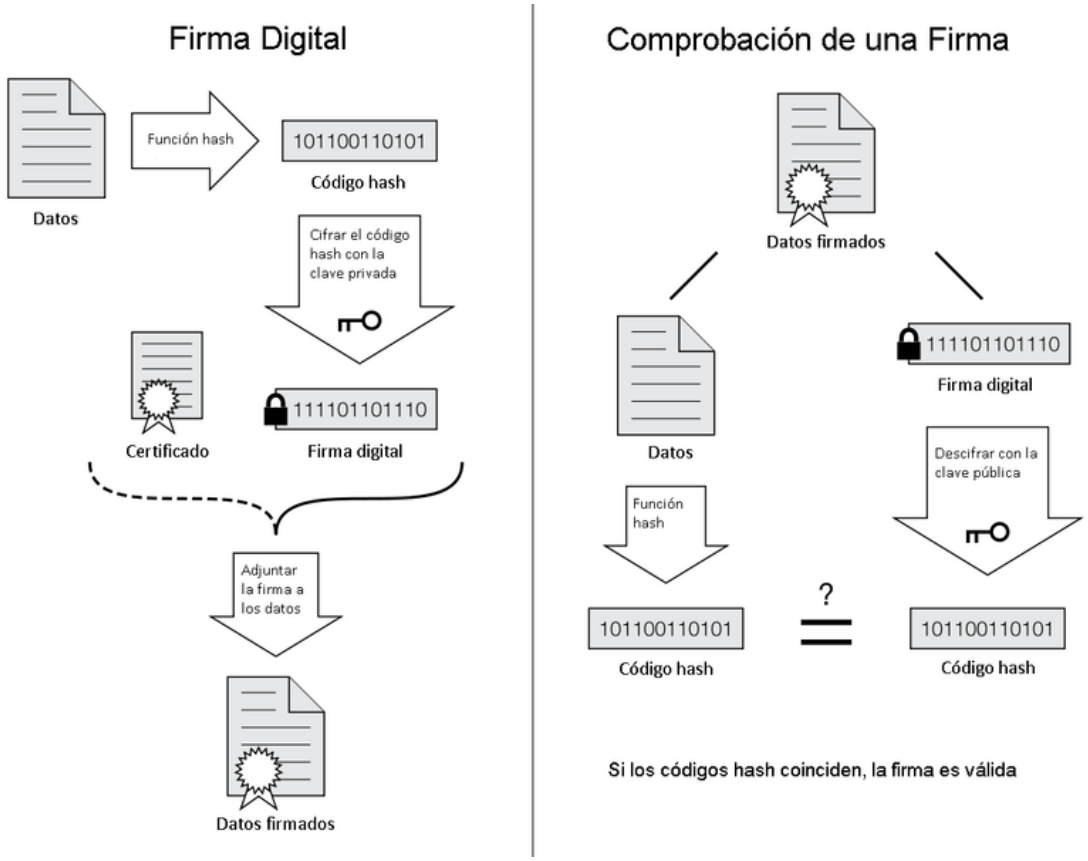


Figura 5: Firma digital y comprobación de la misma

4.3 Protocolo entre el emisor y el receptor

Notación:

$(m_1 \| m_2 \| m_3)$: Datos emisor, Datos receptor, Detalle facturación

S_k = procedimiento de firma digital usando la llave privada k,
V_p=verificación de firma digital usando la llave pública p,
CA = certificado digital de la autoridad emisora.
MD5= Message-Digest Algorithm 5
SHA256= Secure Hash Algorithm de 256 bits
||= Concatenación de variables

Emisor

1. $m_4 = (m_1 + m_2 + m_3)$
2. $m_5 = MD5(m_4)$
3. $Factura\_Digital = (m_1 + m_2 + m_3 + m_4)$
4. $h_1 = SHA256(Factura\_Digital)$

5. $Firma\_Digital = S_k(h_1)$
6. $Factura\_Digital\_Firmada = (Firma\_Digital + CA + Factura\_Digital)$
7. $\{Factura\_Digital\_Firmada\} \rightarrow \text{Re}ceptor$

Receptor (Factura_Digital_Firmada)

8. $h_2 = SHA256(Factura\_Digital)$
9. $h_3 = V_p(Firma\_Digital)$
10. Si $(h_2 = h_3)$

a. Firma digital válida
Sino
b. Firma digital inválida

El uso de Hash MD5, es con la finalidad de proteger la integridad de los datos de la factura, debido que se aplica al resultado de la concatenación de, los Datos del Emisor, Datos del Receptor y Detalle de Facturación. A esto se denominamos Sello Digital.

La Hash SHA256, se utiliza para proteger la integridad de la factura digital como un todo donde se aplica el hash tanto a los Datos del Emisor, Datos del Receptor, detalle de Factura y al resultado del HASH MD5 que le hemos llamado sello digital

4.4 Análisis de seguridad

La factura electrónica es el documento que cumple los mismos requisitos de la factura expedida en papel, siempre y cuando se garantice su autenticidad e integridad, además de que el emisor no pueda negar su emisión y que el destinatario lo confirme. Un protocolo de emisión de factura electrónica debe cumplir los siguientes requisitos:

a) ***Integridad:*** Avala que la información con la que fue generada la factura ya está protegida. Asimismo, puede detectarse la manipulación y/o modificación del documento.
b) ***Autenticidad:*** Permite verificar el contenido, así como la identidad del emisor y del receptor.
c) ***No repudio:*** El emisor no podrá negar la generación por el uso de un certificado digital.

En el modelo de factura electrónica propuesto en el presente documento se generan en formato PDF los cuales, por medio de firmas electrónicas, certifican al creador del documento y además impide la falsificación del contenido, ya que, al ser modificado se produce una alerta.

Para firmar documentos de forma digital, lo primero es tener un certificado digital emitido por una entidad certificadora que pueda corroborar a un tercero que dicho certificado es válido y

corresponde a la persona que identifica. El alcance del presente proyecto es proponer un protocolo de firma segura por lo que, a manera de propuesta, se recomienda que La Superintendencia General de Electricidad y Telecomunicaciones (SIGET), institución autónoma sin fines de lucro con atribuciones para aplicar las normas contenidas en tratados internacionales sobre electricidad y telecomunicaciones vigentes en El Salvador, realice las funciones de entidad certificadora.

5 Sistema Emisor de Factura Electrónica

El propósito de los capítulos anteriores es brindar las bases teóricas para la comprensión de los elementos que debe contener una factura digital considerando su formato, contenido y elementos criptográficos que deben ser integrados para ser considerado un documento digital legal, valido y seguro. En este capítulo se desarrolla un prototipo de Sistema Emisor de Factura Electrónica, en adelante denominado SEFE. El propósito de esta implementación es llevar a la práctica el protocolo que se ha definido para generar una factura digital utilizando tecnología de software disponible y que sirva como versión inicial para que se desarrolle un sistema completo. Para realizar la implementación se utilizó información de las siguientes referencias [16-25]

SEFE utiliza Java Estándar Edition (SE) versión 8 como lenguaje de programación orientado a objetos en conjunto con la plataforma Netbeans versión 8.0.2. Ambas tecnologías brindan una amplia gama de librerías, clases y herramientas necesarias para generar un producto de software funcional.

Para los componentes de seguridad se utiliza la librería BouncyCastle versión 1.51, es una colección de interfaces de programación de aplicaciones, conocidas por su siglas API de la palabra en inglés Application Program Interface, que cuentan con una amplia gama de algoritmos criptográficos.

Para el formato digital del archivo que contendrá la factura, SEFE utiliza el Portable Document Format o PDF. Para visualizar este tipo de formato se utiliza Adobe Reader versión 11 o superior. Para generar archivos PDF, SEFE utiliza las librerías iText version 5.5.3, iText es una biblioteca de código abierto para crear y manipular archivos PDF utilizado código Java.

5.1 Implementación.

En esta sección especificaremos con más detalle la etapa de diseño, se usara un lenguaje más técnico de lo que se requirió para la construcción de SEFE.

El marco de trabajo Netbeans provee una forma amigable de visualización de la estructura de clases y paquetes para que un desarrollador almacene los archivos necesarios para cualquier desarrollo de software bajo java.

Para SEFE se definió la siguiente estructura de clases y paquetes:

- ✓ Paquete sefe.udb.edu.sv: contenedor único de todas las clases definidas para el funcionamiento de SEFE,
- ✓ Clase Entidad: contiene todas las propiedades y métodos para procesar la entidad emisora y cliente. Contiene además los métodos para la generación de una cadena de texto que sirve de insumo para generar el sello digital,
- ✓ Clase Factura: contiene todas las propiedades y métodos para procesar la entidad Factura. Esta clase permite la manipulación de toda la información que debe contener el objeto factura, así como la manipulación del detalle de facturación,
- ✓ Clase DigestDefault: contiene los métodos para la generación de digestos (hash),
- ✓ Clase PDFProcesor: contiene las propiedades y método para la construcción de la factura digital con la estructura de contenido y formato digital definido en la etapa de diseño,
- ✓ Clase PDFSigner: contiene las propiedades y métodos para la manipulación de los componentes criptográficos requeridos por la factura digital: llave privada, certificados, archivo para firmar y destino de factura firmada,
- ✓ Clase PDFSign: contiene un único método que se encarga de firmar y estampar un sello en el contenido de la factura,
- ✓ Clase PDFProperties: contiene las propiedades y métodos para parametrizar valores definidos por el usuario emisor,
- ✓ Clase FormularioFacturacion: contiene las propiedades y métodos para generar una interfaz gráfica para que el emisor de la factura ingrese la información que SEFE debe procesar,
- ✓ Clase MainMenu: contiene las propiedades y métodos para generar una interfaz gráfica utilizada como menú principal de SEFE,
- ✓ Clase PDFFrontProperties: contiene las propiedades y métodos para generar una interfaz gráfica utilizada como pantalla de parametrización de SEFE,

La Figura 6 muestra el diagrama de clases de SEFE con las principales propiedades y métodos de cada una.

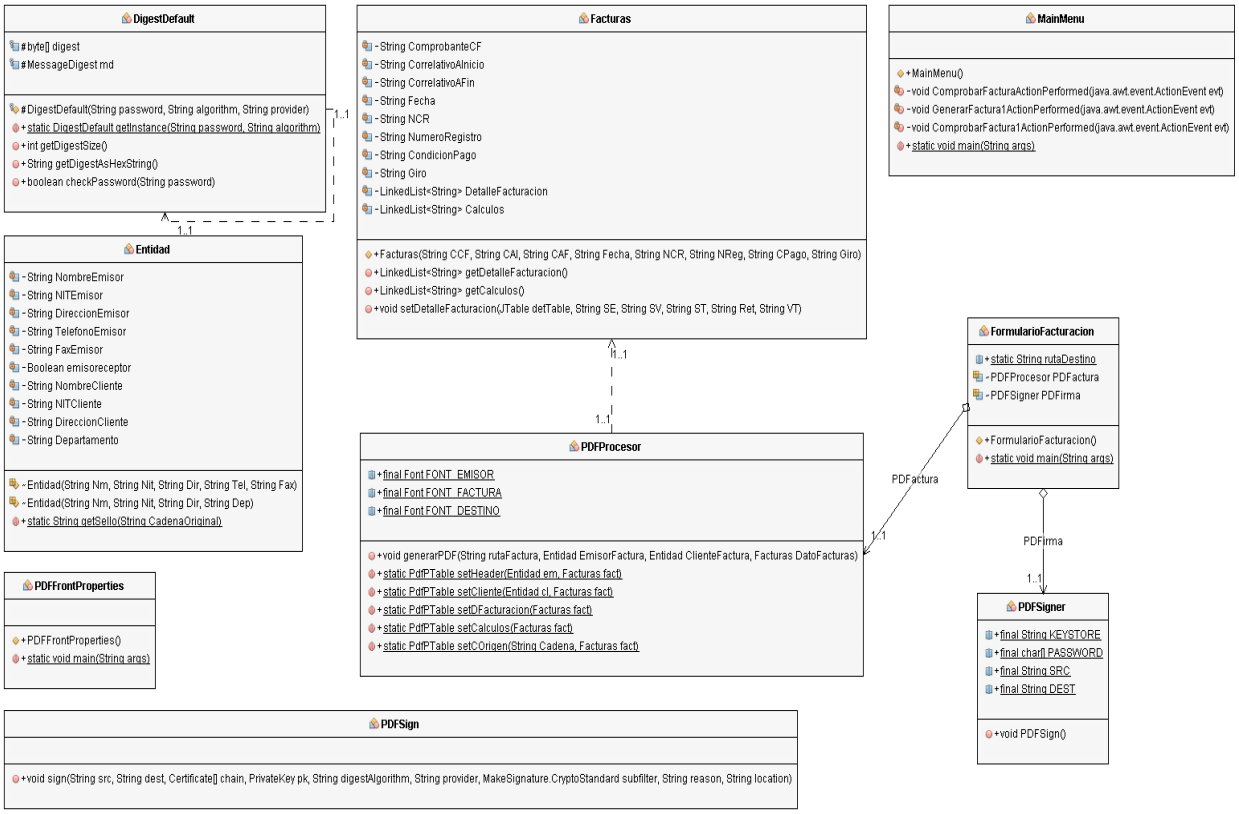


Figura 6: Diagrama de clases SEFE

Para que la entidad Emisor pueda ingresar los datos requeridos por el objeto Factura, SEFE presenta al emisor un menú principal como se muestra en la Figura 7 con tres opciones:

1. Generar Factura: se encarga de cargar el formulario con todos los campos requerido por la Factura y que el Emisor debe completar,
2. Firmar Factura: se encarga de cargar un formulario de selección de archivo con el propósito de firmarlo con componentes de infraestructura de llave pública,
3. Propiedades: se encarga de cargar un formulario para crear persistencia, a través de archivo planos, de datos relevantes para generar y firmar la factura digital.

Para generar el menú inicial se utilizó un marco (frame) de java, con la funcionalidad básica de una ventana de Windows, con tres botones (button).

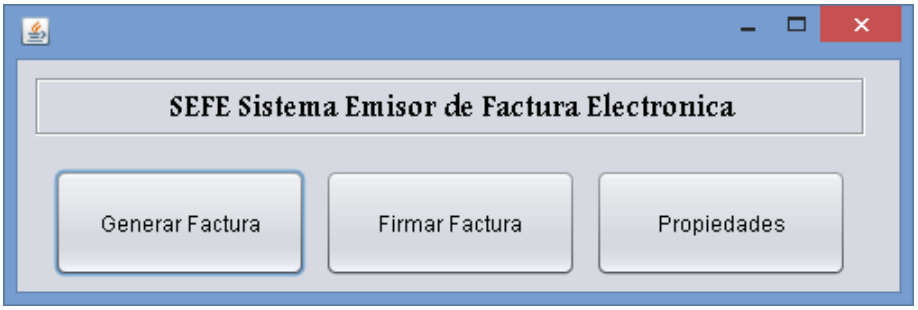


Figura 7: Menú Principal Sistema SEFE

SEFE muestra a la entidad Emisor un formulario de ingreso de datos que componen el objeto Factura. Este consiste en un marco (frame) de java, compuesto de una etiqueta (label) con el título del sistema, un panel separado por tabuladores con las diferentes categorías de los datos a ingresar y un botón que desencadena el procesamiento de los datos ingresados.

Las Figuras 8 y 9 muestran los componentes que fueron considerados en la construcción del formulario para el Emisor y los datos correctos a ingresar, respectivamente.

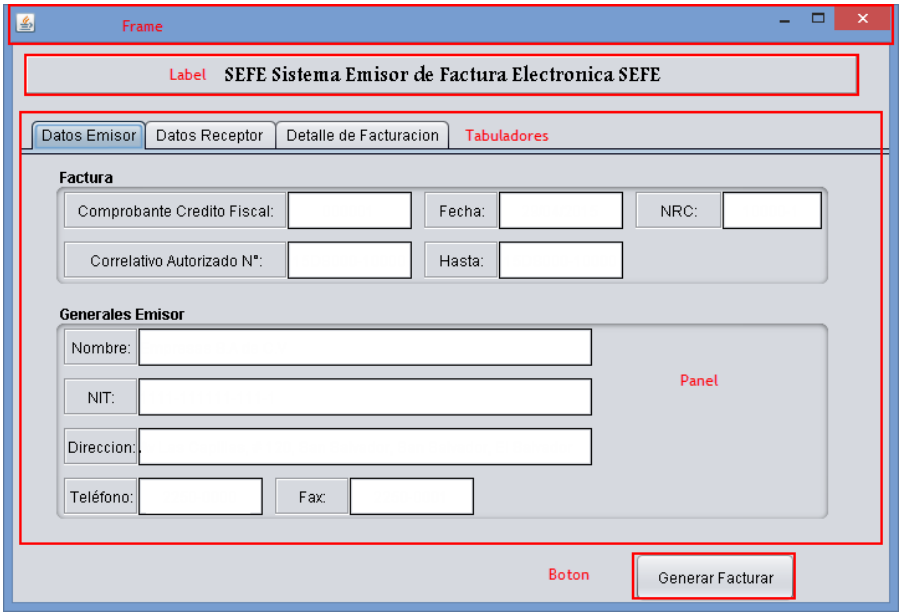


Figura 8: Formulario entidad Emisor

En los tabuladores, se categorizaron los datos a ingresar por el emisor en: Datos de Emisor, Datos Receptor y Detalle de Facturación.

1. Datos de Emisor: En la siguiente figura muestra los datos que serán ingresados bajo esta categoría:

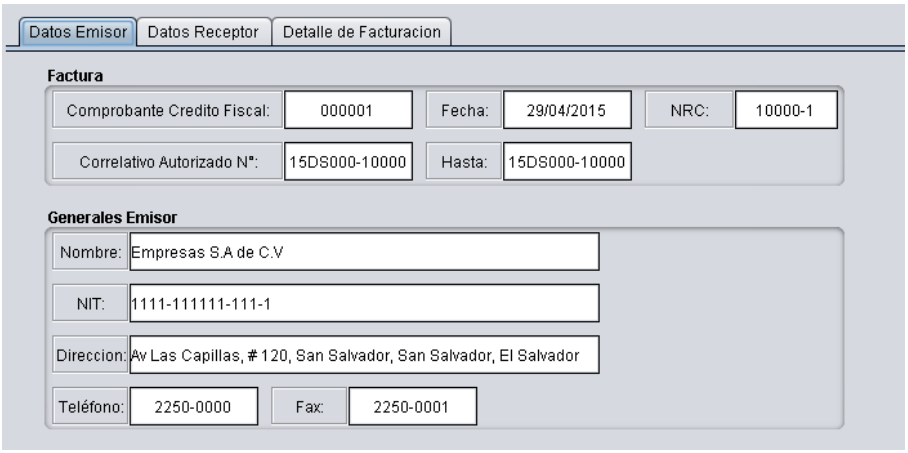


Figura 9: Formulario Datos del Emisor

En la sección Factura, se ingresa datos que forma parte de la información legal requerida por la factura. Los campos de Comprobante Crédito Fiscal, Correlativo Autorizado y NCR, son valores alfanuméricos que manualmente ingresa el emisor de la factura. El campo fecha, es un valor alfanumérico para la fecha de emisión en formato día-mes-año (dd-mm-yyyy) y se carga automáticamente.

En la sección Generales Emisor, se ingresa manualmente los datos relevantes concernientes al emisor tributario. Los campos Nombre, Número de Identificación Tributaria (NIT), Dirección, Teléfono y Fax, son valores alfanuméricos.

2. Datos de Receptor: Se muestra los datos que serán ingresados bajo esta categoría (veáse Figura 10):

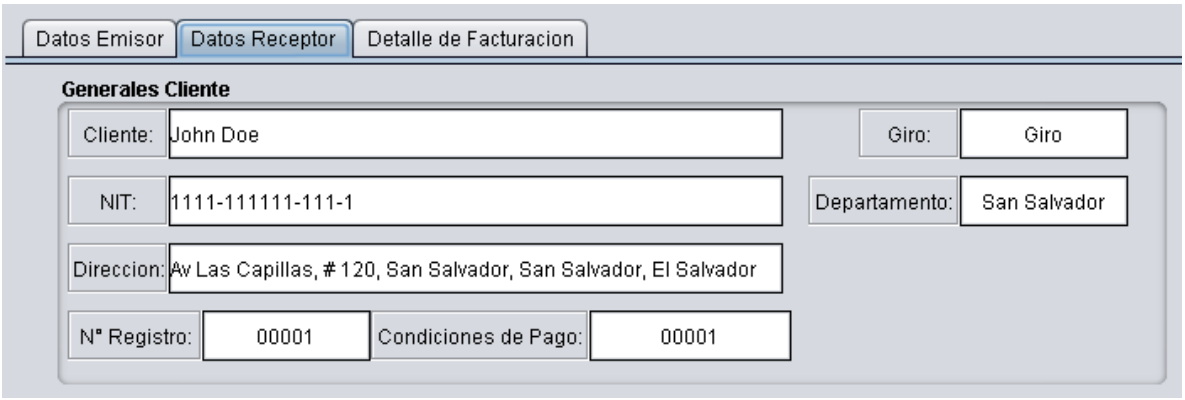


Figura 10: Formulario Datos del Receptor

En la sección Cliente, se ingresa manualmente los datos del obligado tributario (Cliente). Los campos Cliente, NIT (Número de Identificación Tributaria), Dirección, Departamento, Giro, Numero de Registro y Condiciones de Pago, son valores alfanuméricos.

3. Detalles de Facturación: Aquí se ingresan los ítems a facturar. En la sección Detalle Facturación, se ingresan los datos de todos los conceptos e importes de facturación. Se hace un ingreso manual en una tabla detallando: Cantidad, Descripción y Precio Unitario del producto el emisor entrega. Al final de cada línea, se realiza de manera automática el cálculo de la venta exenta y ventas afectas. Con los botones (+) y (-), se pueden adicionar o remover líneas para detallar o quitar productos. Una vez el emisor completa la tabla con todos los productos acordados a entregar, con el botón (=) se realiza los cálculos de manera automática del total de sumas exentas y afectas, sumándole los porcentajes de Impuesto al Valor Agregado (IVA) y Renta, finalizando con la Venta Total que es el equivalente al pago total que realizará el cliente.
   Cuando el emisor completa, verifica y acepta los datos ingresado en el formulario, debe indicarle a SEFE que proceda a procesar los datos del formulario para estructurarlos como información en una estructura de factura en formato digital. Esto lo realiza al presionar el botón "Generar Factura" (Figura 11).

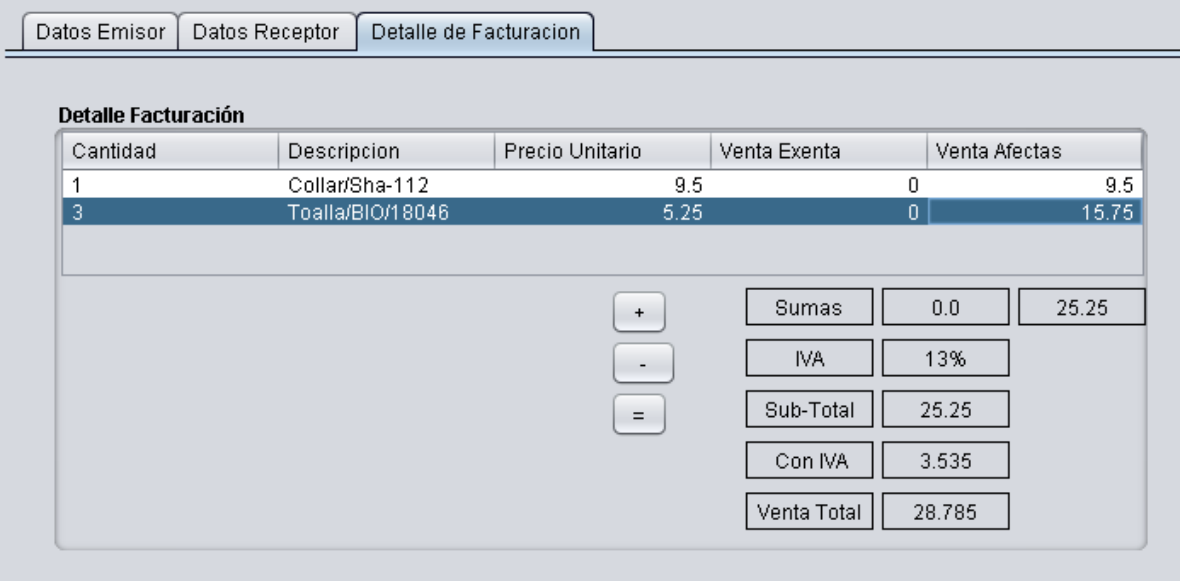


Figura 11: Formulario para detalle de la facturación

5.1.1 Proceso de Generar Factura

1. Cuando el emisor presiona el botón Generar Factura, se activa un evento que desencadena las siguientes acciones:
2. El emisor selecciona el nombre y ruta donde desea almacenar la factura. La extensión del archivo será PDF y automáticamente será asignado por SEFE.
3. Los datos del emisor son procesado por el objeto emisorFactura, instancia de la clase Entidad. Los datos del receptor son procesados por el objeto clienteFactura, también instancia de la clase Entidad. Los datos del emisor y receptor no son del todo similares, y

aunque son instancias de la misma clase, se definieron constructores diferentes para cada uno.

4. Los datos de la factura son procesados por el objeto Facturación, instancia de la clase Facturas. Para procesar el detalle de facturación, cálculo de retenciones y total de importes, dentro de la clase Facturas se definió una función llamada setDetalleFacturacion que se encarga de realizar los cálculos requeridos.
5. Con todos los datos procesado y almacenados por sus respectivos objetos. SEFE procede a generar la factura por medio de la función generarPDF utilizando el objeto PDFactura, instancia de la clase PDFProcesor. Esta función toma como insumos el nombre y ruta del archivo PDF, los objetos emisorFactura, clienteFactura y Facturacion.

En la creación de la factura, la clase PDFProcesor es la encargada de distribuir los datos en el archivo PDF con el formato de la factura establecido en la fase de diseño. Se utiliza el objeto facturapdf, instancia de la clase Document de la librería iText, para colocar las diferentes secciones en el orden establecido en la fase de diseño.

En la figura 12 se muestra la factura generada por SEFE y las diferentes secciones que forman parte de su construcción:

1. Esta sección es generada utilizando la función setHeader. En la sección de lado izquierdo se coloca el nombre, dirección, teléfonos del emisor de la factura. En la sección del lado derecho Comprobante de Crédito Fiscal, Numero Correlativo y NCR de la factura, además el Número de Identificación Tributaria del Emisor.

2. Esta sección es generada por la función setCliente, se coloca el nombre, dirección, departamento y número de identificación tributaria del cliente. El número de registro, giro y condición de pago es información concerniente a la factura.

3. Esta sección es generada por la función setDFacturacion, se coloca el listado de artículos con la cantidad, descripción, precio unitario, ventas exentas y ventas afectas que son entregados al cliente.

4. Esta sección es generada por la función setCalculos, donde estan los totales de las ventas exentas y afectas, además del cálculo de las retenciones. El final total será lo que el cliente acuerda pagar producto del intercambio de bien o servicio.

5. Estas secciones son generadas por la función setCOrigen, la cual es una secuencia de los siguientes datos:

    a. Nombre del Emisor
    b. Número de identificación tributaria del emisor
    c. Dirección
    d. Teléfono

e. Fax
f. Nombre del Cliente
g. Número de identificación tributaria del cliente
h. Dirección
i. Detalle de facturación
j. Cálculos.

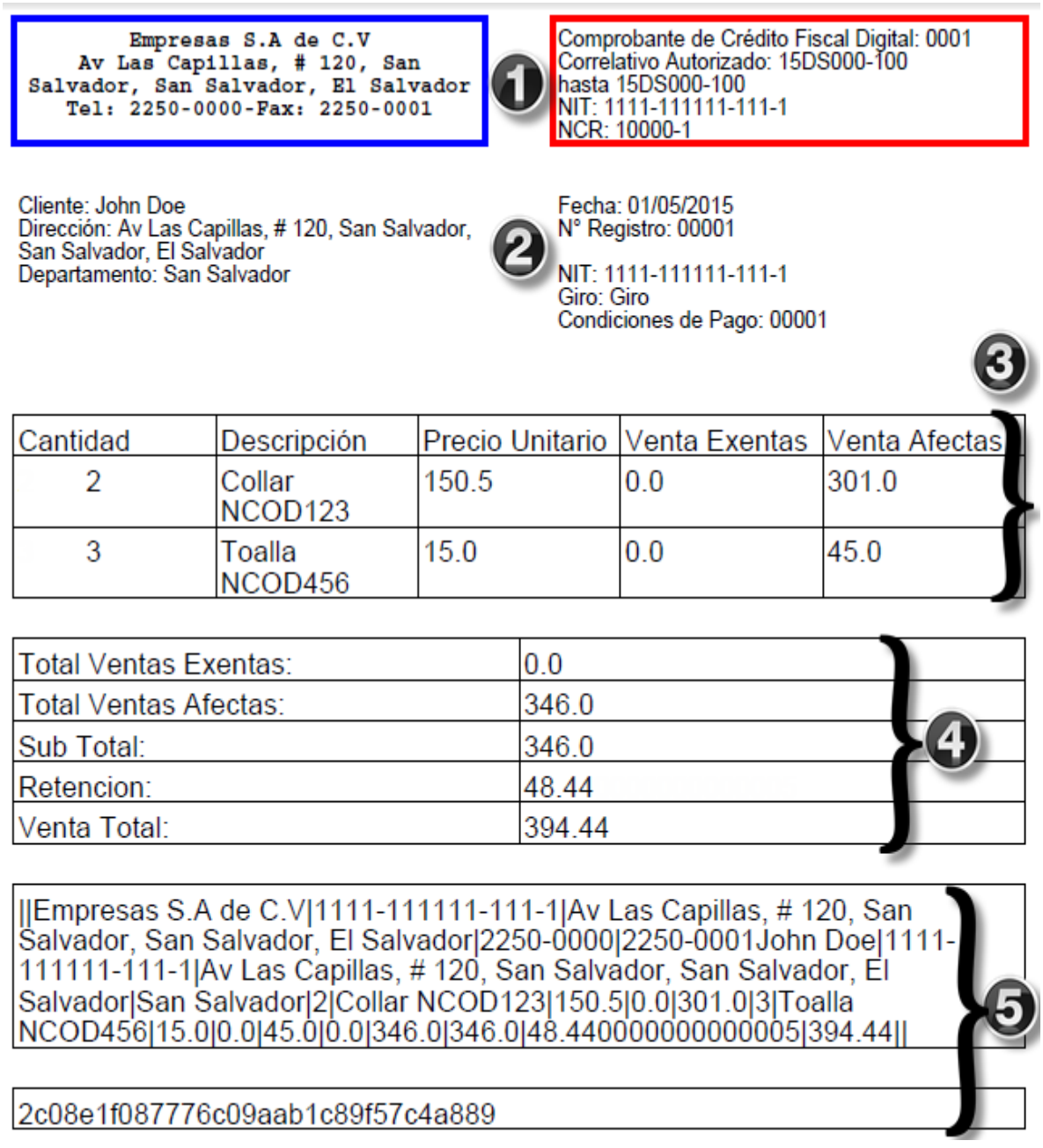


Figura 12: Ejemplo de factura generada en SEFE

Cada uno de ellos se encuentran separados por el carácter "|" (pipe), delimitando el inicio y el final de la cadena con un doble pipe "||". Con la cadena generada, se hace un digesto con MD5 con el propósito de generar un sello del contenido relevante de la factura en caso el receptor considera generar una versión impresa.

En las siguientes líneas de código se muestra todo el proceso de creación de factura.

```
1  Document facturapdf = new Document(PageSize.LETTER);
2                    PdfWriter.getInstance(facturapdf,          new
FileOutputStream(rutaFactura));
3  facturapdf.open();
4
5   // SEFE: Metadata de factura.
6   facturapdf.addTitle("Factura SV");
7   facturapdf.addAuthor("SEFE");
8   facturapdf.addSubject("Prototipo de Factura Electronica");
9   facturapdf.addKeywords("efactsv, iText, PDF");
10 facturapdf.addCreator(EmisorFactura.getNombreEmisor());
11
12  // SEFE: Secciones de factura.
13 facturapdf.add(setHeader(EmisorFactura,DatoFacturas));
14 facturapdf.add(setCliente(ClienteFactura,DatoFacturas));
15 facturapdf.add(setDFacturacion(DatoFacturas));
16 facturapdf.add(setCalculos(DatoFacturas));
17 facturapdf.add(setCOrigen(EmisorFactura.getCadenaEmisor() +
18 ClienteFactura.getCadenaEmisor(),DatoFacturas));
19
20 facturapdf.close();
```

Las líneas 6 – 10 agrega a la factura digital la información que sirve como metadata. A continuación se muestra como Acrobat Reader muestra esta información.

Para el emisor de la factura, con presionar el botón Firmar Factura, SEFE abre un cuadro de dialogo con un filtro de búsqueda tipo PDF donde el emisor localiza el archivo que desea firmar. La Figura 14 muestra la interfaz para generarla.

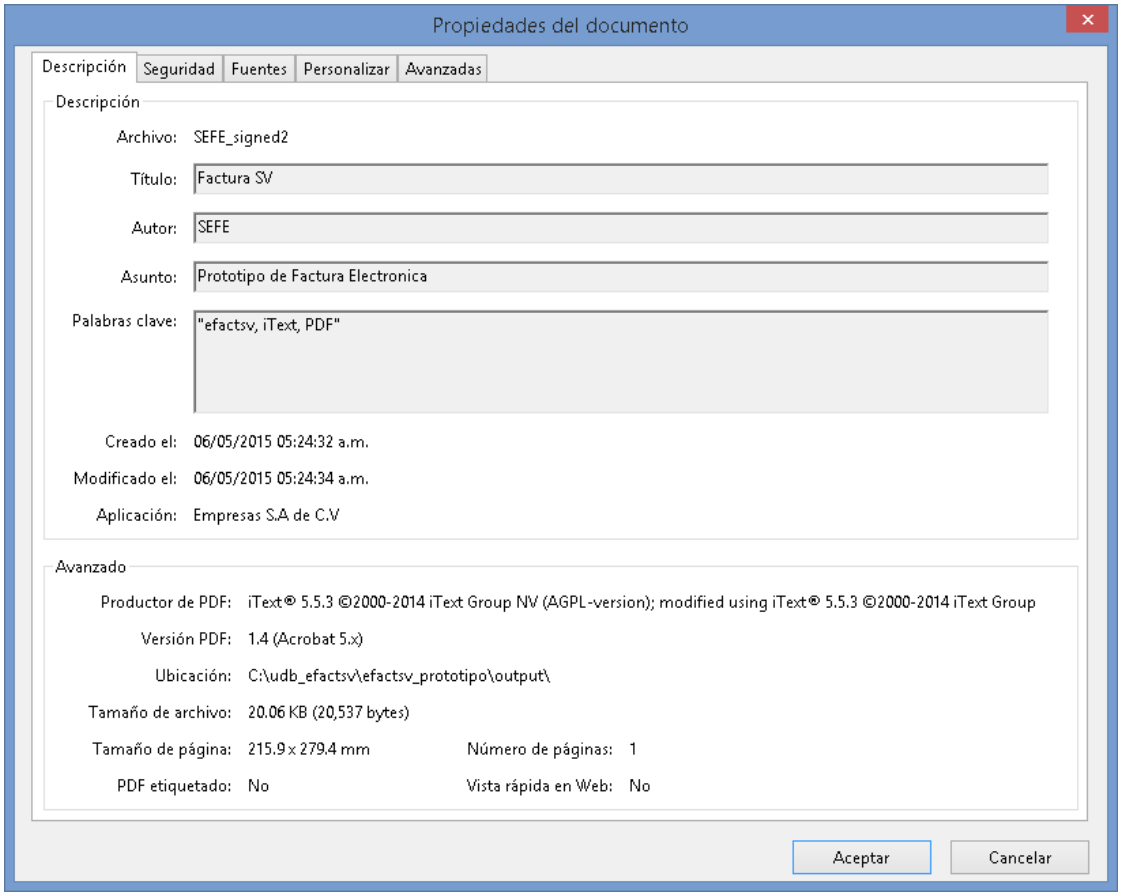


Figura 13: Opción Propiedades del Documento en Acrobat Reader

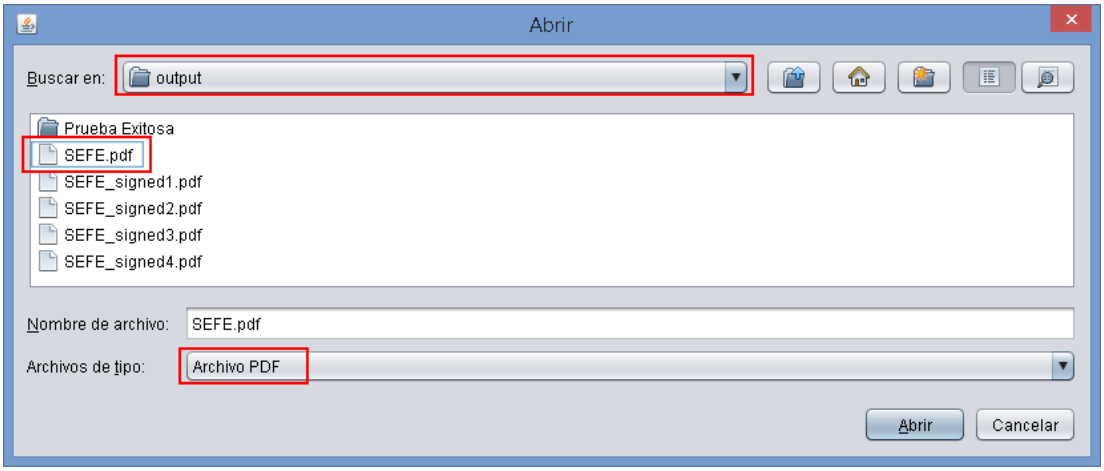


Figura 14: Opción para firma de factura digital

Especificado el archivo, SEFE crea un nuevo archivo con el contenido exacto de la factura especificada y agrega una estampa en la esquina superior izquierda que representa la firma digital del documento (Figura 15).

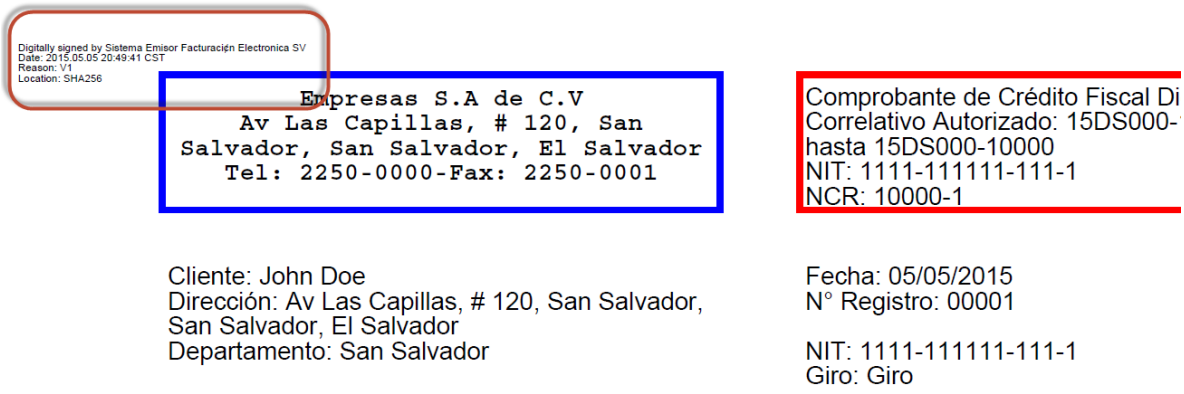


Figura 15: Factura con firma digital

El propósito de la firma es garantizar que la factura es segura por sí misma, SEFE garantiza las siguientes características de seguridad:

Integridad: cuando la factura es firmada y posteriormente se modifica la información, se emitirá una advertencia de que el contenido ha sido modificado.

Autenticidad y no repudio: para garantizar estas características, SEFE utiliza componentes de infraestructura de llave pública. Una llave privada ubicada en un almacén de llaves (keystore) que solo el emisor posee y una llave pública o certificado digital que será compartida con el receptor. El alcance de SEFE es a nivel de prototipo, por lo que se utiliza certificados autofirmados para realizar la verificación de la firma en un entorno controlado, caso contrario deberá considerarse una entidad certificadora que sirve de garante de la entidad del emisor.

5.1.2 Almacén de llaves

Para generar la llave privada se hará uso de keytool, una herramienta incluida en el kit de desarrollo de software (SDK) de Java. Keytool permite la creación de un almacén privado de llaves utilizando la línea de comandos. En el siguiente cuadro se muestra el comando utilizado para crear el almacén.

```
$ keytool -genkey -alias sefe_sv -keyalg RSA –keysize 2048 -keystore sefe_ks
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: Sistema Emisor Facturación Electronica SV
What is the name of your organizational unit?
[Unknown]: UDB
What is the name of your organization?
```

```
[Unknown]: UDB
What is the name of your City or Locality?
[Unknown]: SAN SALVADOR
What is the name of your State or Province?
[Unknown]: SAN SALVADOR
What is the two-letter country code for this unit?
[Unknown]: SV
Is CN= Sistema Emisor Facturación Electronica SV, OU=UDB, O=UDB, L=SAN SALVADOR, ST=SAN SALVADOR, C=SV correct?
[no]: yes
Enter key password for < sefe_sv >
(RETURN if same as keystore password):
```

Como resultado del proceso anterior se genera un almacén de llaves con el nombre de sefe_ks y un alias (con el mismo nombre) para referenciar a la llave privada, se utiliza una identidad genérica llamada Sistema Emisor Facturación Electrónica SV para propósito de pruebas, sin embargo es en este proceso que se especifica información del emisor de la factura. Para garantizar la seguridad del almacén de llaves, keytool solicita el ingreso de dos contraseñas, una para acceder al contenido del almacén de llaves y otra para almacén como tal.

Utilizando el entorno de IDE, es posible visualizar el contenido del almacén de llaves como se ve en la Figura 16:

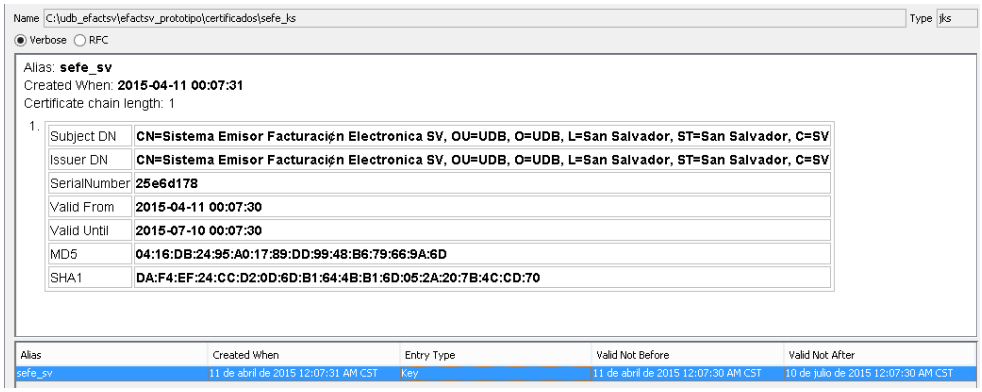


Figura 16: Almacén de llaves

Para generar la llave publica, haremos uso de certificados digitales. Este se genera con base al almacén de llaves creado por el emisor. El comando con keytool se muestra en el siguiente cuadro:

```
$ keytool -export -alias sefe_sv -file SEFESV.CER -keystore sefe_ks -storepass password
Certificate stored in file < SEFESV.CER >
```

Como resultado, se obtiene un archivo con el nombre SEFESV con extensión CER. Utilizando Adobe Reader es posible ver el contenido del certificado. Tanto el almacén de llaves como el certificado digital son componentes externos a SEFE, dentro de la codificación del sistema serán referenciados para firmar la factura digital.

Respecto a la firma digital, la clase PDFSigner es la encargada de firmar la factura, el objeto PDFirma instancia de esta clase se encarga de realizar esta tarea y requiere de insumo:

1. Ruta física donde se encuentra el almacén de llaves.
2. La contraseña del almacén de llaves.
3. Ruta física del archivo que de la factura que se desea firmar.
4. Ruta física destino de la factura firmada.

La función PDFSigner procesa la información en las siguientes líneas de código:

```
1 BouncyCastleProvider provider = new BouncyCastleProvider();
2 Security.addProvider(provider);
3                KeyStore                ks                =
KeyStore.getInstance(KeyStore.getDefaultType());
4 ks.load(new FileInputStream(KEYSTORE), PASSWORD);
5 String alias = (String)ks.aliases().nextElement();
6 PrivateKey pk = (PrivateKey) ks.getKey(alias, PASSWORD);
7 Certificate[] chain = ks.getCertificateChain(alias);
```

En la línea 1 y 2, utilizando la librería BouncyCastle se define en Java un nuevo proveedor de seguridad indicándole a SEFE utilice el objeto provider como elemento criptográfico.

En la línea 3, el objeto ks sirve como objeto para manipular el almacén de llaves definido para SEFE.

En la línea 4, se utilizan dos valores constantes KEYSTORE y PASSWORD. KEYSTORE es el valor de la ruta física donde se encuentra ubicado el almacén de llaves utilizado para firmar la factura. PASSWORD es una cadena de caracteres con la contraseña del almacén de llaves.

En la línea 5, se carga en memoria el alias que se definió internamente en el almacén de llaves.

En la línea 6, se carga en memoria la llave privada con base a los valores del alias y contraseña definidos.

En la línea 7, se extrae el certificado digital del almacén de llaves utilizado por SEFE.

Con lo anterior, SEFE utiliza la función sign del objeto app, instancia de la clase PDFSign. Esta función utiliza como parámetros de entrada: la constante SRC que contiene la ruta del archivo PDF origen, la constante DEST que es el archivo PDF firmado, la llave privada pk, el algoritmo para generar el digesto, nombre del proveedor, el estándar de cifrado.

```
1 PDFSign app = new PDFSign();
2   app.sign(SRC,   String.format(DEST,   1),   null,   pk,
DigestAlgorithms.SHA256,
  provider.getName(), MakeSignature.CryptoStandard.CMS, "V1",
"SHA256");
```

PDFSign procesa la información de la siguiente manera:

```
1 PdfReader reader = new PdfReader(src);
2 FileOutputStream os = new FileOutputStream(dest);
3 PdfStamper stamper = PdfStamper.createSignature(reader, os,
'\0');
4         PdfSignatureAppearance         appearance         =
stamper.getSignatureAppearance();
5 appearance.setReason(reason);
6 appearance.setLocation(location);
7 appearance.setVisibleSignature(new Rectangle(36, 748, 144,
780), 1, "sig");
8 ExternalDigest digest = new BouncyCastleDigest();
9 ExternalSignature signature =
    new PrivateKeySignature(pk, digestAlgorithm, provider);
10 MakeSignature.signDetached(appearance, digest, signature,
chain, null, null, null, 0, subfilter);
```

En la líneas 1 – 3 se definen los objetos reader y stamper como instancias de las clases PdfReader y PdfStamper, definidos en las librerías iText. Estos objetos permiten la manipulación de archivos PDF existentes y los cuales SEFE utiliza como entrada y salida. El archivo de entrada es el documento PDF con el contenido de la factura y el de salida la factura PDF firmada.

En las líneas 4 – 7, se definen características para crear una marca visible de la firma digital en el documento.

En las líneas 8 – 9, los objetos digest y signature interfaces de las clases ExternalDigest y ExternalSignature, permiten definir el tipo de digesto y el tipo de firma.

En la línea 10 se firma el documento con la información. En la Figura 17 se muestra la información visible en el documento. En el apéndice A puede verse el contenido del certificado.

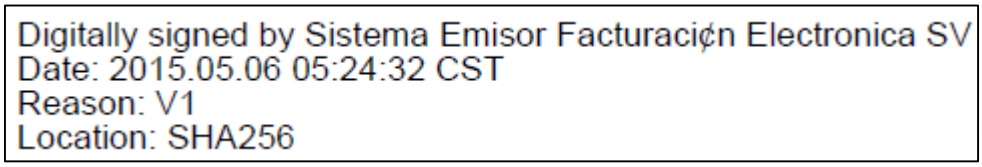


Figura 17: Ejemplo de Firma digital

5.1.3 Opción Propiedades

SEFE posee una pantalla (Figura 18) para que el emisor pueda definir valores que sirven de parámetros implícitos dentro de la codificación. Por ser un prototipo únicamente se consideró los siguientes parámetros:

- KeyStore: Ruta con la ubicación del archivo que su utiliza como almacén de llaves,
- KeyStore Password: Cadena de caracteres con la contraseña para el alias de la llave privada,
- Retención IVA: Valor entero para el cálculo del IVA,
- Retención Renta: valor entero para el cálculo de Renta.

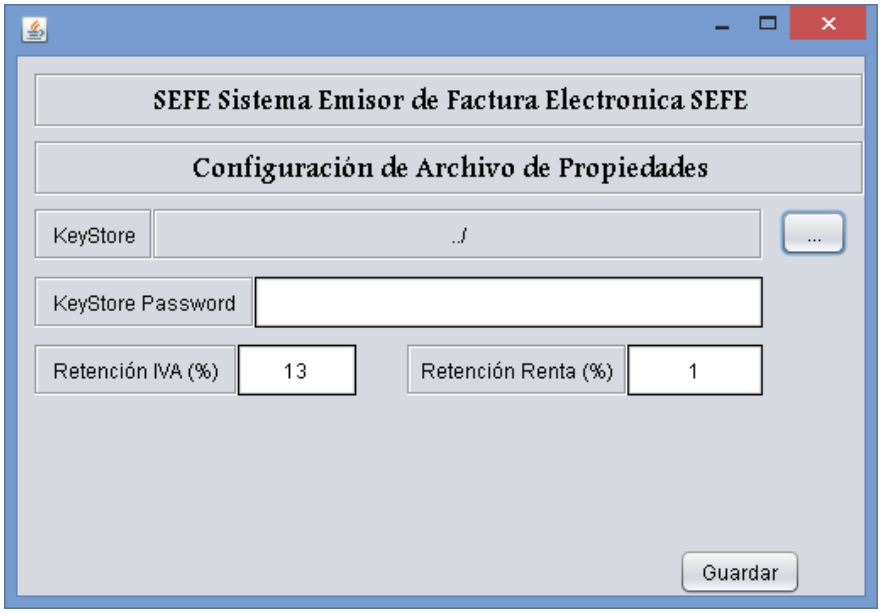


Figura 18: Configuración de propiedades de SEFE

SEFE no cuenta con una base de datos, por lo que se utiliza un archivo de texto para almacenar esta información.

Cuando SEFE ha creado la factura firmada, el emisor puede enviar el archivo PDF por cualquier medio de comunicación que considere conveniente. Para que el receptor pueda validar la factura firmada necesita el certificado digital del emisor y el archivo PDF, (Figura 19).

Como software de verificación se utiliza Acrobat Reader debido a su popularidad y libre descarga. El receptor debe especificar el certificado del emisor como de confianza, en la figura siguiente se muestra el administrador de ID digital y certificados de confianza de Acrobat Reader (Figura 20).

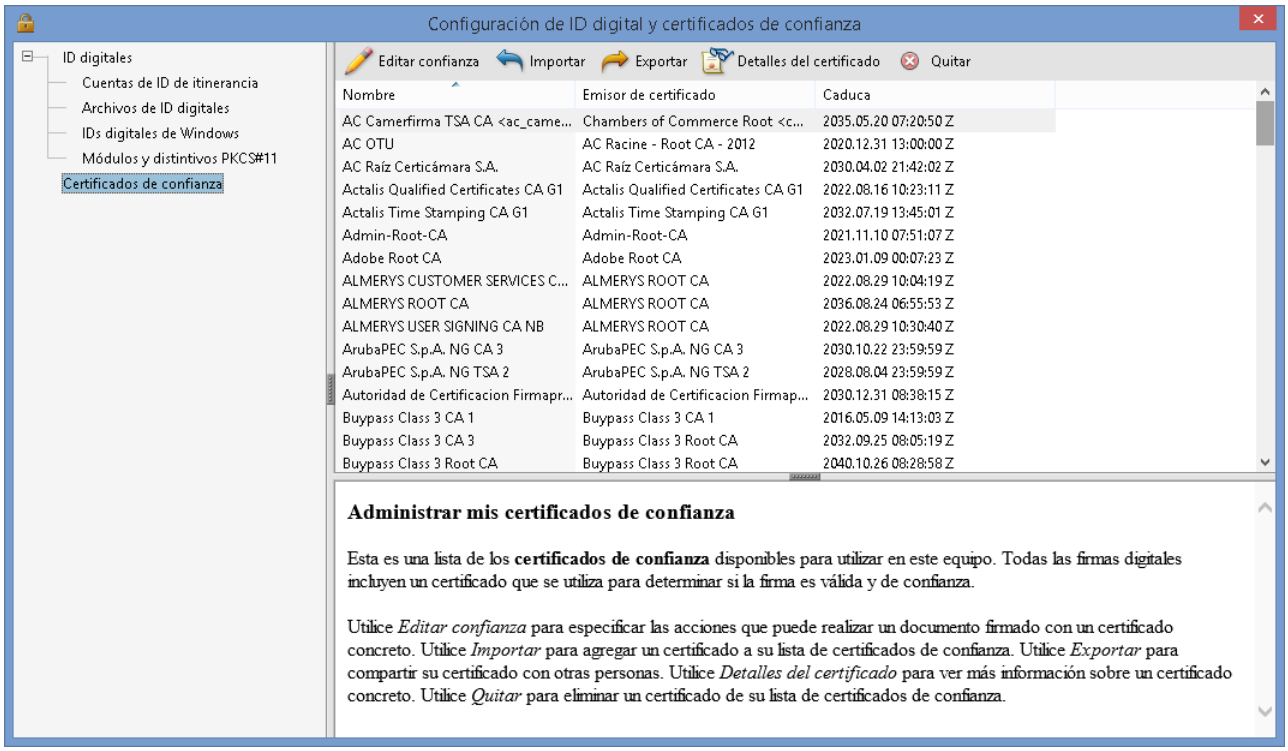


Figura 19: Configuración de ID digital y Certificado de Confianza en Adobe Reader

En la opción Importar, el usuario especifica la ubicación del certificado digital del emisor y es agregado al listado de certificado de Acrobat Reader (Figura 20).

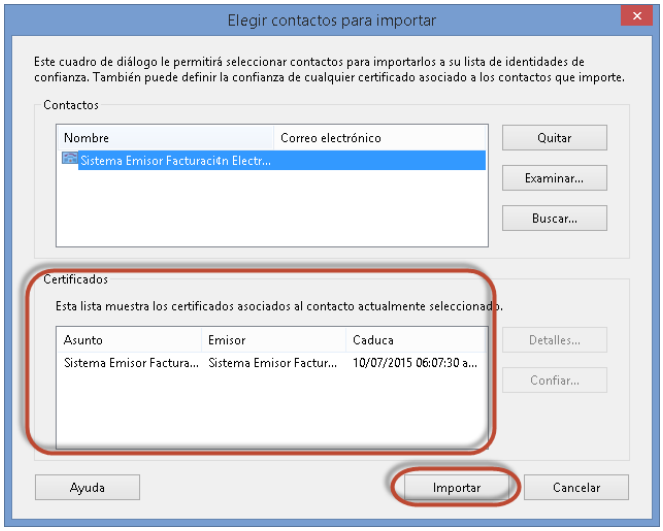


Figura 20: Ejemplo de importación de Certificado de Confianza

Realizado este proceso, el receptor accede a la factura digital firmada para revisar el contenido. Acrobat Reader realiza internamente el proceso de verificación utilizando la firma digital embebida en el archivo PDF y el certificado digital instalado. Si el contenido de la factura no ha sido alterado y la entidad verificada, se muestra una marca azul como se ve en la Figura 22. Este es el garante que la factura digital es un documento válido.

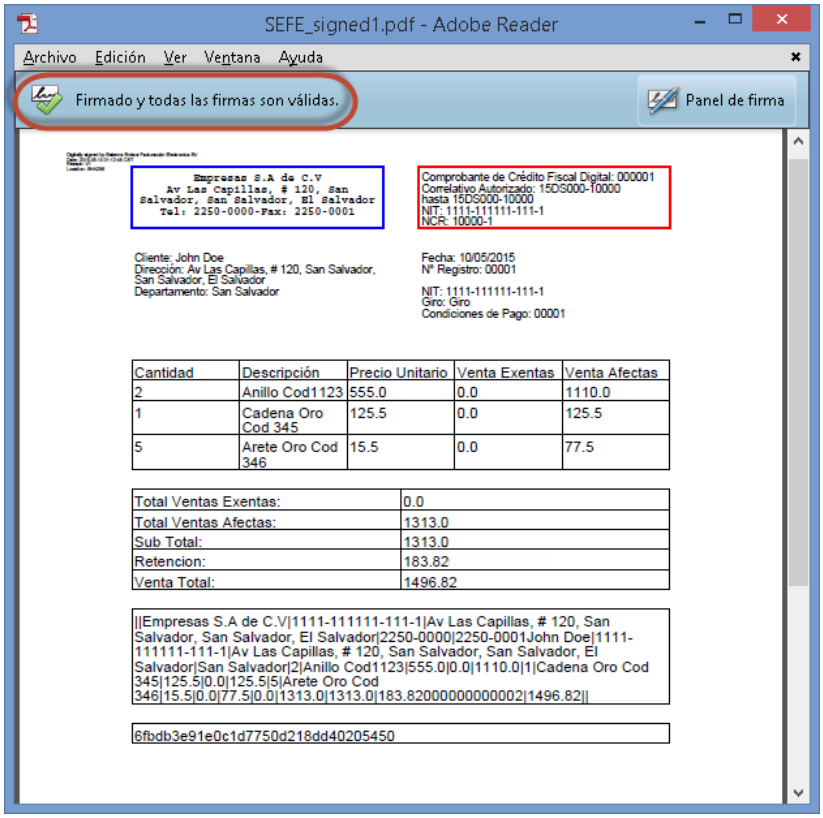


Figura 21: Mensaje de certificación de firmas

Si en caso hay alguna alteración del documento o la entidad no puede ser comprobada, como en las Figuras 22 y 23 respectivamente, se muestran el mensaje visible de notificación. Si este es el caso, el receptor puede rechazar la factura argumentando que no es un documento válido y solicitar al emisor una nueva factura.

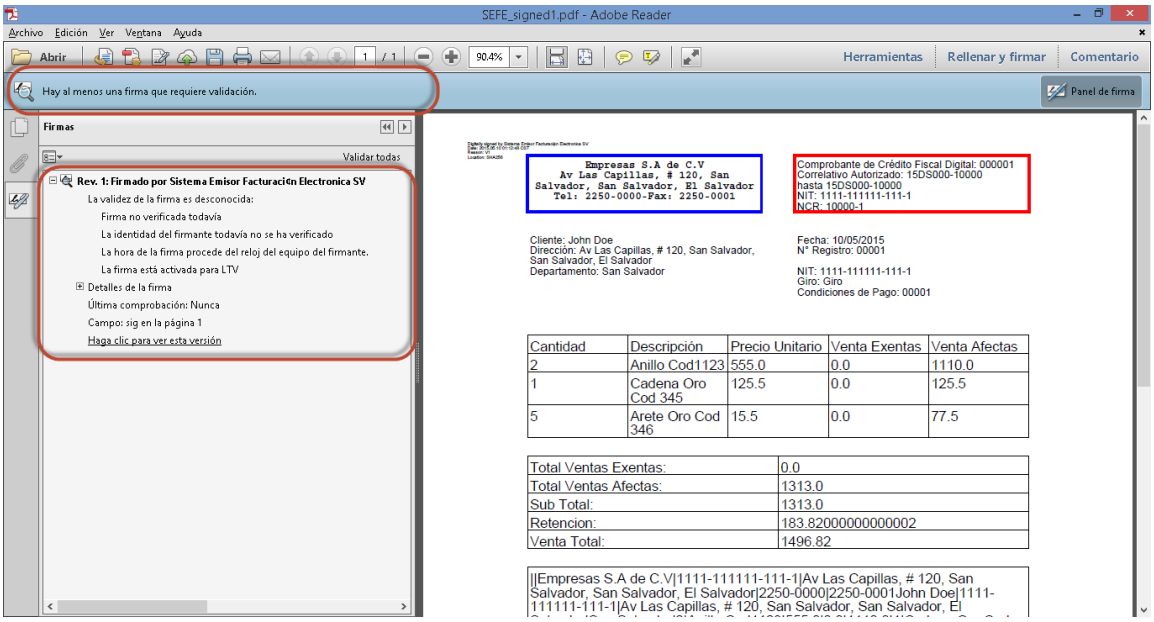


Figura 22: Mensaje de notificación de firma que requiere validación

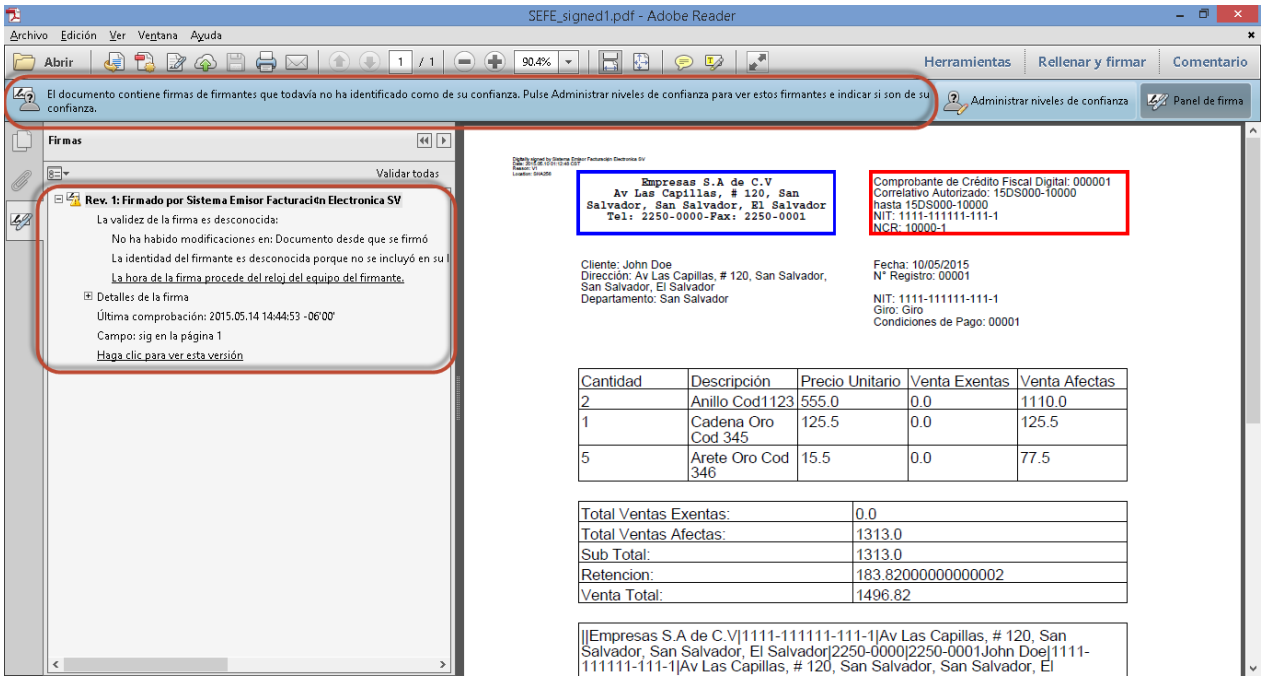


Figura 23: Mensaje de Certificación

6 Conclusiones

En este proyecto se realizó la implementación del Sistema Emisor de Facturas Electrónicas (SEFE) que es una versión digital del proceso manual indicado en el Código Tributario de El Salvador. Con el sistema diseñado se consigue lo siguiente:

1. Reducción de tiempo de envío: brinda rapidez y seguridad en el intercambio de información y agiliza la recepción de productos o servicios, lo cual requiere ahorros y un importante incremento de productividad.
2. Ahorro en gastos de administración como papelería, almacenaje y envíos, etc.
3. Mayor seguridad en el manejo, resguardo y envío de facturas disminuyendo la posibilidad de falsificación ya que para ello, se debería descifrar el código de una llave privada asociada a un certificado de sello digital.

El prototipo propuesto no certifica la validez de la firma digital, por lo que se propone que a nivel país se designe a la entidad responsable de la validación. Se sugiere a SIGET como empresa encargada de esta verificación.

7 Referencias

[1] Constitución de la República de El Salvador, 1983. Extraído de: Página 22.

[2] Código Tributario de El Salvador, 2000. Extraído de: Páginas 37, 41, 43.

[3] Reglamento de aplicación del Código Tributario, 2001. Extraído de: Páginas 17, 43.

[4] Ley régimen especial de las facturas cambiarias y los recibos de las mismas. Extraído de: Páginas 1, 2, 3, 4.

[5] José Salvador Sánchez Garreta, Ingeniería de proyectos informáticos: actividades y procedimientos, Universitat Jaume I. pp. 102,103. 2003.

[6] Douglas R. Stinson, Cryptography: Theory and Practice, 3ra. Edición, Chapman and Hall/CRC, 2005.

[7] Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. IT-22, No. 6, Noviembre1976.

[8] William Stallings, Fundamentos de Seguridad en Redes Aplicaciones y Estándares, 2da. Edición, Pearson Educación, 2004.

[9] RFC 6234 referente a los estándares para algoritmos SHA y SHA basando en HMAC and HKDF. https://tools.ietf.org/html/rfc6234.

[10] Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, 1ra. Edición. Chapman and Hall/CRC, 2007.

[11] RFC 3447 referente a los estándares para algoritmos de criptografía de llave pública. https://tools.ietf.org/html/rfc3447.

[12] Sistema Nacional de Certificación Digital, Firma digital, Ministerio de Ciencia, Tecnología y Comunicaciones, Extraído de: http://www.firmadigital.go.cr/Info.html, 2015.

[13] Gobierno de la República de Panamá, Firma electrónica, Extraído de: https://www.firmaelectronica.gob.pa/, 2015.

[14] Manuel José Lucena López, Criptografía y Seguridad en Computadores, 3ra. Edición, Universidad de Jaén, España. 2003.

[15] RFC 5280 referente a los estándares para certificado de infraestructura de llave pública. https://tools.ietf.org/html/rfc5280

[16] Purificación Aguilera, Redes Seguras (Seguridad Informática), Editex, Octubre 2011.

[17] Kenneth C. Laudon, Jane P. Laudon, Sistemas de Información Gerencial, 10ma. Edición, Pearson, 2013.

[18] Bruno Lowagie, Digital Signatures for PDF Documents, a White Paper, iText Software BVBA, 2011. http://www.pdfa.org/download/brunos-whitepaper-on-digital-signatures/

[19] Superintendencia de Administración Tributaria, Factura Electrónica, Extraído de: http://portal.sat.gob.gt/sitio/index.php/tramites-o-gestiones/tramites-y-requisitos-tributarios/factura-electronica.html, 2015.

[20] Servicio de Administración Tributaria, Generación gratuita de facturas electrónicas, Extraído de: http://www.sat.gob.mx/informacion_fiscal/factura_electronica/Paginas/servicio_generacion_cfdi.aspx, 2015.

[21] Diario Oficial de la Federación, Ley de Firma Electrónica Avanzada, Extraído de: http://www.dof.gob.mx/nota_detalle.php?codigo=5228864&fecha=11/01/2012, 2015.

[22] Bruno Lowagie, iText in Action: overview of the examples, Extraído de: http://itextpdf.com/book/examples.php, 2015.

[23] Documento explicativo del Anteproyecto de Ley de firma electrónica El Salvador, Secretaría para Asuntos Legislativos y Jurídicos de la Presidencia Ministerio de Economía Dirección de Innovación Tecnológica e Informática del Gobierno de El Salvador, 2012.

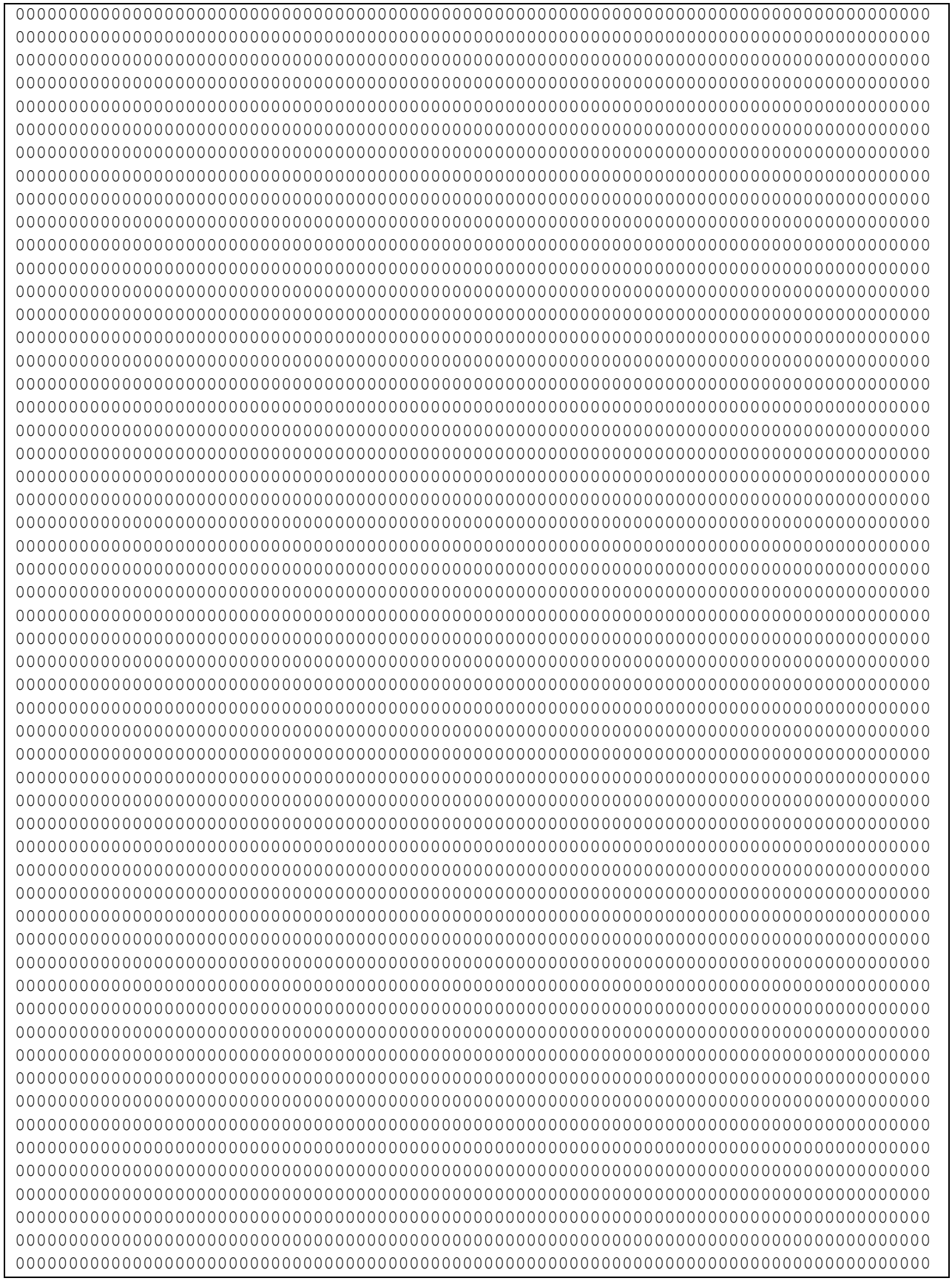
[24] Walter Augusto García Rojas, Tesis: Implementación de firma digital en una plataforma de comercio electrónico, Universidad Católica del Perú, Septiembre 2011.

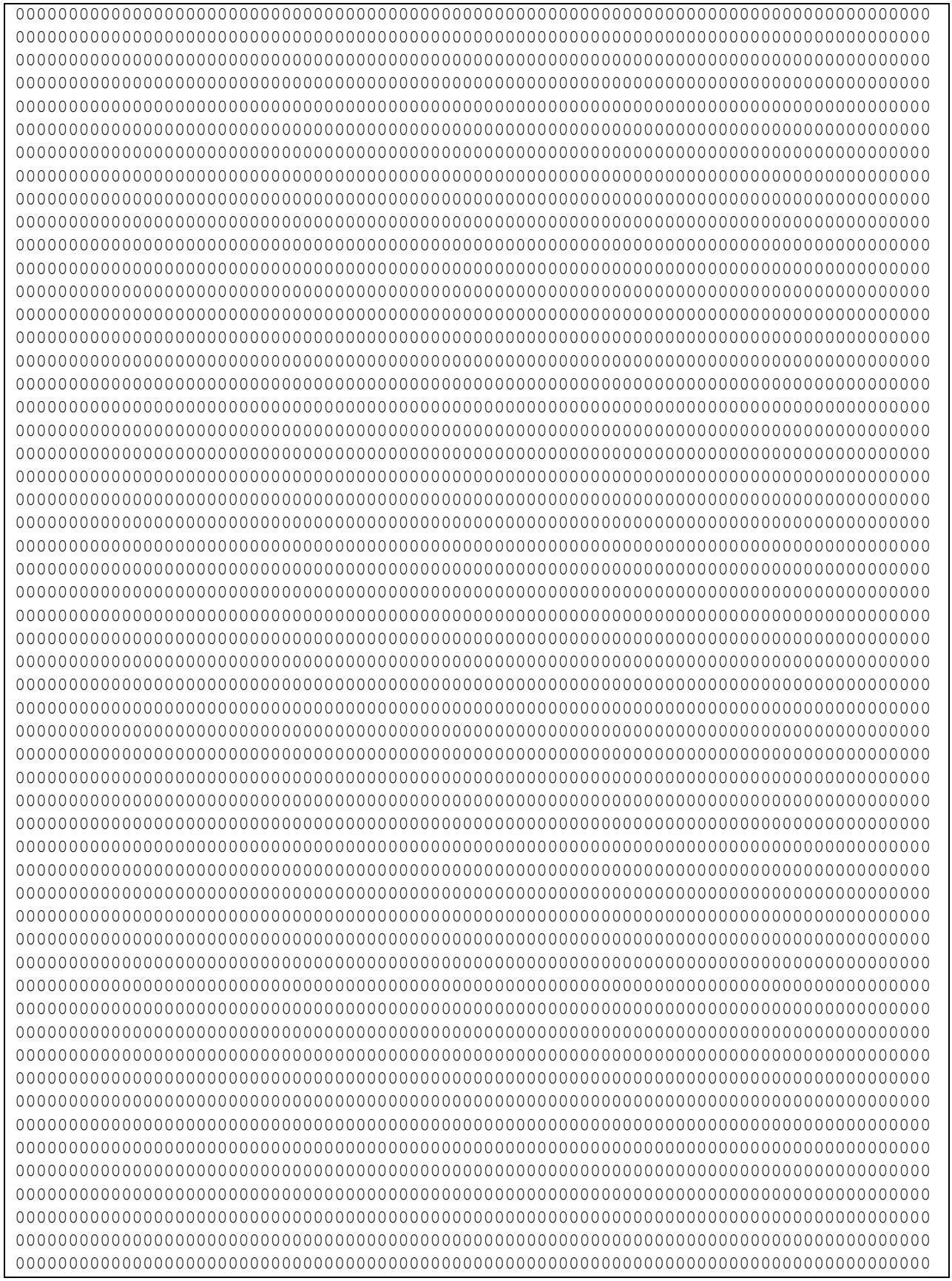
[25] Francisco Javier Cañabate Bernete, eFactura: Aplicación de gestión de facturas electrónicas basado en la tecnología .NET, Universitat de Catalunya, Junio 2008.

Apéndice A

Firma Digital embebida en el documento PDF


```
<</Contents
<3082062506092a864886f70d010702a0820616308206120201013 10f300d06096086480165030402010500
0300b06092a864886f70d010701a08203bd308203b9308202a1a003020102020425e6d178300d06092a864
886f70d01010b050030818c310b3009060355040613025356311530130603550408130c53616e2053616c7
661646f72311530130603550407130c53616e2053616c7661646f72310c300a060355040a1303554442310
c300a060355040b13035544423133303106035504030c2a53697374656d6120456d69736f7220466163747
572616369c2a26e20456c656374726f6e696361205356301e170d313530343131303630373330 5a170d313
530373130303630373330 5a30818c310b3009060355040613025356311530130603550408130c53616e205
3616c7661646f72311530130603550407130c53616e2053616c7661646f72310c300a060355040a1303554
442310c300a060355040b13035544423133303106035504030c2a53697374656d6120456d69736f7220466
163747572616369c2a26e20456c656374726f6e696361205356308201220300d06092a864886f70d0101010
5000382010f003082010a02820101009f8f4c0679f9ba6902d1abb88f63cf5e12c1d1cb516ea792bc3a597
2eba8eb40becb45ad3a0852ee53179c87da1c0e51e269904e4456dd368b7cbd5b1ca3f58c6e812067b5b06
897a7a3c29ff1d19fd0326a35d1c69a7ad118f25ecadd770c0af1a50fa41f725a290a35b7772a8c9f6fbe8
f3823f92da0759359e5c53e00f5308f806a26d9b2163f6d8e329ffa2a450b612945042d3994c41ae00ad8d
35c48a0eadbd098efcb862c29262f2acd9bc630c64c4ece4aab41f83f2d60c81dc1df410a0ec5e29a5352f
b941fd016f481a171412ac02839cbd961cee17178dbc77aa12b6e99a6cc7810d51d65ed472187a211c93fc
2f597be5efd14ee8ddba72620a90203010001a321301f301d0603551d0e041604148ee39a4c269c79ea184
b9682da193d282cebda9e300d06092a864886f70d01010b050003820101 0008a77fb24a539cec42d38401c
8d66397587527b248ff0c6bac1de5e7d5d813976a863e4f6dd946c256861cd152a3d0bc795c80c5015a2cd
0aa04bf4dc97039be95294b075c3f57e860d831823ea00debbf1c39a468b14705ab8b46234faa2f03bf92e
da81e99b168185e1baff755427b7024bf2d70b4d9920224625d5520a041051ac07a6b54afd9cd6928e5dd9
80a6dab5b460f7efea3e1afcc374ecb46ec678af5fa01e0b31c767f8e190b53f1b257bda747cb1fa73c495
bbe7f78e136c92c56760d6e7bcf034e7281ae2def72b6eacf84e9a085d781006d5698e963daff484b1fd5e
7b0aa0990064709b719542a6a2e0ad46607f1bbd53da90a570e09efd13182022c308202280201013081953
0818c310b3009060355040613025356311530130603550408130c53616e2053616c7661646f72311530130
603550407130c53616e2053616c7661646f72310c300a060355040a1303554442310c300a060355040b130
355444231333031060355040 30c2a53697374656d6120456d69736f72204661637475726163 69c2a26e204
56c656374726f6e696361205356020425e6d178300d060960864801650304020105 00a069301806092a864
886f70d010903310b06092a864886f70d010701301c06092a864886f70d010905310f170d3135303530363
131323433325a302f06092a864886f70d010904312204204b08833201f3d8900ab1f7af84e92b692262c32
f87b6225f560a9dc2573203e1300d06092a864886f70d0101010500048201009b6fe05141676e9b291cae3
2c459a876ffc16a04e59c5cfadf555ca4fd4928a7bceb7208cbbc9a9ff62e5bafd0395f6aca432e28dde44
2629fe8de29d6152713445447d63290f1b6ef6a5bba34a64857b3503a537659bf897717d91c27ebf9cccc6
38bbe10c9436cf6000031b150ba31fa6165f2796831d1616a4db7f7d39cba73d454ee0f485bdf80af5c621
0ed930ab6012063d3057dabcc13c4cdc7692d1cef7eeb96ea3bbd9e65ce4d57f926f0dee7f34f46012fc6f
720b46c513d7c188349818940b9286cc184b2ed93b5c8cf28a0990cf843e05a0ddb4e7b50fc1fd1c6d477d
53b9e2eb1b4ff41b668054c682630892badc16788cdc3a27b6366e2c9be0000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
```





```
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000>/Filter/Adobe.PPKLite/Type/Sig/Prop_Buil
d<</App<</Name/iText#ae#205.5.3#20#a92000-2014#20iText#20Group#20NV#20#28AGPL-
version#29>>>>/ByteRange          [0          182          16568          3969          ]
/SubFilter/adbe.pkcs7.detached/Reason(V1)/Location(SHA256)/ContactInfo()/M(D:201505060
52432-06'00')>>
```