



Ingeniería Técnica Informática de Sistemas

Curso académico: 2009-2010

Proyecto Fin de Carrera

LA FACTURA ELECTRÓNICA

Autor: Angel Montes Sánchez

Tutor: Francisco Domínguez

Madrid 2010

A mi familia.

Resumen

Una factura es un documento en el que queda reflejado la entrega de un producto o la prestación de un servicio por parte del emisor al receptor. Este documento, tradicionalmente en papel, contiene la fecha de devengo, los datos del emisor y del receptor y la cantidad a pagar como contraprestación. En la actualidad, donde las tecnologías de la información y las comunicaciones cada vez tienen una mayor relevancia, este sistema de facturación queda obsoleto y es una de las causas por las que ha nacido el concepto de factura electrónica. Son ya varios los países que están impulsando la utilización de la factura electrónica por los beneficios ecológicos y económicos que presenta respecto a la factura en papel. En España, por ejemplo, ya es obligatorio el uso de este sistema de facturación en las administraciones del Estado.

En este proyecto vamos a realizar el estudio del estado del arte de la factura electrónica. Vamos a ver qué es una factura electrónica, qué ventajas presenta respecto a la factura tradicional en papel, cuáles son las normativas legales vigentes para que tengan validez tanto legal como fiscal y qué tecnologías se están utilizando en la actualidad para generar facturas electrónicas.

Una vez realizado el estado del arte, vamos a desarrollar un sistema de facturación, que nos permita emitir facturas electrónicas que tengan validez legal en el mundo real. Concretamente vamos a realizar la implementación del formato FacturaE en su versión 3.1. Este formato de facturación es libre y está basado en la utilización de XML para facilitar el intercambio de datos. Es el modelo que está desarrollando la Agencia Tributaria

(AEAT) junto con el Ministerio de Industria y Comercio (MITyC) en España para impulsar el uso de la factura electrónica. Para que las facturas que genere nuestro sistema sean facturas electrónicas válidas, tienen que estar firmadas siguiendo una política de firma digital avanzada como es el estándar XADES, por esto vamos a implementar también un sistema de firma digital y verificación de firmas que cumpla con este estándar.

Índice general

Resumen	I
1. Introducción	1
1.1. Estado del arte	1
1.1.1. ¿Qué es una factura electrónica?	1
1.1.2. Beneficios de la factura electrónica	3
1.1.3. Legislación y normativa	4
1.1.4. La firma digital	10
1.1.5. ¿Qué es y para qué sirve?	10
1.1.6. Formatos de factura electrónica	18
1.1.7. FacturaE v3.1	19
2. Objetivos	27
2.1. Descripción del problema	27
2.2. Requisitos	28
2.3. Metodología empleada	29
2.3.1. Desarrollo en espiral	29

3. Descripción informática	32
3.1. Arquitectura general de la aplicación	32
3.2. Componente FacturaE	35
3.2.1. Especificación	35
3.2.2. Diseño e Implementación	35
3.3. Componente FirmaDigital	44
3.3.1. Especificación	44
3.3.2. Diseño e Implemetación	44
3.4. Componente Facturación	48
3.4.1. Especificación	48
3.4.2. Diseño e Implemetación	48
3.5. Componente FacturaElectronica	51
3.5.1. Especificación	51
3.5.2. Diseño e Implementación	51
4. Pruebas	54
5. Conclusiones	57
5.1. Logros alcanzados	57
5.2. Conocimientos adquiridos	58
5.3. Trabajos futuros	59

Capítulo 1

Introducción

En el siguiente capítulo vamos a ver el estado del arte de la factura electrónica, en el que vamos a explicar qué es una factura electrónica, qué normativas legales la regulan y qué tecnologías utiliza. En los capítulos posteriores, describiremos cómo se ha desarrollado nuestra aplicación Factura Electrónica, veremos el diseño principal de la aplicación, qué metodología se ha seguido, qué tecnologías se han utilizado y una descripción informática del código fuente.

1.1. Estado del arte

1.1.1. ¿Qué es una factura electrónica?

Para dar una definición de qué es una factura electrónica vamos a definir primero qué es una factura. Una factura es el justificante legal en el intercambio de un producto o la prestación de un servicio entre dos partes. En el proceso de facturación intervienen dos entidades, el emisor, que es el que presta un servicio o proporciona un producto, y el receptor, que es el beneficiario del servicio o el que adquiere el producto. En la factura se encuentran los datos del expedidor y del destinatario, el detalle de los productos y servicios suministrados, los precios unitarios, los precios totales, los descuentos y los impuestos.

Existen distintos tipos de facturas, de forma general se pueden clasificar como:

- Ordinarias: documentan la operación de suministro.
- Rectificativas: documentan correcciones de una o más facturas anteriores, o bien devoluciones de productos, envases y embalajes o comisiones por volumen.
- Recapitulativas: documentan agrupaciones de facturas de un período.

Además existen las siguientes variantes:

- Pro-forma: documenta una oferta, con indicación de la forma exacta que tendrá la factura tras el suministro. No tienen valor contable ni como justificante.
- Copia: documenta la operación para el emisor, con los mismos datos que el original. Debe llevar la indicación de copia para permitir distinguirla del original.
- Duplicado: documenta la operación para el receptor, en caso de pérdida del original. La expide el mismo emisor que expidió el original y tiene los mismos datos que el original. Debe llevar la indicación de duplicado para permitir distinguirla del original, especialmente para el caso de que reaparezca el original.

La facturación electrónica consiste en el intercambio telemático o electrónico de un documento digital equivalente a la factura en papel, entre el emisor y el receptor. Este documento digital puede tener distintos formatos, como por ejemplo EDIFACT, UBL, XML, PDF, HTML, .doc, .xls, GIF, JPEG, TXT, etc.

La transmisión de la factura tiene que realizarse de forma telemática, es decir, entre un ordenador o sistema de datos a otro ordenador o sistema de datos y tiene que garantizar la autenticidad y la integridad de los datos transmitidos. Para conseguir estas garantías el documento ha de estar firmado digitalmente por medio de un tipo de firma electrónica reconocida como por ejemplo un certificado X.509 o el DNI-e.

1.1.2. Beneficios de la factura electrónica

La adaptación de la factura electrónica supone una serie de mejoras y ventajas respecto a la factura tradicional tanto del lado del emisor como del receptor. Existen varias razones para adaptar este modelo, desde motivos de tipo económico hasta ecológicos.

Podemos destacar las siguientes ventajas:

- Ahorro de costes: Gracias a la supresión del papel, al abaratamiento de los medios de comunicación electrónicos (en contraposición a los medios tradicionales de envío postal), a la eliminación de los gastos de franqueo, a los gastos derivados de la introducción manual de datos, etc.
- Integración con otras aplicaciones informáticas: desde el punto de vista del emisor continúa el proceso que ya se está realizando electrónicamente, sólo tiene que emitir y enviar la factura. Desde el lado del receptor los datos pueden ser introducidos automáticamente en sus aplicaciones. Ya no se exige imprimir la factura para que ésta sea válida legal y fiscalmente y, todo el tratamiento (emisión, distribución y conservación) puede realizarse directamente sobre el fichero electrónico generado por el emisor.
- Optimización de la tesorería: la automatización permite cuadrar los apuntes contables y comparar documentos (albarán / factura), minimizando a la vez el margen de error humano.
- Obtención de información en tiempo real: permite verificar el estado en el que se encuentra una factura y toda su información asociada (errores, rectificaciones, cobros, pagos, recepción de mercancías, albaranes,...) de forma exacta.
- Reducción de tiempos de gestión: El envío y recepción de las facturas, pasa a ser instantáneo.

- Agilidad en la toma de decisiones: la inmediatez de las comunicaciones permite adoptar decisiones, como la necesidad de financiación, en un espacio más corto de tiempo.
- Administración y contabilidad automatizadas: la integración en los sistemas de la empresa permite que toda la inserción de datos y las operaciones contables requieran mucha menos participación humana.
- Control de errores: a través de sistemas de alertas que detectan discrepancias entre operaciones de contabilidad y facturación.

1.1.3. Legislación y normativa

Antes de comentar qué requisitos tiene que cumplir la factura electrónica, vamos a definir qué es obligatorio en una factura tradicional, que también es aplicable a la factura electrónica y en general a cualquier tipo de factura:

Toda factura tiene la obligación legal y fiscal de contener como mínimo los siguientes elementos:

- Un número de factura.
- La fecha de emisión de la factura.
- Razón social del emisor y del receptor.
- NIF del emisor y del receptor.
- Domicilio del emisor y del receptor.
- Descripción de las operaciones y de la base imponible.
- El tipo impositivo.

- La cuota tributaria.
- La fecha de prestación del servicio, en caso de que sea distinta a la de emisión.

Para que una factura electrónica tenga validez legal, a parte de contener estos elementos, tiene que cumplir con la legislación y normativa actual por el que se rigen las facturas electrónicas y la firma digital.

En esta sección vamos a recapitular el conjunto de leyes y las obligaciones que la regulan:

Legislación sobre factura electrónica:

- SEXTA DIRECTIVA DEL CONSEJO de 17 de mayo de 1977 en materia de armonización de las legislaciones de los Estados miembros relativas a los impuestos sobre el volumen de negocios. Sistema común del IVA: Base imponible uniforme (77/388/CEE) [Vigente a 15 de mayo de 2004].
- DIRECTIVA 2001/115/CE DEL CONSEJO de 20 de diciembre de 2001 por la que se modifica la Directiva 77/388/CEE con objeto de simplificar, modernizar y armonizar las condiciones impuestas a la facturación en relación con el impuesto sobre el valor añadido.
- Directiva 2006/112/CE del consejo de 28 de noviembre de 2006 relativa al sistema común del impuesto sobre el valor añadido modificada por la Directiva 2006/138/CE del consejo de 19 de diciembre de 2006.
- LEY 58/2003, de 17 de diciembre, General Tributaria.
- Real Decreto 1624/1992, de 29 de diciembre, que aprueba el Reglamento del Impuesto sobre el Valor Añadido y modifica el Real Decreto 1041/1990, de 27 de julio, sobre declaraciones censales, el Real Decreto 338/1990, de 9 de marzo, sobre el Número de Identificación Fiscal; el Real Decreto 2402/1985, de 18 de diciembre sobre el deber

de expedir y entregar factura (los empresarios y profesionales), y el Real Decreto 1326/1987, de 11 de septiembre, sobre aplicación de la Directivas de la Comunidad.

- LEY 30/2007, de 30 de octubre, de Contratos del Sector Público.
- REAL DECRETO 1496/2003, de 28 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación, y se modifica el Reglamento del Impuesto sobre el Valor Añadido. Ver Real Decreto 87/2005, de 31 de enero.
- Real Decreto 87/2005, de 31 de enero, por el que se modifican el Reglamento del Impuesto sobre el Valor Añadido, aprobado por el artículo 1 del Real Decreto 1624/1992, de 29 de diciembre, el Reglamento de los Impuestos Especiales, aprobado por el artículo único del Real Decreto 1165/1995, de 7 de julio, y el Reglamento por el que se regulan las obligaciones.
- Orden EHA 962/2007 de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas, contenidas en el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el reglamento por el que se regulan las obligaciones de facturación.
- ORDEN PRE/2971/2007, de 5 de octubre, sobre la expedición de facturas por medios electrónicos cuando el destinatario de las mismas sea la Administración General del Estado u organismos públicos vinculados o dependientes de aquélla y sobre la presentación ante la Administración General del Estado o sus organismos públicos vinculados o dependientes de facturas expedidas entre particulares. (BOE n. 247 de 15/10/2007).
- RESOLUCIÓN de 24 de octubre de 2007, de la Agencia Estatal de Administración Tributaria, sobre procedimiento para la homologación de software de digitalización contemplado en la Orden EHA/962/2007, de 10 de abril de 2007.

- ORDEN HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria.
- Resolución de 24 de julio de 2003 de la Dirección General de la Agencia Estatal de Administración Tributaria por la que se establece el procedimiento a seguir para la admisión de certificados de entidades prestadoras de servicios de certificación electrónica.
- Sexta Directiva del Consejo, de 17 de mayo de 1977, en materia de armonización de las legislaciones de los Estados miembros relativa a los impuestos sobre el volumen de negocios. Sistema común del IVA: Base imponible uniforme (77/388/CEE).
- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

Legislación sobre Firma electrónica:

- DIRECTIVA 1999/93/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica .
- Ley 59/2003 de 19 de diciembre de Firma Electrónica.
- ORDEN HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria.
- Resolución de 24 de julio de 2003 de la Dirección General de la Agencia Estatal de Administración Tributaria por la que se establece el procedimiento a seguir para

la admisión de certificados de entidades prestadoras de servicios de certificación electrónica.

El Ministerio de Industria, Turismo y Comercio de España, define una serie de obligaciones legales, que han de cumplir tanto el emisor como el receptor de facturas electrónicas. Estas obligaciones son:

Obligaciones del emisor:

1. Reglamento sobre factura electrónica, la Orden 962/2007, de 10 de abril, desarrolla determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas, contenidas en el Real Decreto 1496/2003, que es el reglamento de facturación. Al respecto del consentimiento del destinatario, se encuentra recogido en el Artículo 2 de la citada Orden, donde dice que el consentimiento podrá formularse de forma expresa por cualquier medio, verbal o escrito.
2. Creación de la factura mediante una aplicación informática, con los contenidos obligatorios mínimos requeridos.
3. Firma electrónica reconocida.
4. Remisión telemática.
5. Conservación de copia o matriz de la Factura. Esta obligación se regula en el artículo 1 del RD 1496/2003, donde se especifica la obligación de expedir, entregar y conservar facturas. También han existido dudas sobre si las facturas electrónicas pueden emitirse en copia o sólo se debe guardar la matriz. Al respecto la Agencia Tributaria lo ha aclarado en el borrador antes citado (Art. 5) con la siguiente definición: Se entiende por Matriz de una factura (...) un conjunto de datos, tablas, base de datos o sistemas de ficheros que contienen todos los datos reflejados en las facturas junto a los programas que permitieron la generación de las facturas....

6. Contabilización y anotación en registros de IVA.
7. Conservación durante el período de prescripción.
8. Garantía de accesibilidad completa, deber de gestionar las facturas de modo que se garantice una accesibilidad completa: visualización, búsqueda selectiva, copia o descarga en línea e impresión. Esta es una obligación inherente a la conservación de las facturas por medios electrónicos que el legislador denomina acceso completo a datos, tratando de facilitar la auditoria e inspección de las facturas electrónicas. (Artículo 9 del RD 1496/2003).
9. Subcontratación a un tercero: Todas las fases anteriores pueden ser subcontratadas a un tercero, sin perder su responsabilidad. Regulado en el artículo 5.1 del RD 1496/2003 el legislador deja claro en ese mismo párrafo que, aunque se permite la subfacturación a terceros, es el obligado tributario el responsable de cumplir todas estas obligaciones.

Obligaciones del receptor:

1. Recepción de la factura por medio electrónico: Verificación de los contenidos mínimos exigibles y verificación segura de la firma electrónica. Regulado en el artículo 21 e inherente a las obligaciones de la conservación de las facturas electrónicas se indica que: El destinatario se debe asegurar de la legibilidad en el formato original en el que se haya recibido, así como, en su caso, de los datos asociados y mecanismo de verificación de firma. A diferencia del emisor, al que se permite construir la factura desde la matriz, el destinatario debe conservar los originales firmados.
2. Contabilización y anotación en registros de IVA.
3. Conservación durante el período de prescripción.

4. Deber de gestionar las facturas de modo que se garantice una accesibilidad completa: visualización, búsqueda selectiva, copia o descarga en línea e impresión.
5. Todas las fases anteriores puede subcontratarlas a un tercero, sin perder su responsabilidad.

1.1.4. La firma digital

1.1.5. ¿Qué es y para qué sirve?

La firma digital puede ser definida como una secuencia de bits que se obtienen mediante la aplicación a un mensaje determinado, de un algoritmo de cifrado asimétrico o de clave pública, y que equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje.

La aparición de las redes de ordenadores y sobre todo de Internet, han hecho posible que el intercambio de información entre personas situadas geográficamente distantes sea posible. Este intercambio de información plantea el problema de acreditar tanto la autenticidad como la autoría de los mismos.

Concretamente, para que dos personas puedan intercambiar entre ellas mensajes electrónicos que sean mínimamente fiables y puedan dar la confianza y la seguridad que necesitan, esos mensajes deben cumplir los siguientes requisitos:

1. Identidad, que implica poder verificar formalmente la identidad de las entidades participantes en una comunicación o intercambio de información.
2. Integridad, que implica la certeza de que el mensaje recibido por el receptor es exactamente el mismo mensaje emitido por el emisor, sin que haya sufrido alteración alguna durante el proceso de transmisión desde el emisor hacia el receptor.

3. No repudiación o no rechazo en origen, que implica que el emisor del mensaje no pueda negar en ningún caso que el mensaje ha sido enviado por él.

La firma digital es un procedimiento técnico que basándose en técnicas criptográficas trata de dar respuesta a estas necesidades, a fin de posibilitar el intercambio de información de forma electrónica.

Por otra parte, a los tres requisitos anteriores, se une un cuarto elemento, que es la confidencialidad, que no es un requisito esencial de la firma digital sino que complementa a la misma. La confidencialidad implica que el mensaje no haya podido ser leído por terceras personas distintas del emisor y del receptor durante el proceso de transmisión del mismo.

Criptografía

El principal mecanismo sobre el que se basa la firma digital es la criptografía. La firma digital se basa en la utilización combinada de dos técnicas distintas, que son la criptografía asimétrica o de clave pública para cifrar mensajes y el uso de las llamadas funciones hash o funciones resumen.

El diccionario de la Real Academia Española de la Lengua define la criptografía como *“el arte de escribir con clave secreta o de forma enigmática ”*. La criptografía es un conjunto de técnicas que mediante la utilización de algoritmos y métodos matemáticos sirven para cifrar y descifrar mensajes. La criptografía ha venido siendo utilizada desde hace bastante tiempo, fundamentalmente con fines militares. Tradicionalmente se ha hablado de dos tipos de sistemas criptográficos: los simétricos o de clave privada y los asimétricos o de clave pública.

Los sistemas criptográficos simétricos son aquellos en los que dos personas (A y B), que van a intercambiarse mensajes entre sí, utilizan ambos la misma clave para cifrar y descifrar el mensaje. Así, el emisor del mensaje (A), lo cifra utilizando una determinada clave, y una vez cifrado, lo envía a B. Recibido el mensaje, B lo descifra utilizando la misma

clave que usó A para cifrarlo. Los sistemas criptográficos simétricos más utilizados son los conocidos con los nombres de DES, TDES y AES.

Los principales inconvenientes del sistema simétrico son los siguientes:

- La necesidad de que A (emisor) y B (receptor) se intercambien previamente por un medio seguro la clave que ambos van a utilizar para cifrar y descifrar los mensajes.
- La necesidad de que exista una clave para cada par de personas que vayan a intercambiarse mensajes cifrados entre sí.

Estas dificultades determinan que los sistemas de cifrado simétricos no sean los ideales para ser utilizados en redes como internet, en la que intervienen numerosas personas que se desconocen entre sí y que en la mayoría de los casos no podrán intercambiarse previamente claves de cifrado por ningún medio seguro.

Los sistemas criptográficos asimétricos o de clave pública se basan en el cifrado de mensajes mediante la utilización de un par de claves diferentes privada y pública, de ahí el nombre de asimétricos, que se atribuyen a una persona determinada y que tienen las siguientes características:

- Una de las claves, la privada, permanece secreta y es conocida únicamente por la persona a quien se ha atribuido el par de claves y que la va a utilizar para cifrar mensajes. La segunda clave, la pública, es o puede ser conocida por cualquiera.
- Ambas claves, privadas y públicas, sirven tanto para cifrar como para descifrar mensajes.
- A partir de la clave pública, que es conocida o puede ser conocida por cualquiera, no se puede deducir ni obtener matemáticamente la clave privada, ya que si partiendo de la clave pública, que es o puede ser conocida por cualquier persona, se pudiese obtener la clave privada, el sistema carecería de seguridad dado que cualquiera podría

utilizar la clave privada atribuida a otra persona pero obtenida ilícitamente por un tercero partiendo de la clave pública.

Todo esto se basa en una característica de los números primos y en el problema de la factorización. El problema de la factorización es la obtención a partir de un determinado producto de los factores cuya multiplicación ha dado como resultado ese producto.

Los números primos (números enteros que no admiten otro divisor que no sea el 1 o ellos mismos), se caracterizan porque si se multiplica un número primo por otro número primo, da como resultado un tercer número primo a partir del cual es imposible averiguar y deducir los factores.

El criptosistema de clave pública más utilizado en la actualidad es el llamado RSA, creado en 1978 y que debe su nombre a sus tres creadores (Rivest, Shamir y Adleman).

La utilización del par de claves (privada y pública) implica que A (emisor) cifra un mensaje utilizando para ello su clave privada y, una vez cifrado, lo envía a B (receptor). B descifra el mensaje recibido utilizando la clave pública de A. Si el mensaje descifrado es legible significa necesariamente que ese mensaje ha sido cifrado con la clave privada de A (es decir, que proviene de A) y que no ha sufrido ninguna alteración durante la transmisión de A hacia B, porque si hubiera sido alterado por un tercero, el mensaje descifrado por B con la clave pública de A no sería legible.

Así se cumplen dos de los requisitos anteriores, que son la integridad (certeza de que el mensaje no ha sido alterado) y no repudiación en origen (imposibilidad de que A niegue que el mensaje recibido por B ha sido cifrado por A con la clave privada de éste). El tercer requisito (identidad del emisor del mensaje) se obtiene mediante la utilización de los certificados digitales.

Las funciones Hash:

Junto a la criptografía asimétrica se utilizan en la firma digital las funciones hash o

funciones resumen. Los mensajes que se intercambian pueden tener un gran tamaño, lo que dificulta el proceso de cifrado. Por ello, no se cifra el mensaje entero sino un resumen del mismo, obtenido aplicando al mensaje una función hash.

Partiendo de un mensaje determinado que puede tener cualquier tamaño, dicho mensaje se convierte mediante la función hash en un mensaje con una dimensión fija (generalmente de 160 bits). Para ello, el mensaje original se divide en varias partes cada una de las cuales tendrá ese tamaño de 160 bits, y una vez dividido se combinan elementos tomados de cada una de las partes resultantes de la división para formar el mensaje-resumen o hash, que también tendrá una dimensión fija y constante de 160 bits.

Este resumen de dimensión fija es el que se cifrará utilizando la clave privada del emisor del mensaje.

Los sellos temporales:

Finalmente, en el proceso de intercambio de mensajes electrónicos es importante que, además de los elementos o requisitos anteriormente analizados, pueda saberse y establecerse con certeza la fecha exacta en la que los mensajes han sido enviados. Esta característica se consigue mediante los llamados sellos temporales o *time stamping*, que es una función atribuida generalmente a los Prestadores de Servicios de Certificación mediante la cual se fija la fecha de los mensajes electrónicos firmados digitalmente.

La confidencialidad de los mensajes:

En ocasiones, además de garantizar la procedencia de los mensajes electrónicos que se intercambian por medio de internet y la autenticidad o integridad de los mismos, puede ser conveniente garantizar también su confidencialidad. Esto implica tener la certeza de que el mensaje enviado por A (emisor) únicamente será leído por B (receptor) y no por terceras personas.

En tales casos, también se acude al cifrado del mensaje con el par de claves, pero de

manera diferente al mecanismo propio y característico de la firma digital. Para garantizar la confidencialidad del mensaje, el cuerpo del mismo se cifra utilizando la clave pública de B (receptor), quien al recibir el mensaje lo descifrará utilizando para ello su clave privada (la clave privada de B). De esta manera se garantiza que únicamente B pueda descifrar el cuerpo del mensaje y conocer su contenido.

Los certificados digitales:

Para resolver el problema de la identidad en las comunicaciones, existen los certificados digitales. Un certificado digital básicamente es un documento que acredita la asociación de una persona con su clave pública. Esta asociación tiene que realizarla una tercera entidad, una Autoridad de Certificación, que es de confianza y que verifica que la clave asociada a una determinada entidad o persona es esa entidad o persona. Gracias al certificado digital, el par de claves obtenido estará vinculado a una determinada identidad, y si sabemos que el mensaje ha sido cifrado con la clave privada de esa entidad, sabremos también quién es la persona titular de esa clave privada.

Los certificados digitales tienen una duración determinada, transcurrida la cual deben ser renovados, y pueden ser revocados anticipadamente en ciertos supuestos (por ejemplo, en el caso de que la clave privada, que debe permanecer secreta, haya pasado a ser conocida por terceras personas no autorizadas para usarla).

¿Cómo funciona la firma digital?

El proceso de firma digital de un mensaje o documento electrónico comprende en realidad dos procesos sucesivos: la firma del mensaje por el emisor del mismo y la verificación de la firma por parte del receptor del mensaje. Vamos a ver un ejemplo de los pasos necesarios para conocer como sería el proceso de firma electrónica :

La firma del mensaje:

1. El emisor crea el documento electrónico que desea firmar.

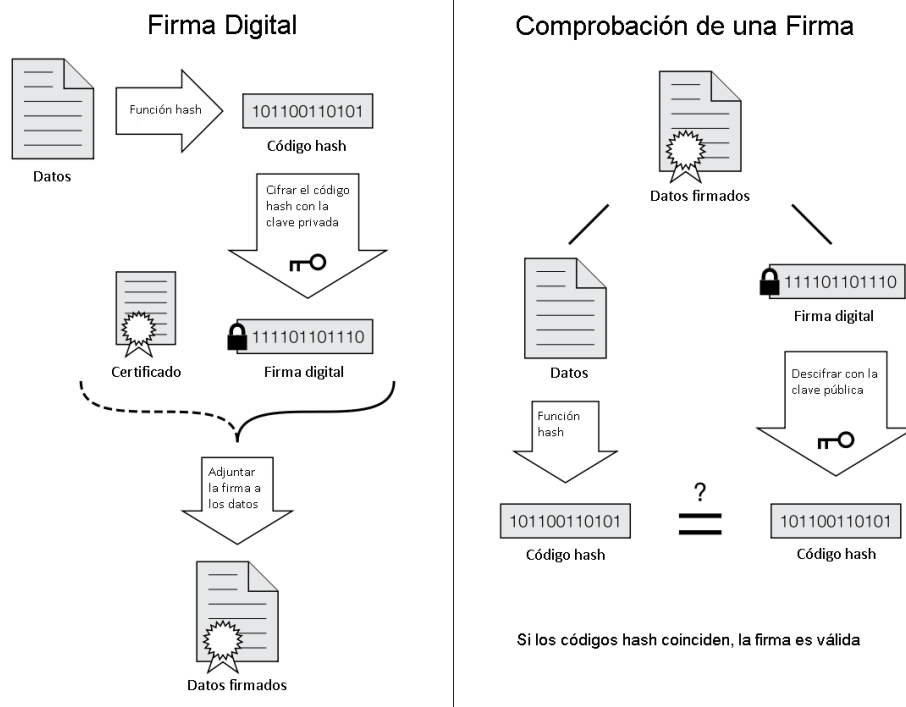


Figura 1.1: Proceso de firma digital.

2. El emisor aplica una función hash a ese documento y obtiene un resumen del mismo.
3. El emisor, utilizando su clave privada cifra dicho resumen.
4. El documento ya puede ser enviado, por tanto el emisor debería enviar lo siguiente:
 - El documento que quiere enviar en texto claro, es decir sin cifrar. Esto supone un problema de confidencialidad, que se puede arreglar cifrando el mensaje, pero con la clave pública del destinatario para que sólo él por medio de su clave privada pueda descifrarlo.
 - La firma del mensaje, que se compone del resumen generado por la función hash y cifrado con la clave privada del emisor y el certificado digital del emisor, que contiene los datos personales del emisor y su clave pública, que a su vez están cifrados con la clave privada del Prestador de Servicios de Certificación.

Verificación por parte del receptor de la firma del mensaje

1. El receptor recibe el mensaje del emisor.
2. El receptor primero tiene que descifrar el certificado digital cifrado por el Prestador de Servicios de Certificación, con la clave pública que el Prestador de Servicios de Certificación debe poner a disposición de los interesados.
3. Una vez que se ha descifrado el certificado, se puede obtener la clave pública del emisor y sus datos personales para comprobar quién es el que envía el mensaje.
4. Con la clave pública del emisor, se descifra el resumen hash que le ha sido enviado.
5. El receptor ahora debe volver a hacer el resumen del documento con la misma función hash que utilizó el emisor. Si el documento fue anteriormente cifrado con la clave pública del receptor para evitar problemas de confidencialidad, antes de realizar el resumen hay que descifrarlo con la clave privada del receptor.
6. El último paso es comparar los dos resúmenes o hash, el que se ha recibido con el que se ha generado. Si coinciden entonces se deduce que:
 - El mensaje no ha sufrido alteración durante su transmisión, es decir cumple con la integridad de los datos.
 - El resumen recibido que se ha descifrado con la clave pública del emisor ha tenido que ser necesariamente cifrado con la clave privada del emisor y, por tanto, ha de provenir necesariamente de él.
 - Como el certificado digital nos dice quién es el emisor, podemos concluir que el mensaje ha sido firmado digitalmente por dicho emisor, siendo el emisor una persona con identidad determinada y conocida.

Por el contrario, si los mensajes-resumen no coinciden quiere decir que el mensaje ha sido alterado por un tercero durante el proceso de transmisión, y si el mensaje-resumen descifrado por el receptor es ininteligible quiere decir que no ha sido cifrado

con la clave privada del emisor. En resumen, que el mensaje no es auténtico o que el mensaje no ha sido firmado por el emisor sino por otra persona.

1.1.6. Formatos de factura electrónica

Para trabajar con la facturación electrónica es necesario crear un fichero que contenga los datos de las facturas. No existen requisitos formales respecto a la forma en que se debe proceder a la codificación de la factura y puede estar en cualquier tipo de formato como pueden ser: .doc, xml, pdf, html, txt, etc. siempre que respete el contenido legal según la normativa vigente. Las modalidades más habituales en España son las siguientes:

- UBL: Su uso no solo se centra en la factura, sino que cuenta con una gran variedad de documentos de la cadena de suministro, e-commerce, leyes, administración, etc. Es un formato extendido internacionalmente; todo parece indicar que podría convertirse en el estándar europeo, ya que en su definición y desarrollo están participando un gran número de países.
- EDIFACT: Existen diferentes versiones por cada documento y utilización según cada país. Por ejemplo, para la factura en España se usa el INVOIC D93A y, en otros países como Francia y Portugal, se utiliza el INVOIC D96A. Actualmente se está trabajando para el uso generalizado para toda Europa de la versión INVOIC D01B. Su uso principalmente se ha basado en los sectores de automoción y distribución.
- FACTURAE: La Agencia Tributaria, (AEAT) se ha basado en este formato para definir el formato estándar CCI-AEAT (XML-CCI 1.2) para la factura electrónica. Su utilización no es masiva, pero es el formato que está impulsando la AEAT para la relación con sus proveedores. Actualmente se encuentra en su versión 3.1. En la siguiente sección vamos a ver con más detalle este formato porque es el que vamos a implementar en nuestra aplicación.

1.1.7. FacturaE v3.1

Para hablar de este formato primero vamos a explicar que es un XML Schema. XML Schema es un lenguaje de esquema escrito en XML, basado en la gramática y pensado para proporcionar una mayor potencia expresiva que las DTD, menos capaces al describir los documentos a nivel formal. Los documentos esquema (usualmente con extensión .xsd de XML Schema Definition (XSD)) se concibieron como una alternativa a las DTD, más complejas, intentando superar sus puntos débiles y buscar nuevas capacidades a la hora de definir estructuras para documentos XML. La principal aportación de XML Schema es el gran número de tipos de datos que incorpora. De esta manera, XML Schema aumenta las posibilidades y funcionalidades de aplicaciones de procesado de datos, incluyendo tipos de datos complejos como fechas, números y strings.¹ El formato FacturaE v3.1 sigue un XSD² que ha sido desarrollado por la AEAT y el MITyC en España. Para comprender mejor cómo es el formato, lo mejor es ver un ejemplo del XML de una factura con datos ficticios:

```
<?xml version="1.0" encoding="utf-8"?>
<Facturae xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="http://www.facturae.es/Facturae/2007/v3.1/Facturae">
  <!-- Encabezado de la factura -->
  <FileHeader xmlns="">
    <!-- Modalidad individual -->
    <Modality>I</Modality>
    <!-- Emitida por el Emisor -->
    <InvoiceIssuerType>EM</InvoiceIssuerType>
    <!-- Lote de factura -->
    <Batch>
      <BatchIdentifier>1</BatchIdentifier>
      <InvoicesCount>1</InvoicesCount>
      <TotalInvoicesAmount>
        <TotalAmount>68.08</TotalAmount>
      </TotalInvoicesAmount>
      <TotalOutstandingAmount>
        <TotalAmount>68.08</TotalAmount>
      </TotalOutstandingAmount>
      <TotalExecutableAmount>
```

¹http://es.wikipedia.org/wiki/XML_Schema

²<http://www.facturae.es/NR/rdonlyres/56F4132E-2AF9-41DD-AADC-CB412AE3F79C/0/1Facturaev31.xsd>

```
<TotalAmount>68.08</TotalAmount>
</TotalExecutableAmount>
<!-- Tipo de moneda: Euro -->
<InvoiceCurrencyCode>EUR</InvoiceCurrencyCode>
</Batch>
</FileHeader>
<Parties xmlns="">
  <!-- Datos del vendedor -->
  <SellerParty>
    <TaxIdentification>
      <!-- Tipo de persona jurídica-->
      <PersonTypeCode>J</PersonTypeCode>
      <!-- Tipo de residencia Residente -->
      <ResidenceTypeCode>R</ResidenceTypeCode>
      <TaxIdentificationNumber>12345678Z</TaxIdentificationNumber>
    </TaxIdentification>
    <LegalEntity>
      <CorporateName>Empresa S.L.</CorporateName>
      <!-- Direccion en España-->
      <AddressInSpain>
        <Address>Tulipan s/n</Address>
        <PostCode>28934</PostCode>
        <Town>Mostoles</Town>
        <Province>Madrid</Province>
        <CountryCode>ESP</CountryCode>
      </AddressInSpain>
      <!-- Datos de contacto -->
      <ContactDetails>
        <Telephone>913100505</Telephone>
        <TeleFax>913100506</TeleFax>
        <ElectronicMail>miguel@urjc.es</ElectronicMail>
        <ContactPersons>D. Miguel</ContactPersons>
      </ContactDetails>
    </LegalEntity>
  </SellerParty>
  <!-- Datos del comprador -->
  <BuyerParty>
    <TaxIdentification>
```

```
<!-- Tipo de persona física -->
<PersonTypeCode>F</PersonTypeCode>
<!-- Tipo de residencia Residente -->
<ResidenceTypeCode>R</ResidenceTypeCode>
<TaxIdentificationNumber>987654321A</TaxIdentificationNumber>
</TaxIdentification>
<Individual>
  <Name>Angel</Name>
  <FirstSurname>Montes</FirstSurname>
  <SecondSurname>Sanchez</SecondSurname>
  <!--Direccion en España-->
  <AddressInSpain>
    <Address>c/ Empecinado</Address>
    <PostCode>28937</PostCode>
    <Town>Alcorcon</Town>
    <Province>Madrid</Province>
    <CountryCode>ESP</CountryCode>
  </AddressInSpain>
  <!--Datos de contacto -->
  <ContactDetails>
    <Telephone>916460202</Telephone>
    <TeleFax>916460203</TeleFax>
    <ElectronicMail>angelmontes@gmail.com</ElectronicMail>
    <ContactPersons>Angel Montes</ContactPersons>
  </ContactDetails>
</Individual>
</BuyerParty>
</Parties>
<!--Facturas -->
<Invoices xmlns="">
  <Invoice>
    <!--Cabecera de factura -->
    <InvoiceHeader>
      <!-- Número de factura -->
      <InvoiceNumber>1</InvoiceNumber>
      <!-- Tipo factura: Factura completa -->
      <InvoiceDocumentType>FC</InvoiceDocumentType>
      <!-- Clase factura: Original -->
```

```
<InvoiceClass>00</InvoiceClass>
</InvoiceHeader>
<!-- Datos de emisión-->
<InvoiceIssueData>
  <!--Fecha-->
  <IssueDate>2009-01-26</IssueDate>
  <!-- Tipo de moneda: Euro-->
  <InvoiceCurrencyCode>EUR</InvoiceCurrencyCode>
  <!-- Tipo de moneda de impuestos: Euro-->
  <TaxCurrencyCode>EUR</TaxCurrencyCode>
  <!-- Idioma: Español -->
  <LanguageName>es</LanguageName>
</InvoiceIssueData>
<!-- Impuestos repercutidos-->
<TaxesOutputs>
  <!-- IVA 16 % -->
  <Tax>
    <TaxTypeCode>01</TaxTypeCode>
    <TaxRate>16.00</TaxRate>
    <TaxableBase>
      <TotalAmount>58.69</TotalAmount>
    </TaxableBase>
    <TaxAmount>
      <TotalAmount>9.39</TotalAmount>
    </TaxAmount>
  </Tax>
</TaxesOutputs>
<!-- Impuestos retenidos -->
<TaxesWithheld>
  <!-- IRPF 0 %-->
  <Tax>
    <TaxTypeCode>01</TaxTypeCode>
    <TaxRate>0.00</TaxRate>
    <TaxableBase>
      <TotalAmount>58.69</TotalAmount>
    </TaxableBase>
    <TaxAmount>
      <TotalAmount>0.00</TotalAmount>
    </TaxAmount>
  </Tax>
</TaxesWithheld>
```

```
</TaxAmount>
</Tax>
</TaxesWithheld>
<!-- Totales -->
<InvoiceTotals>
  <TotalGrossAmount>58.69</TotalGrossAmount>
  <TotalGrossAmountBeforeTaxes>58.69</TotalGrossAmountBeforeTaxes>
  <TotalTaxOutputs>9.39</TotalTaxOutputs>
  <TotalTaxesWithheld>0.00</TotalTaxesWithheld>
  <InvoiceTotal>68.08</InvoiceTotal>
  <TotalOutstandingAmount>68.08</TotalOutstandingAmount>
  <TotalExecutableAmount>68.08</TotalExecutableAmount>
</InvoiceTotals>
<!-- Lineas de factura -->
<Items>
  <InvoiceLine>
    <ItemDescription>Libro</ItemDescription>
    <!-- Cantidad -->
    <Quantity>1</Quantity>
    <!-- Precio -->
    <UnitPriceWithoutTax>58.690000</UnitPriceWithoutTax>
    <TotalCost>58.69</TotalCost>
    <GrossAmount>58.69</GrossAmount>
    <!-- Impuesto retenido linea -->
    <TaxesWithheld>
      <!-- IRPF 0 %-->
      <Tax>
        <TaxTypeCode>01</TaxTypeCode>
        <TaxRate>0.00</TaxRate>
        <TaxableBase>
          <TotalAmount>58.69</TotalAmount>
        </TaxableBase>
        <TaxAmount>
          <TotalAmount>0.00</TotalAmount>
        </TaxAmount>
      </Tax>
    </TaxesWithheld>
    <!-- Impuestos repercutidos-->
```

```
<TaxesOutputs>
  <!-- IVA 16 % -->
  <Tax>
    <TaxTypeCode>01</TaxTypeCode>
    <TaxRate>16.00</TaxRate>
    <TaxableBase>
      <TotalAmount>58.69</TotalAmount>
    </TaxableBase>
    <TaxAmount>
      <TotalAmount>9.39</TotalAmount>
    </TaxAmount>
  </Tax>
</TaxesOutputs>
</InvoiceLine>
</Items>
</Invoice>
</Invoices>
</Facturae>
```

Políticas de firma del modelo FacturaE:

El estándar XMLDSig ³ recoge las reglas básicas de creación y procesamiento de firmas electrónicas de documentos XML. Las firmas digitales XML (XMLDSIG) son firmas digitales diseñadas para su uso en transacciones XML. El estándar define un esquema para capturar el resultado de la firma digital aplicada a datos en XML.

Los elementos del XML son:

- Elemento Signature: Encapsula la firma digital.
- Elemento SignedInfo: Contiene la información necesaria para la creación y validación de la firma.
- Elemento CanonicalizationMethod: Especifica el algoritmo de transformación

³<http://www.w3.org/TR/xmlsig-core/xmlsig-core-schema.xsd>

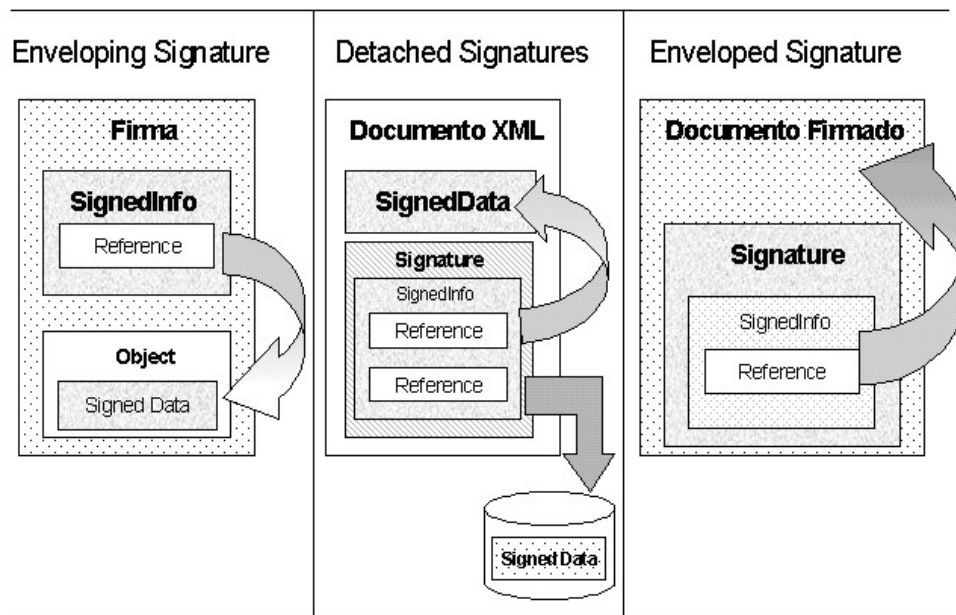


Figura 1.2: Estándar XMLDSig.

canónica aplicado al código XML de SignedInfo antes de realizar el cálculo de su firma digital.

- Elemento SignatureMethod: Referencia al algoritmo utilizado para el cálculo del valor de la firma digital.
- Elemento Reference: Referencia a la información o documento que se encuentra firmado.
- Elemento SignatureValue, contiene el valor de la Firma Digital.
- Elemento KeyInfo: Elemento opcional que permite a los receptores del mensaje obtener datos del certificado, como clave pública.
- Elemento Object: Elemento opcional que permite añadir información a la firma, por ejemplo, los datos que se van a firmar.

En relación con la situación de los datos que se van a firmar con respecto a su firma podemos tener la siguiente clasificación:

1. Enveloping Signature: La firma XML envuelve al contenido que se firma.
2. Detached Signature: El objeto que es firmado está separado de la firma XML.
3. Enveloped Signature: El contenido que se desea firmar engloba a la firma.

Este estándar se amplía con las especificaciones de XADES, donde se definen estructuras que permiten incorporar información adicional a la firma que facilita su validación.

Para las facturas FacturaE, se definen dos formatos de firma electrónica:

1. **Formato de firma electrónica avanzada básico:** Contiene los elementos mínimos y necesarios para que la firma se considere firma electrónica avanzada acorde con la Ley 59/2003, de 19 de diciembre, de firma electrónica. Este perfil se corresponde con una firma XADES-EPES del estándar XADES ETSI TS 101 903 v1.2.2. A su vez se corresponde con el perfil de Firma Básico XMLDsig, al que se le ha añadido información sobre la Política de Firma.
2. **Formato de firma electrónica avanzada con información de validación** Se incorporan propiedades de firma del estándar XADES al formato básico con objeto de proporcionar evidencias suficientes que garanticen la validez de la firma de la factura ante terceros. Este perfil se corresponde con una firma XADES-XL del estándar XADES ETSI 101 903 v1.2.2 .

Capítulo 2

Objetivos

Una vez realizado el estudio del arte de la factura electrónica, en este capítulo vamos a describir qué objetos se persiguen en la realización de este proyecto. El objetivo principal, es realizar un sistema de facturación electrónica que implemente un formato estándar, que firme digitalmente facturas y además compruebe que dicha firma es correcta. Tras analizar los principales estándares de formatos que existen en la actualidad, UBL, EDIFact y FacturaE, en esta aplicación vamos a implementar una solución basada en el formato FacturaE en su versión 3.1. Se ha elegido este formato, porque es el que la AEAT está impulsando para que sea el estándar en España.

2.1. Descripción del problema

Como hemos visto en el capítulo anterior, el sistema de facturación tradicional actual presenta una serie de carencias y desventajas con respecto al nuevo modelo de facturación electrónica. Esta aplicación pretende dar una solución a estos problemas, desarrollando una aplicación de facturación electrónica.

El objetivo principal del proyecto lo hemos dividido en varios subobjetivos que enumeramos a continuación:

- Desarrollar una biblioteca de clases que nos permita generar ficheros XML con el formato FacturaE v3.1 cumpliendo con la especificación de su esquema XSD.
- Desarrollar un componente de firma electrónica, que nos permita firmar digitalmente ficheros XML y verificar la firma en los documentos previamente firmados.
- Desarrollar una interfaz gráfica de usuario que permita generar facturas electrónicas y la posibilidad de verificar la firma digital en las facturas.

2.2. Requisitos

Para el desarrollo de la aplicación hemos definido una serie de requisitos que nuestra aplicación final tiene que cumplir y nos van a guiar en el proceso de desarrollo de la aplicación final.

1. **REQ01:** La aplicación tiene que dar de alta una factura electrónica, siguiendo el formato FacturaE v3.1. La factura tiene que contener los datos necesarios para que la factura tenga validez legal, es decir, tiene que incluir los datos del emisor de la factura, los datos del receptor de la factura, la fecha de emisión de la factura, un número distintivo de factura, los datos de los productos de la factura, incluyendo la descripción del producto, la cantidad, el precio neto, y el tipo y valor de los impuestos de cada uno de los productos que forman la factura.
2. **REQ02:** La aplicación tiene que poder abrir una factura guardada en formato FacturaE v3.1 y modificar su contenido.
3. **REQ03:** La aplicación tiene que poder guardar una factura en formato FacturaE v3.1 en un fichero XML.
4. **REQ05:** La aplicación tiene que permitir firmar electrónicamente una factura, con un certificado digital seleccionado por el usuario.

5. **REQ06:**La aplicación tiene que poder comprobar la validez de la firma electrónica de un fichero XML firmado digitalmente.

2.3. Metodología empleada

Para realizar este proyecto hemos seleccionado el *modelo en espiral basado en prototipos*. En la siguiente sección vamos a explicar en qué consiste este modelo de desarrollo y cómo lo hemos puesto en práctica en nuestro proyecto.

2.3.1. Desarrollo en espiral

En este modelo de desarrollo el producto final es creado a partir de varias iteraciones, que pasan por distintas fases del ciclo de desarrollo, generando varios prototipos o mini proyectos.

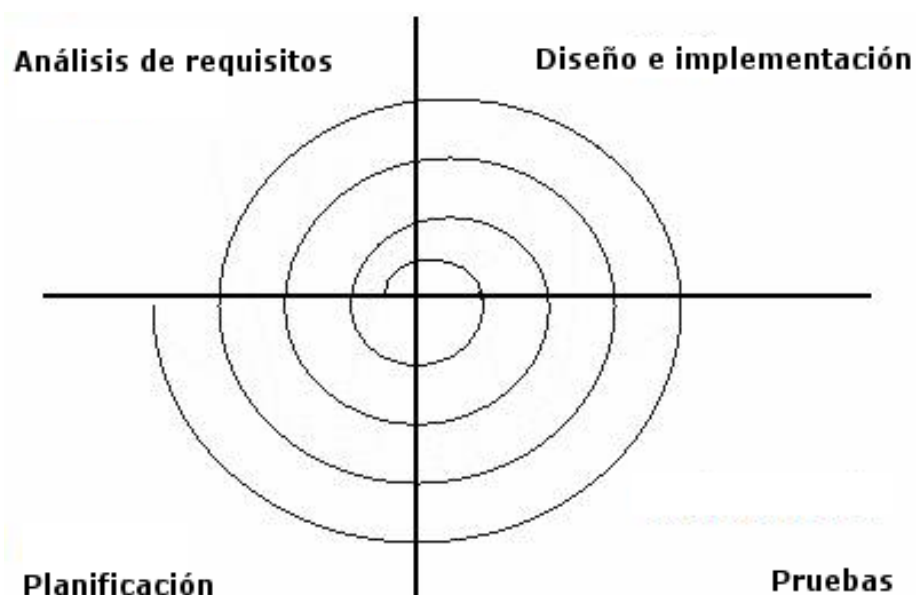


Figura 2.1: Modelo de desarrollo en espiral.

Las fases de desarrollo por las que tienen que pasar cada uno de los prototipos son las siguientes:

- **Análisis de Requisitos:** Durante esta fase se analizan los requisitos que tiene que cumplir el prototipo.
- **Diseño e Implementación:** Durante esta fase se hace un diseño del prototipo y se implementa para que cumpla con las especificaciones de los requisitos.
- **Pruebas:** En esta fase, se comprueba el funcionamiento del prototipo.
- **Planificación:** En el que se comprueba el estado general del proyecto y se planifica la siguiente iteración.

Una vez tenemos creado un prototipo, se vuelve a repetir el mismo proceso para la realización de otro nuevo prototipo, al que se añaden nuevas funcionalidades, y se repite el proceso hasta completar el desarrollo completo. Este modelo de desarrollo nos proporciona una gran flexibilidad a la hora de ir incorporando nuevas funcionalidades y nuevos requisitos a nuestra aplicación final.

En nuestro proyecto este sistema encaja a la perfección, porque hemos generado varios componentes independientes, que son utilizados por la aplicación final. A continuación vamos a enumerar los prototipos que hemos generado para completar nuestra solución final.

- **Prototipo 1: FacturaE.** En este prototipo hemos realizado una biblioteca de clases que modelan el formato FacturaE v3.1, siguiendo su esquema XSD.
- **Prototipo 2: FirmaDigital.** Con este prototipo hemos generado un componente de firma digital, que nos va a permitir firmar documentos XML y verificar las firmas digitales en documentos previamente firmados. En este proyecto, hemos implementado la firma digital siguiendo dos estándares: XMLDsig y XADES.
- **Prototipo 3: Facturación.** En este tercer prototipo creamos la *Capa Lógica* de nuestra aplicación. Esta biblioteca, es la responsable de comunicar la interfaz de

usuario con el resto de componentes.

- **Prototipo 4: Facturación Electrónica.** Con este prototipo creamos la *Interfaz de Usuario*. Este componente es la parte gráfica de la aplicación, desde la cuál el usuario va a interactuar con el sistema.

- **Prototipo 5: Refactorización de la aplicación.** Una vez tenemos desarrollado nuestro sistema completo, que satisface los requisitos especificados, pensamos en la reutilización y escalabilidad del software y optimizamos nuestra aplicación, para permitir incluir nuevos formatos de facturación electrónica y firma digital haciendo uso de los patrones de diseño *Factory* y *Strategy*.

Capítulo 3

Descripción informática

En este capítulo se presentará el diseño de nuestra aplicación, se mostrarán todas las clases e interfaces así como sus relaciones. Además se hará una descripción técnica de los patrones de diseño utilizados.

3.1. Arquitectura general de la aplicación

Para el desarrollo de nuestra aplicación final, hemos desarrollado varios componentes independientes entre sí. Cada uno de estos componentes los podemos agrupar en tres capas lógicas bien diferenciadas atendiendo a una arquitectura de tipo *n Layer*, en la cual cada capa engloba una funcionalidad distinta. Nosotros hemos definido tres capas: La capa de interfaz de usuario, la capa lógica de nuestra aplicación y una tercera capa con los componentes de firma digital y formatos de facturación como podemos ver en la figura 3.1

Siguiendo buenas prácticas de programación hemos tratado de resolver varios problemas utilizando *Patrones de diseño*. Estos patrones, resuelven problemas que se dan con frecuencia en el desarrollo de software y nos dan las pautas para resolver estos problemas de una buena manera.

A continuación vamos a enumerar qué patrones hemos utilizado y cómo nos han servido en nuestro desarrollo:

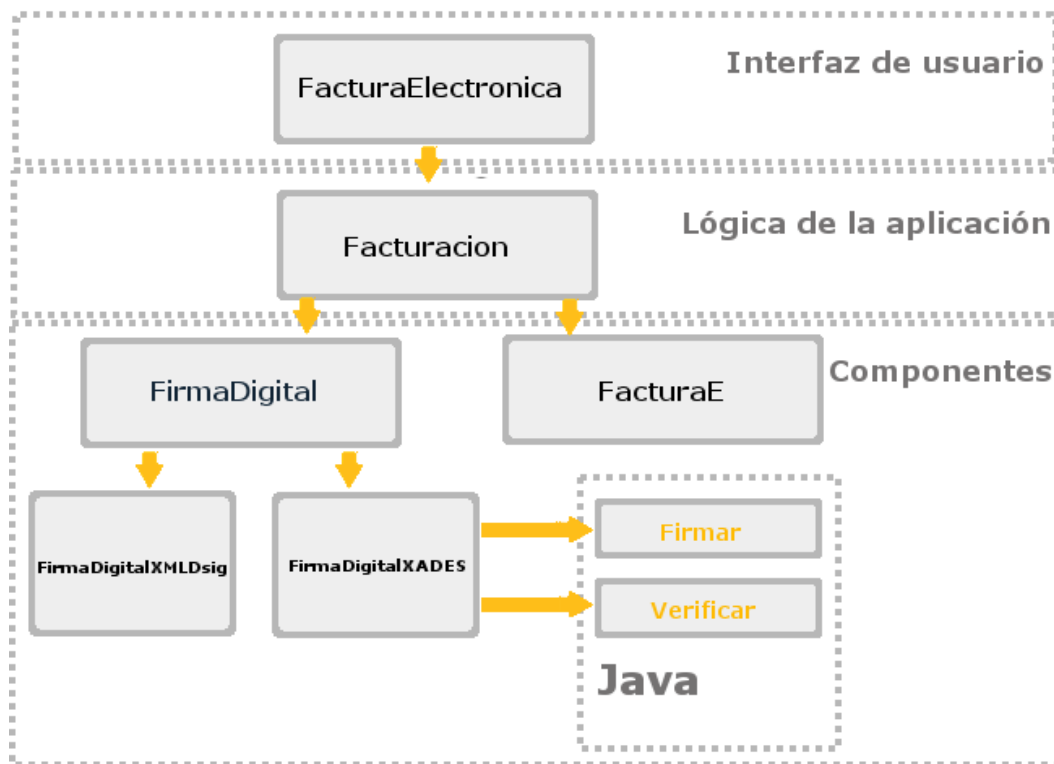


Figura 3.1: Esquema de la aplicación.

▪ Factory Method

Implementando este patrón, se delega la responsabilidad de crear un tipo concreto de objeto a otro objeto denominado `Factoria`. En nuestro caso, utilizamos este patrón para crear el objeto adecuado de tipo `FormatoFactura` y `FirmaDigital`, para poder incorporar de forma sencilla nuevos formatos o nuevos sistemas de firma digital pensando en la escalabilidad de la aplicación. De esta forma nuestras `factorias`, serán las encargadas de crearnos los objetos adecuados que le indiquemos. En la aplicación, esta especificación la realizamos a través del fichero de configuración de la aplicación por medio de los parámetros `FormatoFactura` y `FirmaDigital`.

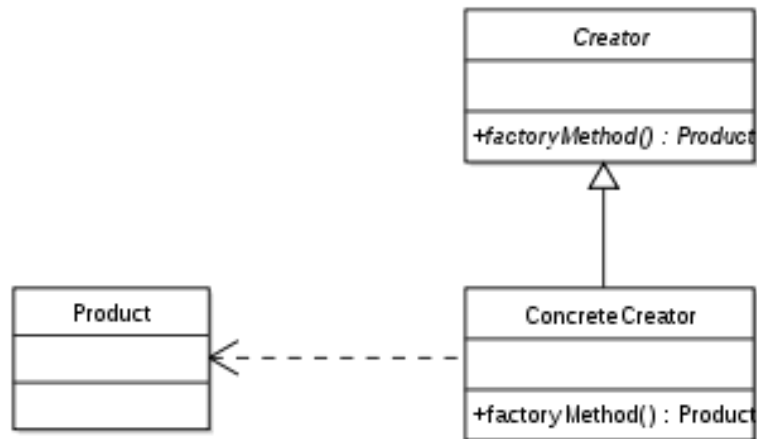


Figura 3.2: Patrón Factory Method.

▪ Singleton

Este patrón nos permite asegurarnos que sólo exista una única instancia de una clase en la aplicación. En nuestro desarrollo, es una buena idea que sólo exista una única clase *Factoria*, que nos genere nuestros objetos, por eso nuestras clases de factoria implementan este patrón.

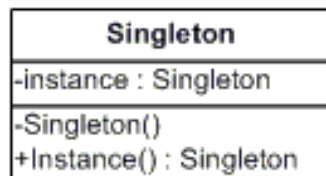


Figura 3.3: Patrón Singleton.

▪ Patrón Strategy

Este patrón resuelve el problema de decidir qué implementación de un determinado método utilizar en un caso concreto, entre una serie de objetos que comparten una interfaz común. Nosotros utilizamos este patrón junto con el **Factory Method** para ejecutar el método adecuado en la implementación de un formato de factura o de un tipo de firma digital.

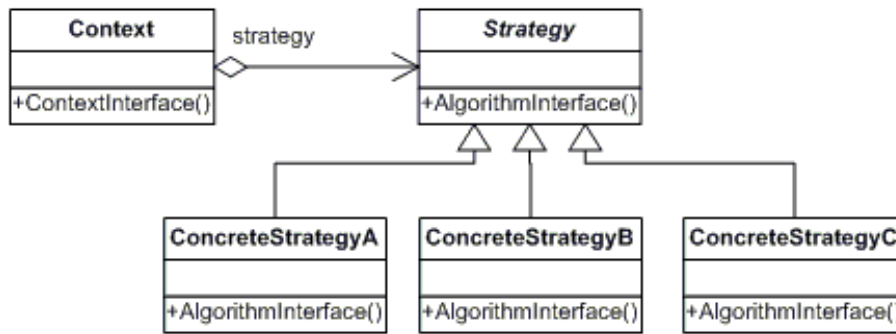


Figura 3.4: Patrón Strategy.

Una vez hemos descrito la arquitectura general de la aplicación, en las siguientes secciones vamos a analizar en detalle cada uno de los componentes que forman nuestra aplicación.

3.2. Componente FacturaE

3.2.1. Especificación

Nuestro componente FacturaE, es el responsable de modelar facturas electrónicas con el formato FacturaE en su versión 3.1.

3.2.2. Diseño e Implementación

Para implementar el formato FacturaE, tenemos que ceñirnos al XSD del formato FacturaE v3.1. Debido a que es un esquema bastante extenso que nos va a permitir generar varios tipos de factura, a saber: Individual, Lote, Completa, Abreviada, Autofactura, Anticipo, Original, Recitficativa, Recapitulativa, Copia, etc. pensamos en que lo mejor sería hacer uso de la *Serialización*. La serialización (o marshalling) consiste en el proceso de codificación de un Objeto en un medio de almacenamiento (como puede ser un archivo) en un formato humanamente más legible como XML o JSON, entre otros. La serialización

es un mecanismo ampliamente usado para transportar objetos a través de una red, para hacer persistente un objeto en un archivo o base de datos, o para distribuir objetos idénticos a varias aplicaciones o localizaciones. Por cada nodo del esquema, hemos creado una clase que nos va a permitir representar el esquema completo en un fichero XML.

En la figura 3.5 tenemos el esquema con el conjunto de las clases principales que forman una factura:

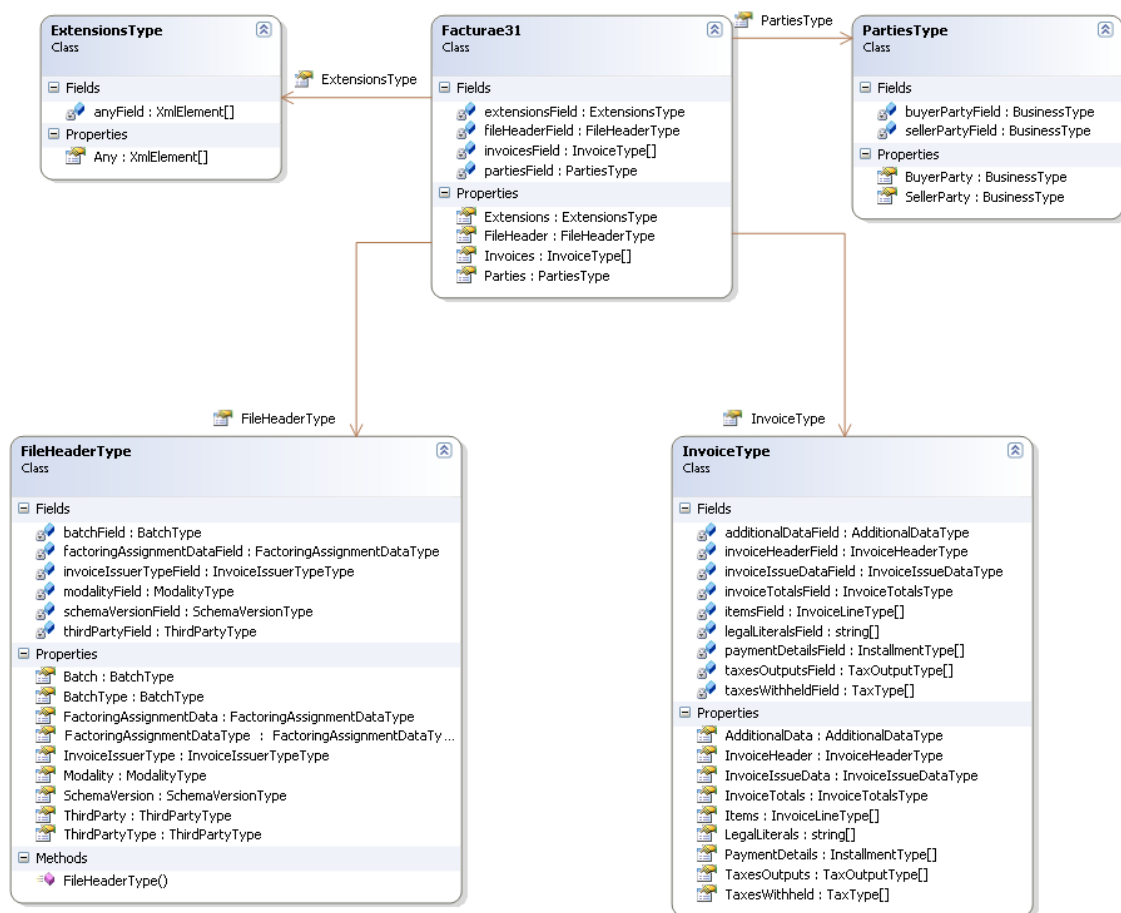


Figura 3.5: Esquema de las clases de una factura.

Facturae31

Esta clase es el elemento origen del fichero de facturas FacturaE.

ExtensionsType

Esta clase representa las extensiones de la factura. Las extensiones sirven para poder incorporar nuevas definiciones estructuradas cuando sean de interés conjunto para emisores y receptores, y no estén ya definidas en el esquema de la factura.

FileHeaderType

Esta clase agrupa los elementos de la cabecera del fichero XML. Aquí se definen el tipo de emisor de la factura, el tipo de modalidad, la versión del esquema, el lote de la factura con el número de facturas que componen el lote, el tipo de moneda utilizada, y los totales, y si la factura está generada por una tercera parte, los datos de esa tercera parte.

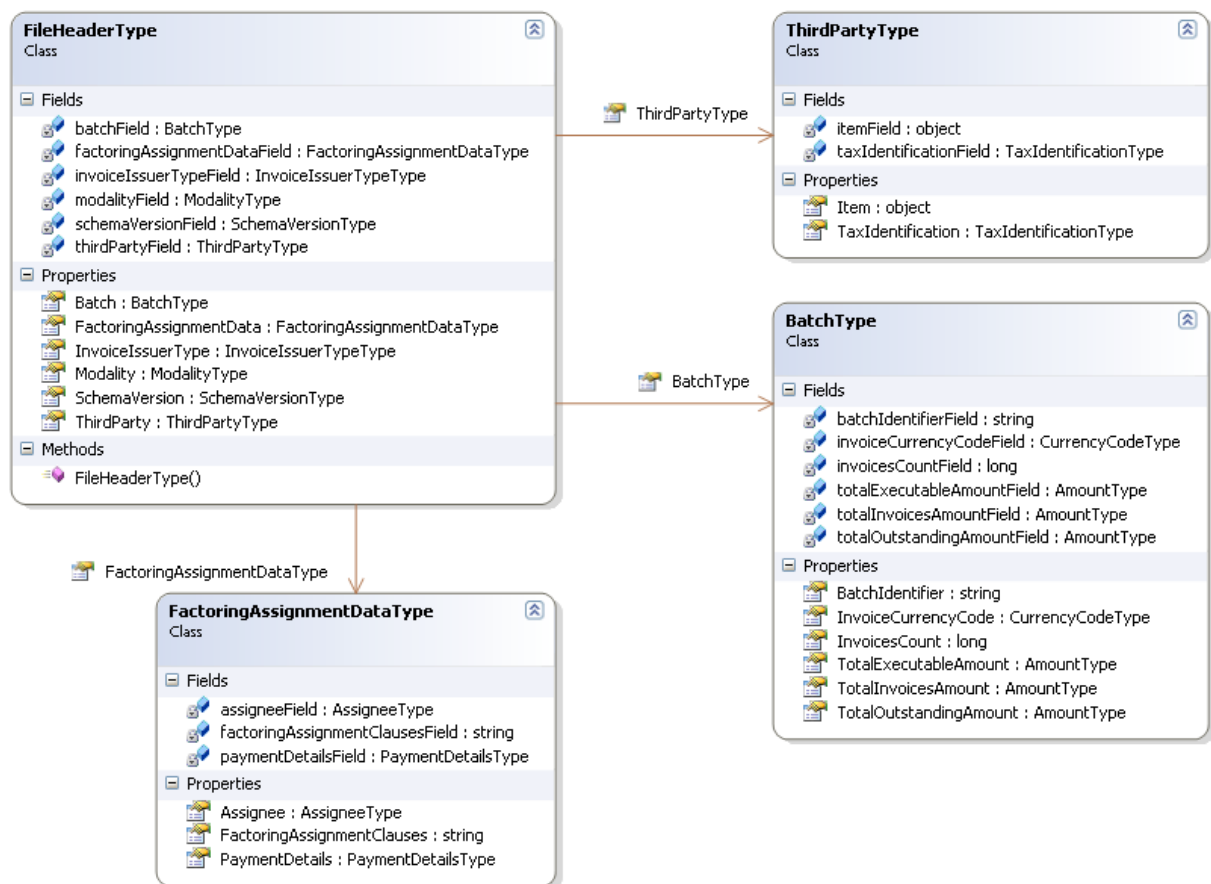


Figura 3.6: Esquema de las clases *FileHeaderType*.

PartiesType

Esta clase está compuesta del conjunto de clases que representan al emisor y al receptor de la factura. En esta sección se detallan los datos identificativos de emisor y receptor, a saber: tipo de persona (Física o Jurídica), nombre, identificación fiscal, datos registrales (tomo, libro, folio, sección, etc.), dirección completa en España o de otro país, datos de contacto (persona, email, teléfono, fax), etc.

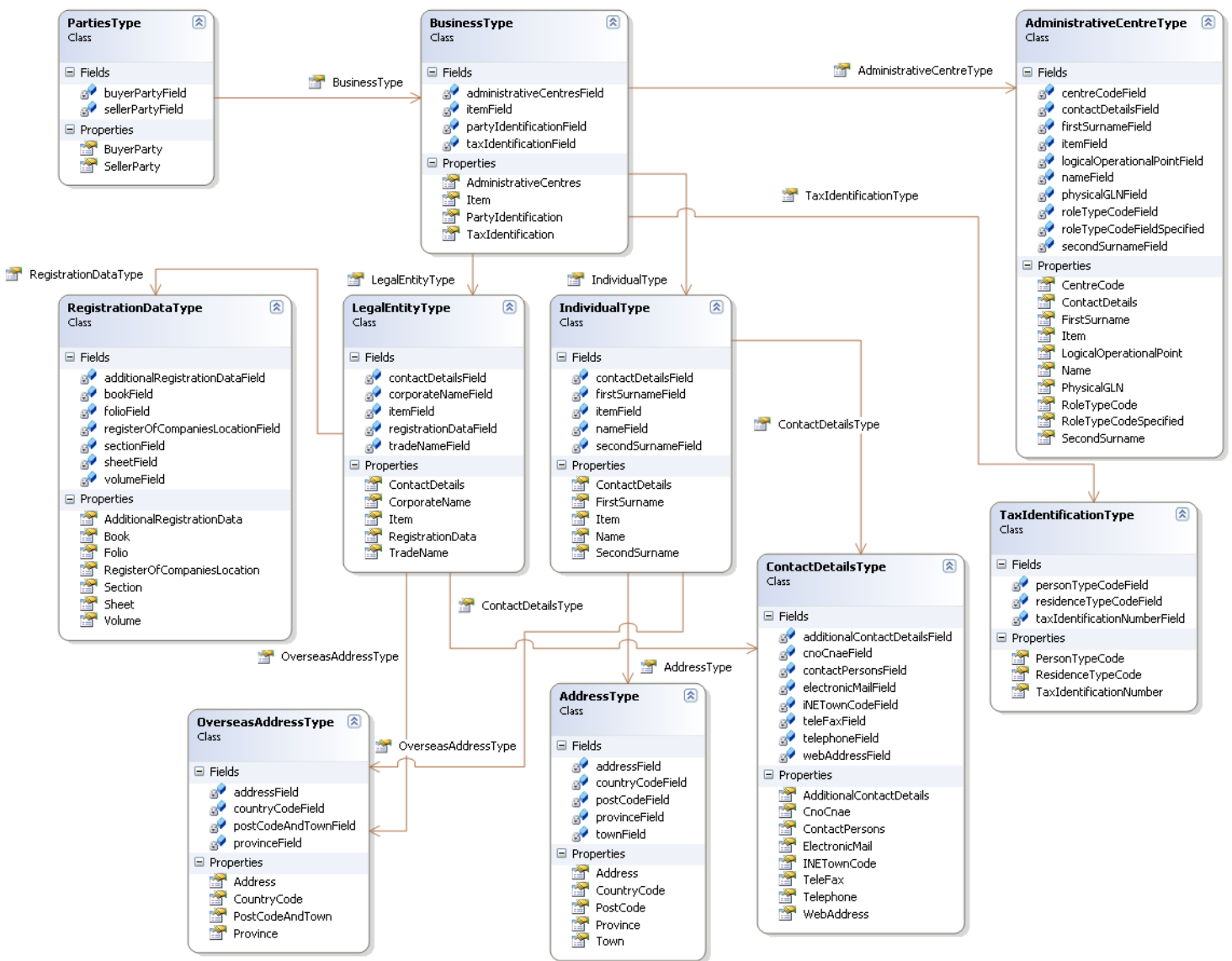


Figura 3.7: Esquema de las clases *PartiesType*.

InvoiceType

Esta clase está compuesta del conjunto de clases que representan los datos de una factura, como son los importes totales de la factura, los importes netos, los totales de impuestos repercutidos, los totales de impuestos retenidos, los descuentos, el número de factura, los detalles de pago, el tipo de factura emitida, etc.

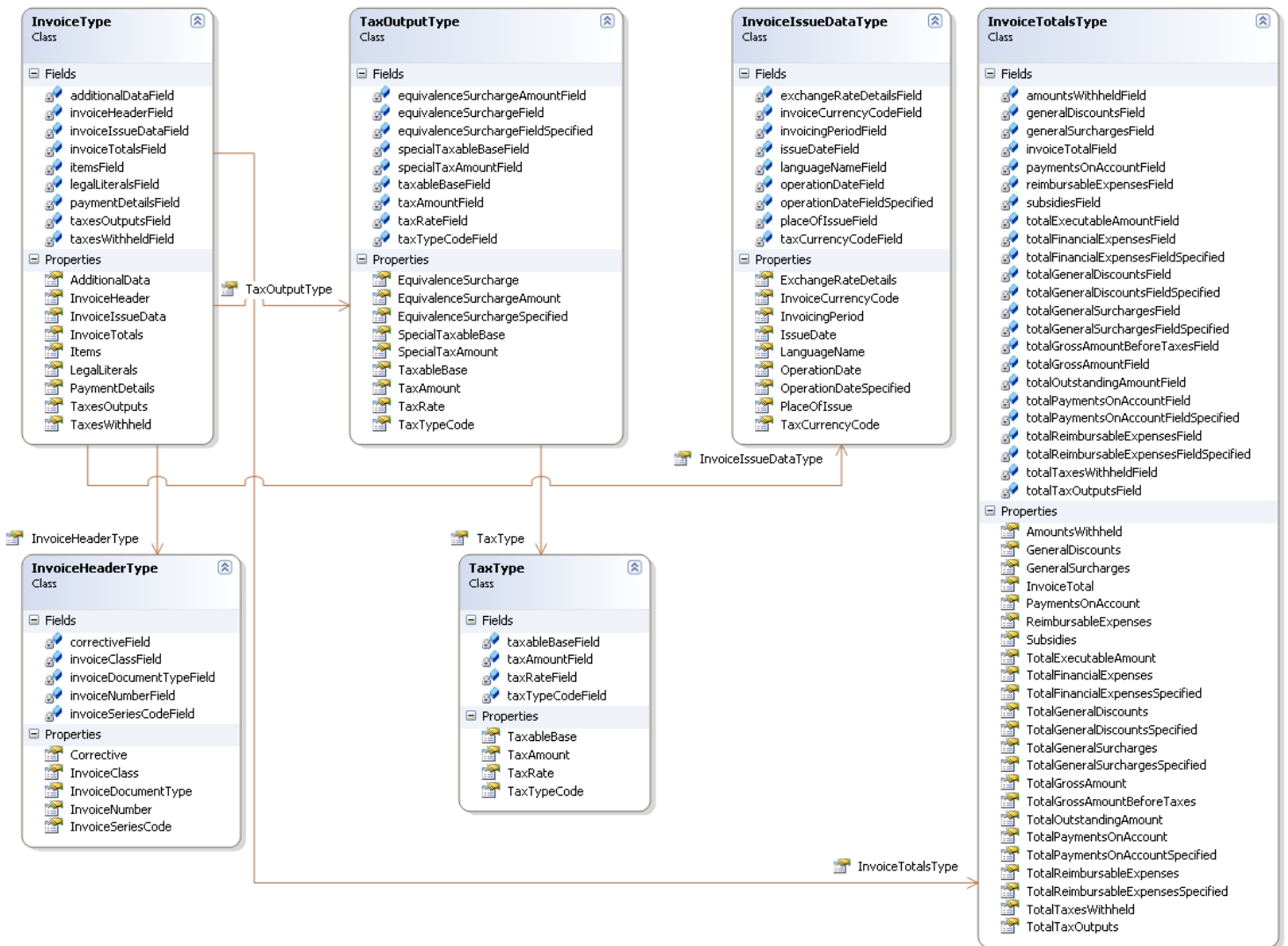


Figura 3.8: Esquema de las clases *InvoiceType*.

InvoiceLineType

Esta clase está compuesta del conjunto de clases que representan los datos de una línea de factura, como son la descripción del artículo, la cantidad de artículos, el precio unitario, el importe total, el importe neto, el total de impuestos repercutidos, el total de impuestos retenidos, los descuentos, los cargos, etc.

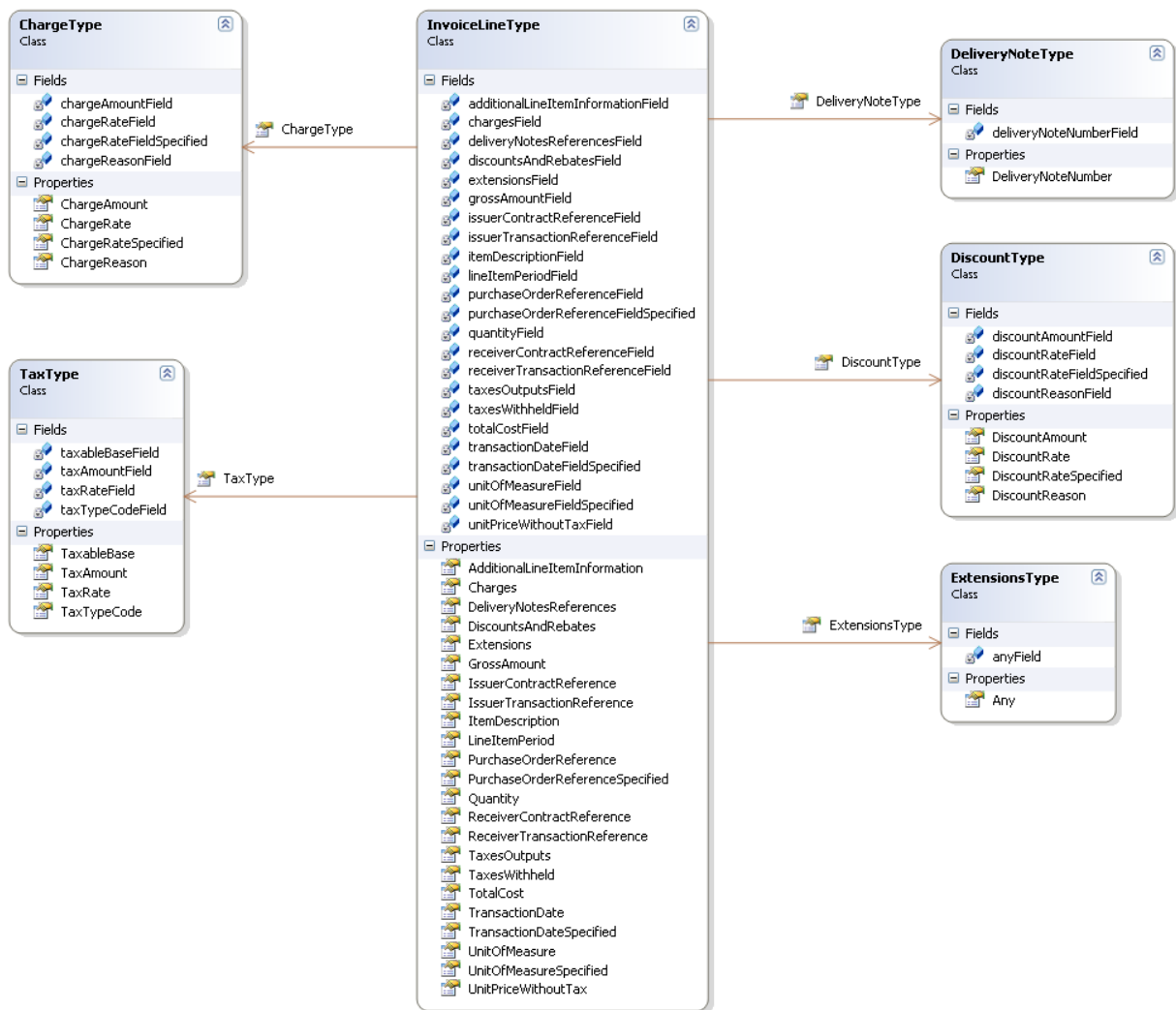


Figura 3.9: Esquema de las clases *InvoiceLineType*.

Enums

Esta clase recoge los distintos tipos de datos enumerados del formato Facturae, que son los siguientes:

- **SchemaVersionType:** Código que indica la versión utilizada.
- **ModalityType:** Tipo de modalidad. Individual o Lote. Si es individual (I) los importes de los campos del grupo Batch coincidirán con sus correspondientes campos del grupo InvoiceTotals y el campo InvoicesCount tendrá siempre el valor 1. Si es lote (L), el valor del campo InvoicesCount será siempre > 1.
- **InvoiceIssuerTypeType:** Tipo Emisor Factura. Actor que firma la factura. Si toma el valor TE el grupo ThirdParty será obligatorio cumplimentarlo en todos sus apartados.
- **PersonTypeCodeType:** Tipo de persona. Física o Jurídica. F - Física; J -Jurídica.
- **ResidenceTypeCodeType:** Identificación del tipo de residencia y/o extranjería. E - Extranjero; R - Residente; U - Residente en la Unión Europea.
- **AttachmentCompressionAlgorithmType:** Algoritmo usado para comprimir el documento adjunto.
- **AttachmentFormatType:** Formato del documento adjunto.
- **AttachmentEncodingType:** Algoritmo usado para codificar el documento adjunto.
- **CountryType:** Código País. Código según la ISO 3166-1:2006 Alpha-3.
- **PaymentMeansType:** Medio de pago concreto para cada vencimiento/importe.

- **UnitOfMeasureType:** Unidad en que está referida la Cantidad. Recomendación 20, Revisión 4 y Recomendación 21, Revisión 5 de UN/CEFACT.
- **TaxTypeCodeType:** Clase de impuesto. Concepto fiscal por el que se tributa o retención a cuenta. Cuando haya lugar, debe recogerse en el elemento observaciones el motivo por lo que este impuesto está no sujeto o exento.
- **CurrencyCodeType:** Código ISO 4217:2001 Alpha-3 de la moneda en la que se emite la factura. Si difiere de la moneda EURO o del campo ExchangeRateDetails será obligatorio indicar el contravalor y el tipo/fecha de cambio para los campos de base imponible y cuota, retenida como repercutida, así como en los totales TotalInvoicesAmount, TotalOutstandingAmount, y TotalExecutableAmount.
- **LanguageCodeType:** Lengua. Código ISO 639-1:2002 Alpha-2 de la lengua en la que se emite el documento.
- **ReasonCodeType:** Código del motivo. Código numérico del motivo de rectificación. 01 a 16 errores según reglamento RD 1496/2003; 80 a 85 errores según Artº 80 Ley 37/92 el IVA.
- **ReasonDescriptionType:** Descripción motivo. Descripción del motivo de rectificación y que se corresponde con cada código
- **CorrectionMethodType:** Código numérico que identifica el criterio empleado en cada caso para una rectificación.
 1. se reflejan todos los detalles a rectificar de la factura original.
 2. sólo se anotan los detalles ya rectificadas.
 3. Rectificación por descuento por volumen de operaciones durante un periodo.
 4. Autorizadas por la Agencia Tributaria.

- **CorrectionMethodDescriptionType:** Descripción del criterio asociada al código indicado en el campo anterior.
 1. Rectificación modelo íntegro.
 2. Rectificación modelo por diferencias.
 3. Rectificación por descuento por volumen de operaciones durante un periodo.
 4. Autorizadas por la Agencia Tributaria.

- **InvoiceDocumentTypeType:** Tipo documento factura. Puede ser una factura completa, abreviada, autofactura, anticipo, tique... En este estándar no se van a contemplar el anticipo y el tique.

- **InvoiceClassType:** Clase de Factura. Este dato refleja la clase de factura, a saber: OO - Original, OR - rectificativa, OC - original recapitulativa, CO - copia de la original, CR - copia de la rectificativa, CC - copia recapitulativa. Una factura rectificativa sólo puede rectificar a una factura original, o bien realizar un abono por volumen correspondiente a un periodo diferido, o algún otro motivo autorizado por la Agencia Tributaria. Cuando la clase se corresponda con alguno de los valores OR ó CR (rectificativas), deberán estar cumplimentados los campos del grupo Corrective.

- **RoleTypeCodeType:** Tipo rol. Indica la función de un Punto Operacional (P.O.) definido como Centro/Departamento. Estas funciones son: Receptor - Centro del NIF receptor destinatario de la factura. Pagador - Centro del NIF receptor responsable de pagar la factura. Comprador - Centro del NIF receptor que emitió el pedido. Cobrador - Centro del NIF emisor responsable de gestionar el cobro. Fiscal - Centro del NIF receptor de las facturas, cuando un P.O. buzón es compartido por varias empresas clientes con diferentes NIF.s y es necesario diferenciar el receptor del mensaje (buzón común) del lugar donde debe depositarse (empresa destinataria).

3.3. Componente FirmaDigital

3.3.1. Especificación

Este componente es el encargado de realizar el proceso de la firma digital en ficheros XML y verificar la validez de la firma. En una primera fase del desarrollo de este componente, implementamos una firma digital del estándar XMLDsig. En la fase de pruebas, comprobamos que este estándar no cumplía con la política de firma del formato FacturaE, que requiere implementar una firma digital avanzada del estándar Xades. En la actualidad, la plataforma .Net no dispone de ningún mecanismo criptográfico que nos permita implementar este estándar, por este motivo desarrollamos dicha funcionalidad en la plataforma JAVA, haciendo uso de la API XADES ¹ que el Ministerio de Industria Turismo y Comercio de España ha puesto a disposición de los desarrolladores para implementar dicho estándar.

3.3.2. Diseño e Implemetación

Este componente implementa los patrones de diseño Singleton, Factory Method y Strategy, que hemos visto anteriormente. En la figura 3.10 podemos ver el esquema general de las clases que forman este componente.

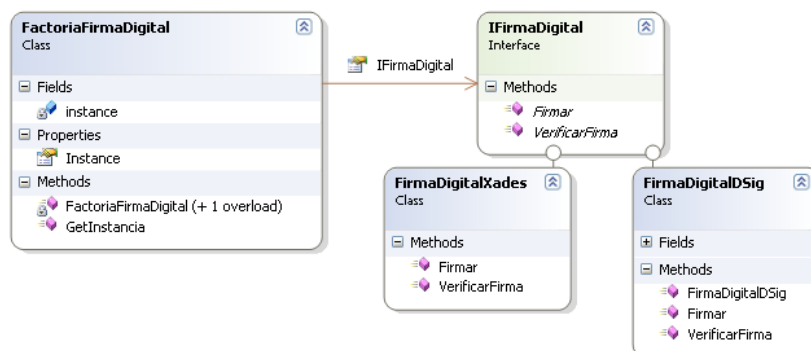


Figura 3.10: Esquema de clases de FirmaDigital.

¹<http://www.facturae.es/Descargas/Desarrollo/>

FactoriaFirmaDigital

Esta clase, a través de su única instancia ya que implementa el patrón `Singleton`, nos devuelve un objeto de tipo `IFirmaDigital`, dependiendo del parámetro `FirmaDigital` del fichero de configuración de la aplicación. Si el parámetro es `Xades`, nos crea un objeto `FirmaDigitalXades`, o si el parámetro es `Dsig` nos creará un objeto `FirmaDigitalDsig`.

IFirmaDigital

En esta interfaz definimos el comportamiento que han de tener las clases que implementen un algoritmo de firma digital. Definimos dos métodos, `Firmar` que recibe como parámetro el path del fichero a firmar y `Verificar`, que recibe como parámetro el path del fichero del cual se quiere verificar su firma.

FirmaDigitalDsig

Esta clase implementa la interfaz `IFirmaDigital`, y nos proporciona un sistema de firma XML simple XMLDsig.

FirmaDigitalXades

Esta clase implementa la interfaz `IFirmaDigital`, y hace uso de dos componentes Java `Firmar` y `Verificar` para proporcionar una firma digital avanzada Xades.

Firmar

Esta aplicación Java, se utiliza para firmar una factura. La aplicación está empaquetada como un fichero jar, para que pueda ser lanzada como un proceso independiente desde la aplicación principal. Consta de una única clase, la clase `Firmar`. Esta clase hace uso de las siguientes librerías jar:

1. activation.jar
2. commons-logging-1.1.jar
3. Facturae-API.jar
4. Facturae-API_CompPack.jar
5. FacturaEBridge.jar
6. jaxb-api.jar
7. jaxb-impl.jar
8. jsr173_1.0_api.jar
9. LibXADESJNI_IE_W.jar
10. log4j-1.2.15.jar
11. swing-layout-1.0.3.jar

Nuestra clase contiene un único método **main**, que recibe estos argumentos desde la entrada estándar:

- `args[0]`: Fichero que se quiere firmar.
- `args[1]`: Fichero firmado.
- `args[2]`: Fichero de errores.

y llama a la función `es.mityc.facturae.utils.SignatureUtil.sign(String pathIn, String pathOut)`, que muestra un listado de los certificados digitales instalados en el sistema, y una vez seleccionamos uno, firma el fichero con ese certificado cuyo path es `pathIn` y lo guarda en el path `pathOut`.

Si ocurre algún error durante el proceso de firma, se captura una excepción y se escribe en un fichero de errores.

Verificar

Esta aplicación Java, se utiliza para verificar la firma digital de una factura. La aplicación está empaquetada como un fichero jar, para que pueda ser lanzada como un proceso independiente. Consta de una única clase, la clase **VerificarFirma**, que hace uso del mismo conjunto de librerías Xades de la aplicación **Firmar**.

La clase está compuesta por los siguientes métodos:

```
public static void main(String[] args)
```

Este método es el punto de inicio de la aplicación y recibe como argumentos desde la entrada estándar:

- args[0]: Path del fichero firmado.
- args[1]: Path del fichero resultados, que contiene el resultado de la validación de la firma y es utilizado por la aplicación principal.

```
public void validarFichero(String ruta, String ficheroResultado)
```

Este método llama al método **validar** de la clase **ValidarFirmaXML** y le pasa como parámetro el path del fichero a validar y devuelve un objeto **ResultadoValidacion** con los datos de la validacion.

```
private void EscribirDatosFirmaXADES(ResultadoValidacion datos, FileWriter  
fResult)
```

Este método escribe en el fichero fResult los resultados del objeto **ResultadoValidacion**, que contiene la firma y los datos del certificado. Los resultados que obtenemos son los siguientes:

1. **Nivel:** Nos dice el último nivel válido de la firma.
2. **Fecha:** Nos dice la fecha en la que se realizó la firma.
3. **Emitido para:** Nos dice el nombre del propietario del certificado.
4. **Emitido por:** Nos dice el nombre de la autoridad certificadora que emitió el certificado.
5. **Datos OCSP:** Nos dice el estado de revocación del certificado digital.
6. **Sello de tiempo:** Si lleva sello temporal, nos indica el emisor y la fecha.
7. **Rol:** Nos dice el tipo de rol que cumple el firmante.

3.4. Componente Facturación

3.4.1. Especificación

Este componente es un conjunto de clases que modelan los objetos principales de una factura y son los responsables de la lógica de la aplicación. La interfaz de usuario se comunica directamente con esta capa que es la encargada de interactuar con el resto de los componentes y realizar las acciones del usuario.

3.4.2. Diseño e Implemetación

Este componente implementa los patrones de diseño **Singleton**, **Factory Method** y **Strategy**. En la figura 3.11 podemos ver el esquema general de las clases que forman este componente.

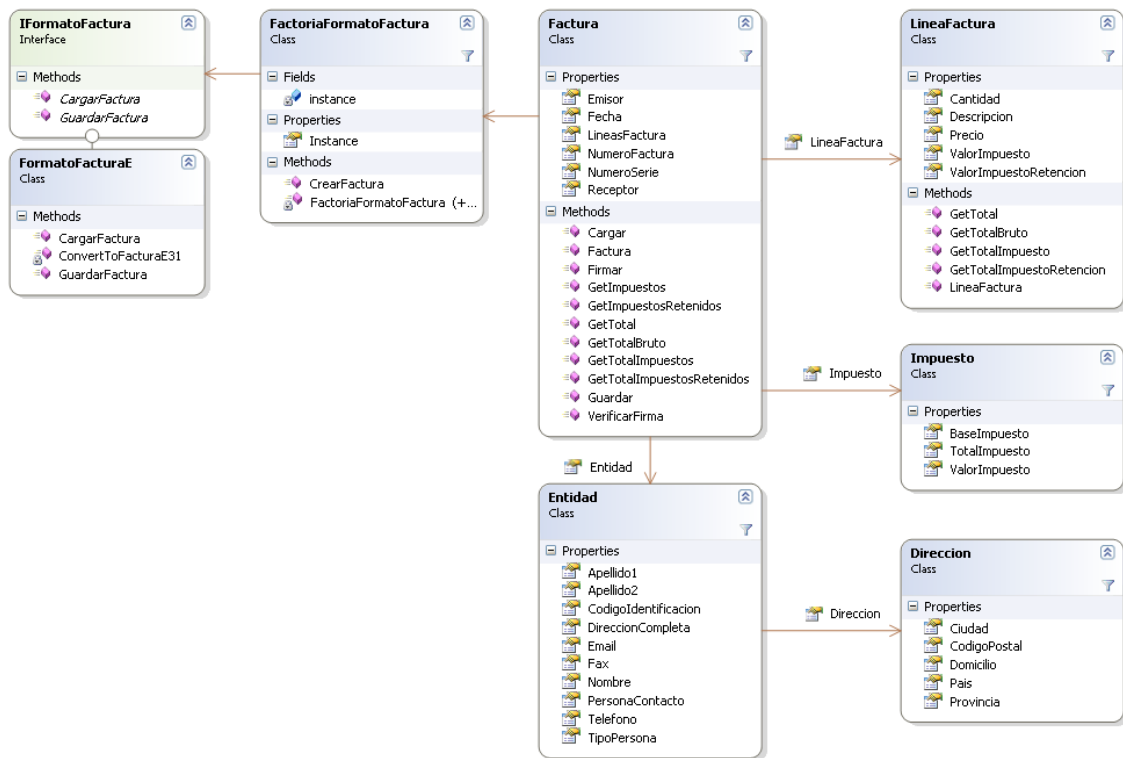


Figura 3.11: Esquema de clases de Facturación.

Impuesto

Esta clase almacena el valor y el tipo de un impuesto. La usaremos para guardar los impuestos repercutidos y los impuestos retenidos de las líneas de la factura

Direccion

Esta clase almacena los datos de una dirección: domicilio, código postal, ciudad, provincia y país. La usaremos para guardar la dirección del emisor y del receptor de la factura.

Entidad

Esta clase almacena los datos de una entidad: El tipo de persona (Física o Jurídica), el código identificativo (Nif, CIF, etc.), el nombre, los apellidos, la persona de contacto, el email, el teléfono y el fax. La usaremos para guardar los datos del emisor y del receptor de la factura.

LineaFactura

Esta clase almacena los datos de una línea de factura: descripción del artículo, cantidad, precio unitario del artículo, valor del impuesto repercutido y el valor del impuesto retenido.

Factura

Esta clase almacena los datos de una factura: El número de la factura, el número de serie, la fecha de emisión, los datos del emisor y del receptor, y las líneas que la componen.

Además es la encargada de crear las instancias de `FactoriaFormatoFactura` y `FactoriaFirmaDigital`, que son las responsables de crear los objetos adecuados para un determinado formato de factura y un determinado tipo de firma digital respectivamente.

FactoriaFormatoFactura

Esta clase, a través de su única instancia ya que implementa el patrón `Singleton`, nos devuelve un objeto de tipo `IFormatoFactura`, dependiendo del parámetro `FormatoFactura` del fichero de configuración de la aplicación. En nuestro caso, que hemos desarrollado el formato `FacturaE`, toma el valor **`FacturaE`**.

IFormatoFactura

En esta interfaz definimos el comportamiento que han de tener las clases que implementen un formato de factura digital. Definimos dos métodos:


```
void GuardarFactura(Factura fra, string fileName)
```

Guarda los datos del objeto **Factura** en un fichero cuyo path es `fileName` con el formato de factura que indicamos en el fichero de configuración.

```
Factura CargarFactura(string fileName))
```

Lee una factura, con un formato concreto almacenada en el fichero con path `fileName` y carga los datos del fichero en un objeto de tipo **Factura**.

FormatoFacturaE

Esta clase implementa la interfaz `IFormatoFactura`, y nos permite cargar los datos de una factura `FacturaE` en un objeto de tipo **Factura** y guardar los datos del objeto **Factura** con el formato `FacturaE` en un fichero.

3.5. Componente FacturaElectronica

3.5.1. Especificación

Este componente es nuestra interfaz de usuario, realiza la función de `FrontEnd` del resto de los componentes. Es el encargado de atender a las acciones del usuario, y se comunica directamente con nuestro componente **Facturacion**, que es el encargado de responder a las peticiones del usuario.

3.5.2. Diseño e Implementación

La interfaz de usuario consta de los siguientes formularios windows:

- **frmMain:** Es el formulario principal de nuestra aplicación. Es un formulario de tipo MDI (Multiple Document Interface), que es el contenedor de los formularios hijos

de las facturas. Esta formado por un menuStrip y un toolStrip, que contienen las siguientes opciones de menú:

■ **Archivo:**

- **Nuevo:** Nos crea un nuevo formulario de factura, dónde insertar los datos de la factura.
- **Abrir:** Nos permite seleccionar una factura guardada en un fichero, y nos carga los datos en un formulario de factura.
- **Guardar:** Nos guarda los datos del formulario factura en un fichero con el nombre que le indiquemos.
- **Vista Preliminar:** Nos muestra el esquema XML de nuestra factura.
- **Salir:** Cierra la aplicación

■ **Herramientas:**

- **Firmar:** Desde esta opción indicamos el fichero que queremos firmar digitalmente, y nos informa del resultado.
- **Verificar:** Desde esta opción indicamos el fichero del cual queremos verificar su firma digital, y nos muestra un formulario con el resultado.
- **Web Mityc:** El ministerio de Industria Turismo y Comercio, pone a nuestra disposición una aplicación web para validar nuestras facturas, a través de esta opción se abre un navegador con esta aplicación, para poder validar nuestras facturas.

En la figura 3.12 podemos ver el formulario principal de nuestra aplicación con un nuevo formulario de factura.

The screenshot shows a Windows application window titled 'Factura electrónica - [Factura 0]'. The window has a menu bar with 'Archivo', 'Ver', 'Herramientas', 'Windows', and 'Ayuda'. Below the menu bar is a toolbar with icons for file operations. The main area is divided into several sections:

- Datos de la Factura:** Includes fields for 'Número de factura:', 'Número de serie:', and 'Fecha de emisión:' (set to 04/01/2010).
- Importes:** Includes fields for 'Importe bruto:', 'Importe total:', 'Total Iva:', and 'Total IRPF:', all showing 0,00.
- Emisor de la factura / Receptor de la factura:** A tabbed section with two tabs. The 'Emisor de la factura' tab is active, showing fields for 'Tipo de persona:' (set to 'Jurídica'), 'Nombre:', 'Apellido1:', 'Apellido2:', 'C.I.F.', 'Dirección:', 'Localidad:', 'Dirección:', 'Provincia:', and 'Código Postal:'.
- Contacto:** Includes fields for 'Contacto:', 'Email:', 'Teléfono:', and 'Fax:'.
- Lineas de factura:** A table with columns: 'Descripción', 'Cantidad', 'Precio', 'I. Repercutido', 'I. Retenido', 'Importe Bruto', and 'Importe Total'. There are 'Añadir' and 'Eliminar' buttons to the left of the table.

Figura 3.12: Formulario principal de una factura.

- **frmFactura:** Este formulario es dónde insertamos o mostramos los datos generales de una factura como su número de serie, número de factura, fecha de factura, importes, las líneas que componen la factura y los datos del emisor y del receptor.
- **frmLineaFactura:** En este formulario insertamos las líneas de factura, con la descripción del artículo, la cantidad, el importe y el valor de los impuestos.
- **frmVerificar:** Es el formulario que nos muestra el resultado de la validación de una firma digital.

Capítulo 4

Pruebas

Para probar nuestra aplicación y comprobar que generamos facturas electrónicas válidas según el estándar FacturaE v3.1, vamos a utilizar la aplicación web que el Ministerio de Industria Turismo y Comercio (MITyc) pone a nuestra disposición en la url <http://www11.mityc.es/FacturaE/index.jsp>. En la figura 4.1 podemos observar el resultado de la verificación de una factura generada por nuestra aplicación.

Factura electrónica

Resultado de la validación

Tipo de validación	Resultado	Comentario
Formato	✓	(FacturaE 3.1)
Contable	✓	
Firma electrónica	✓	** XAdES_BES:1.3.2 Política válida: Política de Firma FacturaE v3.1
Prestador admitido	✓	FNMT Clase 2 CA (FNMT)
Estado certificado	⚠	Servicio no disponible

[Validar otra factura](#)

* Una factura electrónica con formato válido es aquella que se ajusta al esquema de factura electrónica v 3.0, v 3.1 ó v 3.2.

** Una firma digital de una factura electrónica válida es aquella que se ajusta a la política de factura electrónica v 3.0 ó v 3.1. Sin la presencia de la política la firma digital puede seguir siendo válida en el contexto de firma digital XAdES pero no lo será en el contexto de factura electrónica.

*** Relación de prestadores admitidos por el Ministerio de Industria, Turismo y Comercio.

Figura 4.1: Comprobación de la factura.

En la aplicación, se comprueba lo siguiente:

- Formato: Comprueba que la factura se ajusta al esquema de factura electrónica FacturaE.
- Contable: Comprueba que la factura tiene el formato contable permitido.
- Firma electrónica: Comprueba que la firma digital es válida, siendo válida aquella que se ajuste a la política de factura electrónica v 3.0 ó v 3.1. Sin la presencia de la política la firma digital puede seguir siendo válida en el contexto de firma digital XAdES pero no lo será en el contexto de factura electrónica.
- Prestador admitido: Comprueba si el certificado utilizado en la firma es de un prestador admitido por el MITyC. Entre los cuales son admitidos: AC ABOGACÍA, ANCERT Agencia Notarial de Certificación, ANF AC, Autoritat de Certificació de la Comunitat Valenciana ACCV, BANESTO CA, CAMERFIRMA, CATCert, CERES Fábrica Nacional de Moneda y Timbre Real Casa de la Moneda (FNMT RCM), CICCOP, Dirección General de la Policía y de la Guardia Civil Cuerpo Nacional de Policía, EDICOM, Firmaprofesional, S.A., HEALTHSIGN, S.L., Izenpe, S.A, Ministerio de Defensa de España, REGISTRADORES DE ESPAÑA y Santander
- Estado Certificado: Comprueba el estado del certificado utilizado en la firma, utilizando el protocolo OCSP, que es un método para determinar el estado de revocación de un certificado digital X.509. ¹

Para firmar digitalmente las facturas, tenemos que utilizar un certificado de un prestador admitido por este motivo hemos obtenido un certificado digital de la Fábrica Nacional de Moneda y Timbre, que se puede solicitar a través de la url <http://www.cert.fnmt.es/> y posteriormente personarse en cualquiera de las Oficinas de

¹Este protocolo se describe en el RFC 2560

Registro de los Organismos acreditados para verificar nuestra identidad y obtener el certificado.

Con este tipo de certificado no es posible verificar su estado via OSCP, que es lo que indica el resultado de validación de la factura de la figura 4.1. Este tipo de verificación es posible por ejemplo con el DNI-e.

Capítulo 5

Conclusiones

En los capítulos anteriores hemos descrito el problema que abordamos en este proyecto, los objetivos iniciales, y la solución propuesta. Terminamos esta memoria resumiendo los principales logros alcanzados en este proyecto, y las posibles líneas futuras de desarrollo.

5.1. Logros alcanzados

A partir del desarrollo de este proyecto se ha conseguido desarrollar una aplicación gráfica que nos permite generar facturas electrónicas con el formato FacturaE, firmar digitalmente las facturas y verificar facturas firmadas, que puede ser perfectamente utilizado por una empresa o particular para facturar en el mundo real, como hemos comprobado en las pruebas, ya que cumple con la normativa y leyes sobre facturación que existen en la actualidad. Además no nos hemos limitado a cerrar la aplicación a un determinado formato, puesto que hemos diseñado varios componentes para que puedan ser reutilizados y pueda ampliarse a otros formatos tanto de facturas como de firmas digitales. Podemos comprobar por tanto que todos los objetivos propuestos en el capítulo dos de este documento se han completado con éxito.

5.2. Conocimientos adquiridos

Durante la realización de este proyecto hemos adquirido nuevos conocimientos que enumeramos a continuación:

- **Facturación electrónica:** Tras realizar el estado del arte, sabemos en qué consiste una factura electrónica, que ventajas aporta respecto al modelo tradicional, qué tecnologías utiliza y qué formatos se están utilizando en la actualidad.
- **Criptografía:** Hemos aprendido sobre criptografía simétrica y asimétrica, cómo funciona la firma digital, y qué es y cómo se utiliza un certificado digital.
- **XMLDsig y Xades:** Hemos implementado una solución de firma digital en ficheros XML basados en estos dos estándares.
- **XSD y XML:** Para implementar un formato concreto de factura electrónica hemos tenido que estudiar el esquema XSD del formato FacturaE y comprender como se genera una factura en XML a partir de su definición XSD.
- **Patrones de diseño:** Hemos resuelto un problema común que se repite en varios desarrollos, como elegir de forma dinámica qué algoritmo implementar de entre varios, como instanciar distintos objetos que hereden de una clase en común, etc. de una forma elegante utilizando varios *Patrones de diseño*.
- **Diseño de una arquitectura en capas:** Es común hoy en día que las aplicaciones gráficas de usuario, se separen en varias capas lógicas, permitiendo separar la interfaz de usuario de la lógica de la aplicación y del resto de componentes, para que puedan ser reutilizadas en otras aplicaciones.
- **Java y JSDK 1.6:** Hemos desarrollado un par de componentes para poder firmar y verificar firmas digitales según el estándar Xades, utilizando para ello el lenguaje

JAVA y el JSDK, puesto que .Net no nos ofrece en la actualidad ninguna utilidad para utilizar este estándar. Como IDE de desarrollo hemos utilizado NetBeans 6.7

- **C# y .Net Framework 3.5:** Hemos implementado nuestra aplicación gráfica de usuario y la lógica de nuestra aplicación utilizando este lenguaje y su framework de desarrollo. Como IDE de desarrollo hemos utilizado Microsoft Visual C# Express 2008.
- **LATEX:** Para la confección de esta memoria.

5.3. Trabajos futuros

Aunque todos los objetivos que se han propuesto en el capítulo dos de este documento han sido cumplidos con éxito, es posible añadir nuevas funcionalidades y nuevas características a la aplicación, como pueden ser la implementación de otros formatos de facturación electrónica como son los estándares UBL o EDIFACT, o la inclusión de una firma digital utilizando el DNI-e.

Bibliografía

- [1] Davara Rodríguez, M.A., *La trasposición de la directiva sobre privacidad y las comunicaciones electrónicas*, 2004
- [2] Davara Rodríguez, M.A., *La seguridad en las transacciones electrónicas: La firma electrónica*, 2005
- [3] Ministerio de Economía y Hacienda, Formato FacturaE <http://www.facturae.es>
- [4] Ministerio de Industria, Turismo y Comercio, FacturaE <http://www11.mityc.es/FacturaE>
- [5] Grupo de trabajo de factura electrónica y digitalización certificada ASIMELEC <http://www.efactura.org.es>
- [6] Blog de recursos sobre factura electrónica y digitalización certificada <http://www.facturacionelectronica.info>
- [7] Manual del programador de .NET Framework, Cifrado XML y firmas digitales <http://msdn.microsoft.com/es-es/library/ms229749%28v=VS.90%29.aspx>
- [8] XAdES <http://www.w3.org/TR/XAdES>
- [9] Oasis UBL <http://www.oasis-open.org>
- [10] Edicom EDIFACT <http://www.edicomgroup.com/es/index.htm>