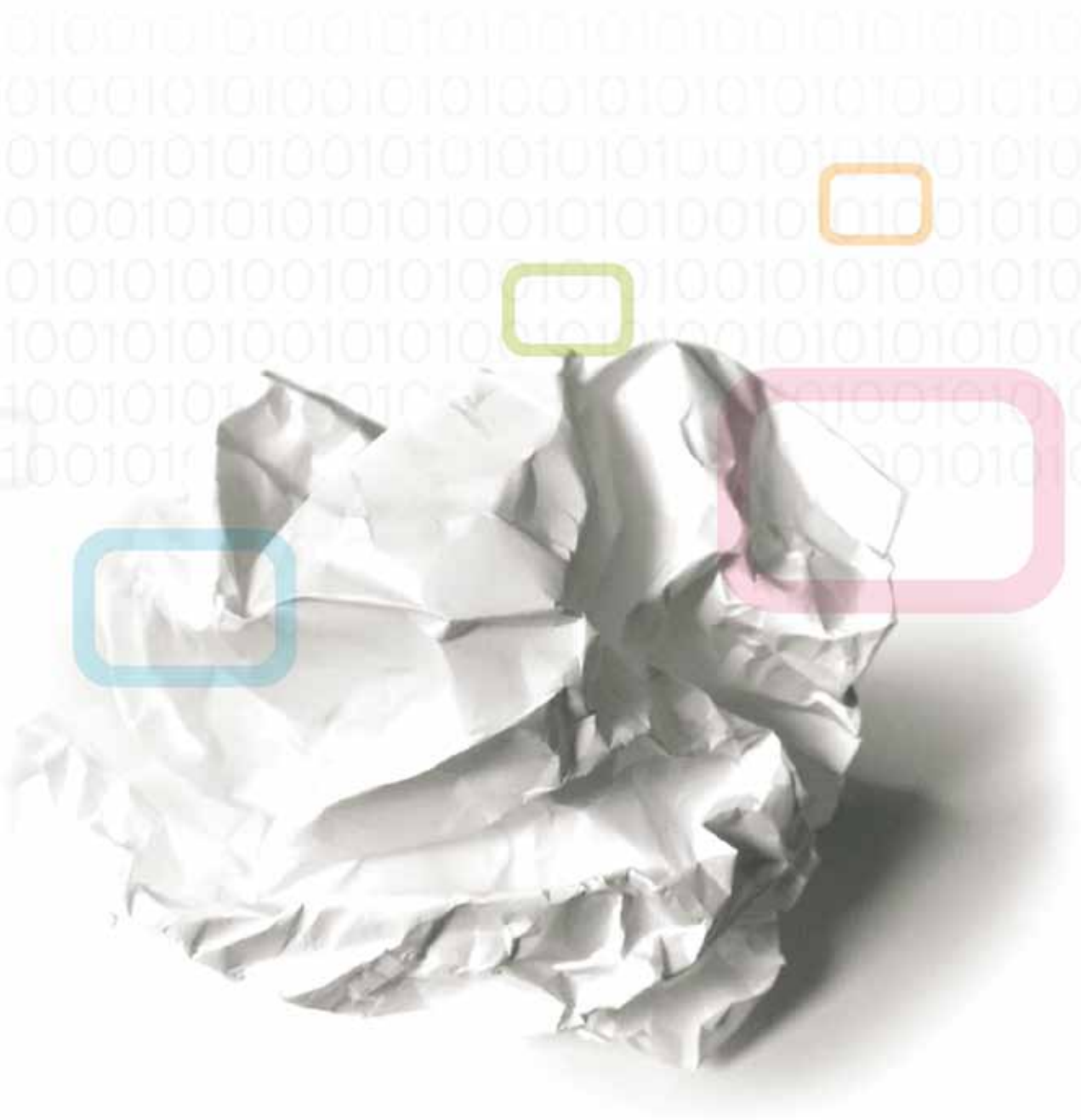




plan **avanza** 2.0



La factura electrónica



www.planavanza.es

www.mityc.es

www.red.es

www.asimelec.es

EDITAN:

©Red.es
Edificio Bronce
Plaza Manuel Gómez Moreno, s/n.
28020 Madrid

© ASIMELEC
Orense nº 62, 28020, Madrid.

Textos: Julián Inza

Coordinación: red.es

Imagen y Diseño: Virginia Zabala

Maquetación y Producción: Scan96, s.l. y Leaders
Comunicación

Imágenes: age FOTOSTOCK

Reservados todos los derechos. Se permite su copia y distribución por cualquier medio siempre que se mantenga el reconocimiento de sus autores, no se haga uso comercial de las obras y no se realice ninguna modificación de las mismas.

Índice

Introducción..... 4

CAPÍTULO 1. EL ABC DE LA FACTURA ELECTRÓNICA 5

- Qué es una factura..... 5
- Qué es la factura electrónica..... 6
- La factura electrónica dentro del proceso contable global 7
- Cómo funciona la factura electrónica 8
- Ventajas, beneficios y ahorros de la factura electrónica..... 9
- Algunos datos 11
- Cuánto cuesta un proyecto de factura electrónica..... 11

CAPÍTULO 2. TRABAJAR CON LA FACTURA ELECTRÓNICA DE MANERA FÁCIL..... 12

- Qué necesito para implantar la factura electrónica..... 12
- Requerimientos en la emisión de facturas electrónicas..... 16
- Requerimientos en la recepción de facturas electrónicas 17
- Cómo se pueden hacer facturas electrónicas mediante plataformas de terceros. 18
- Ejemplos de factura electrónica..... 20
 - Factura Facturae 20
 - Uso de aplicaciones en Internet (software as a service o computación en la nube) 23

CAPÍTULO 3. PROYECTOS AVANZADOS DE FACTURA ELECTRÓNICA .. 24

- Identificación de proyectos avanzados..... 24
- Proyectos orientados a la emisión de facturas..... 25
- Proyectos orientados a la recepción de facturas 26
- Preparación del proyecto 28
- Facturación electrónica a las Administraciones Públicas..... 28

CAPÍTULO 4. INTERACCIÓN CON LA FACTURA PAPEL 30

- Cómo se conservan electrónicamente facturas recibidas en papel 30
- Cómo se conservan en papel facturas recibidas electrónicamente..... 31

CAPÍTULO 5. FORMATOS DE FACTURA Y FIRMA ELECTRÓNICA 33

- Formato de la factura electrónica 33
- Formato de firma..... 35
 - Formatos de firma especiales: firma fechada y validada 35
 - Firmas XML 35

ANEXO I. INTRODUCCIÓN A LA FIRMA ELECTRÓNICA Y A LA CERTIFICACIÓN ELECTRÓNICA 37

- PSC y CA 37
- La firma manuscrita..... 37
- Criptografía 37
- Cifrado simétrico..... 37
- Cifrado asimétrico..... 38
- Prestador de servicios de certificación 40
- Entidad de registro 41
- El esquema completo 42
 - Realización de la firma 42
 - Comprobación de la firma..... 42
- Funciones de seguridad 43
- Custodia de claves y dispositivos seguros de creación de firmas..... 43

ANEXO II. MARCO JURÍDICO DE LA FIRMA Y DE LA FACTURA ELECTRÓNICA 45

- Validez legal de la factura electrónica.... 45
- Aspectos legales de la firma electrónica 47

ANEXO III. ENLACES DE INTERÉS..... 50



Introducción

Esta es la segunda revisión importante del Manual de factura electrónica que se desarrolló en el año 2006 a iniciativa de ASIMELEC y red.es iniciando la colección de Manuales del Plan Avanza de red.es. La primera revisión se publicó a principios de 2008, por lo que ya incorporó las principales novedades que se produjeron durante el año 2007, que fueron muchas.

En esta ocasión, cumplidos los objetivos iniciales de establecer las bases del conocimiento de la factura electrónica y situados en un marco internacional en el que comienza a cobrar importancia la interoperabilidad, la presente versión simplificará algunos de los aspectos tratados en ediciones anteriores destacando las buenas prácticas que ya se han consolidado.

Debido a la simplificación del documento, no se incluye en esta ocasión información sobre los sistemas EDI (Electronic Data Interchange - Intercambio Electrónico de Documentos), pero los interesados pueden acudir a las versiones anteriores, disponibles on-line. A día de hoy, el EDI sigue siendo el sistema preferido en entornos como la distribución comercial y la automoción.

El manual está dirigido fundamentalmente al mercado español, y refleja el escenario de gestión de facturas electrónicas más extendido en España. El uso de la firma electrónica se ha generalizado entre los sistemas de facturación electrónica españoles, y, por tanto, muchas de las indicaciones contenidas en este documento reflejan 'buenas prácticas' que pueden ser de utilidad en el ámbito europeo, en aquellos casos en los que los interlocutores prefieran esta medida de seguridad. Por ello, esta tercera versión se traduce al inglés.

Las ediciones anteriores estuvieron disponibles en forma impresa y en formato PDF. De las versiones impresas se distribuyeron más de 10.000 ejemplares, y la versión en PDF superó las 500.000 descargas. Y por los desarrollos tecnológicos acometidos por las empresas y sus proveedores, cabe decir que supusieron una notable influencia en la adopción de la factura electrónica en España, que en la actualidad es uno de los países europeos con mayor penetración de esta tecnología y con un gran número de soluciones de todo tipo, desde las gratuitas para PYMEs, hasta las sofisticadas de grandes empresas y organismos públicos.

Esta edición viene marcada adicionalmente por dos hechos significativos: por un lado la publicación del Informe Final del Grupo de Expertos en factura electrónica de la Comisión Europea, que ha identificado algunas barreras cuya supresión puede impulsar la adopción de la factura electrónica en toda Europa, y por otro, la adopción el pasado 16 de marzo de 2010, bajo la presidencia española de la UE, del texto consensuado de reforma de la Directiva 112/2006, que recoge las principales sugerencias del Grupo de Expertos y que se espera quede traspuesto a las legislaciones nacionales antes del 1 de enero de 2013.

Con la obligatoriedad de facturar electrónicamente al sector público estatal recogida en la Ley 30/2007, y en la Ley 56/2007, no cabe duda de que la adopción será aún mayor en los próximos años.

01.

Capítulo 1. El ABC de la factura electrónica

Qué es una factura

La factura es un documento que refleja la entrega de un producto o la provisión de un servicio, junto a la fecha de devengo, además de indicar la cantidad a pagar como contraprestación.

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.

Se la considera como 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). El original debe ser custodiado por el receptor de la factura. Habitualmente, el emisor de la factura conserva una copia o la matriz (base de datos) en la que se registra su emisión, en cuyo caso no tiene por qué custodiar las copias de las facturas.

La factura correctamente cumplimentada es el único justificante fiscal, que da al receptor el derecho de deducción del impuesto (IVA). Esto no se aplica en los documentos sustitutos de factura, recibos o tickets.

En Europa, la normativa de facturación se regula por la Directiva 2006/112/CE, para la que ya se han consensuado las modificaciones que incluirá la próxima versión. Las modificaciones introducidas buscan armonizar los requerimientos legales en toda la UE para conseguir mayor interoperabilidad, lo cual facilitará el despegue y penetración de la facturación electrónica.

Las facturas pueden ser:

- **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.

Es interesante mencionar que las tradicionales Notas de Abono no se contemplan en la normativa, aunque su función se cubre con las facturas rectificativas. Cabe identificar ambos documentos siempre que se incluya la mención obligatoria ractura rectificativa y opcionalmente, a título informativo, la de nota de abono y se consignen los signos de las cantidades de forma correcta.

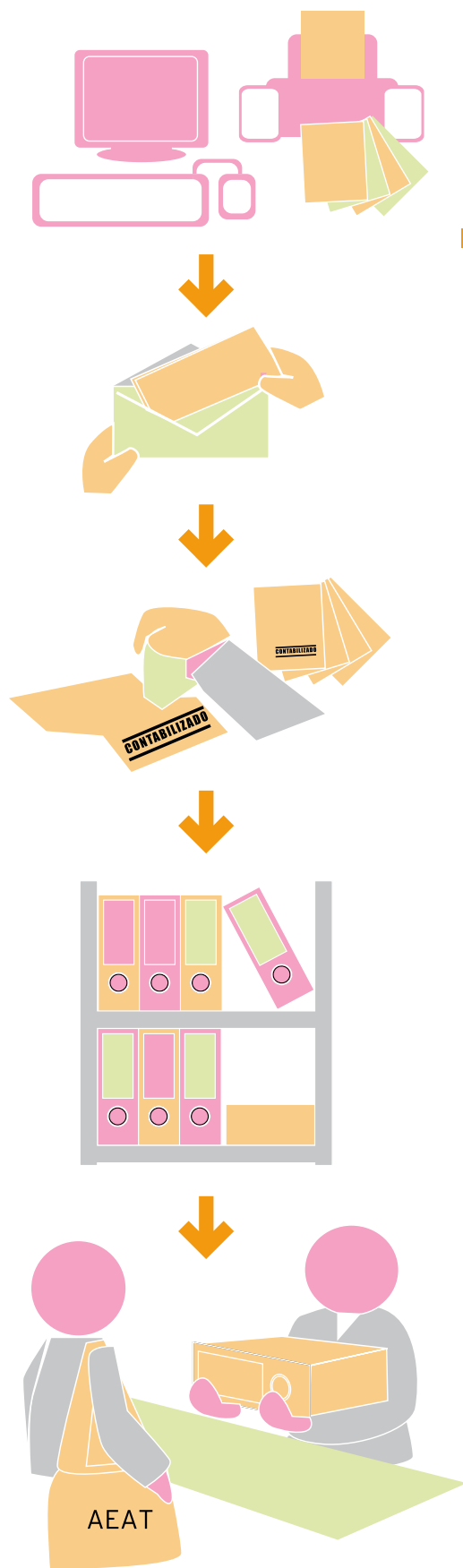


Fig. 1. Proceso genérico de facturación tradicional en papel.

La factura se imprime a partir de ficheros informáticos, se dobla, se ensobra y se franquea. Se envía por correo postal o mensajería y se recibe por el destinatario, que realiza los procesos de conciliación, contabilización y pago. Se archiva y queda a disposición de auditorías o inspecciones fiscales que se basan en el valor documental del soporte en papel.

“La factura correctamente cumplimentada es el único justificante fiscal que da al receptor el derecho de deducción del impuesto (IVA)”

Qué es la factura electrónica

La facturación electrónica consiste en la transmisión de las facturas o documentos análogos entre emisor y receptor por medios electrónicos (ficheros informáticos) y telemáticos (de un ordenador a otro), firmados digitalmente con certificados reconocidos (o cualificados), con la misma validez legal que las facturas emitidas en papel.

Si buscamos una definición específica, podemos recurrir al artículo 1 de la Ley 56/2007: “La factura electrónica es un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la autenticidad de su origen y la integridad de su contenido”.

Aunque existen varios mecanismos para garantizar la autenticidad del origen, la integridad del contenido y la legibilidad de una factura, ya sea en papel o en formato electrónico, desde el momento de su expedición hasta el final del período de conservación de la factura, en el caso de la factura electrónica, el uso de la firma electrónica es el más generalizado en España.

En este sentido, en el texto consensuado de la futura modificación de la Directiva 112/2006, se recoge, en lo que se refiere a su artículo 233:

1. Se garantizará la autenticidad del origen, la integridad del contenido y la legibilidad de una factura, ya sea en papel o en formato electrónico, desde el momento de su expedición hasta el final del período de conservación de la factura. Cada

sujeto pasivo determinará el modo de garantizar la autenticidad del origen, la integridad del contenido y la legibilidad de las facturas. Podrá realizarse mediante controles de gestión que creen un vínculo fiable de auditoría entre la factura y la entrega de bienes o la prestación de servicios.

Se entenderá por "autenticidad del origen", la garantía de la identidad del proveedor de bienes o prestador de servicios o del emisor de la factura.

Por "integridad del contenido" se entenderá que el contenido requerido con arreglo a lo dispuesto en la presente Directiva no ha sido modificado.

2. Además de los tipos de control de la gestión contemplados por el segundo párrafo del apartado 1, otros ejemplos de tecnologías que garantizan la autenticidad del origen y la integridad del contenido de una factura electrónica son:

- *La firma electrónica avanzada en el sentido del punto 2 del artículo 2 de la 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, basada en un certificado reconocido y creada mediante un dispositivo seguro de creación de firma, en el sentido de los puntos 6 y 10 de la Directiva 1999/93/CE.*
- *El intercambio electrónico de datos (IED), tal como se define en el artículo 2 de la Recomendación 1994/820/CE de la Comisión, de 19 de octubre de 1994, relativa a los aspectos jurídicos del intercambio electrónico de datos, si el acuerdo relativo al intercambio contempla el uso de procedimientos que garanticen la autenticidad del origen y la integridad de los datos.*

Esto significa que tras el período de transposición de la Directiva (1 de enero de 2013), la legislación española reflejará la posibilidad de que puedan enviarse facturas electrónicas entre empresas sin ningún requisito formal, si bien probablemente se mantengan los mismos requisitos que existen en la actualidad cuando el destinatario sea una administración pública.

En España, la adopción de la firma electrónica como mecanismo generalizado para garantizar la autenticidad e integridad de las facturas electrónicas se ha visto favorecido por la extensión del DNI electrónico (con más de 15 millones de unida-

des expedidas) y la amplia disponibilidad de certificados electrónicos de múltiples prestadores de servicios de certificación, así como por la disponibilidad de software gratuito que permite la generación y firma electrónica de las facturas electrónicas que se envían, así como su verificación en el caso de la recepción de facturas.

El proceso de facturación es un proceso importante para cualquier empresa, y culmina el proceso de compra y venta. Aunque tradicionalmente la relación entre empresas se ha basado en el intercambio de documentos en papel, esto implica el empleo de grandes cantidades de recursos y la realización de muchas tareas de forma manual. En un contexto de universalización de internet, cada vez más las empresas se plantean la optimización de sus procesos para ganar eficiencia y ahorrar costes.

Y por ello se ha avanzado en la adopción de la facturación electrónica, que en España está regulada en el Reglamento de facturación publicado en Real Decreto 1496/2003 y modificado por el Real Decreto 87/2005.

Esta regulación de la factura electrónica se completa con la publicación de la 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.

Las denominaciones factura electrónica, factura telemática y factura digital son equivalentes, si bien la denominación generalmente utilizada en la normativa es remisión electrónica o remisión por medios electrónicos de factura. Frecuentemente se distingue con la denominación factura digital a la modalidad de factura electrónica que utiliza la firma digital para garantizar la autenticidad e integridad de la factura.

Las facturas electrónicas se pueden emitir en diferentes formatos (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg o txt, entre otros) siempre que se respete el contenido legal exigible a cualquier factura y que se cumplan los requisitos de autenticidad e integridad, por ejemplo con la incorporación de la firma electrónica reconocida (qualified electronic signature, en inglés).

Sin embargo, tras la publicación de la Orden

PRE/2971/2007, en la que se definió el uso obligatorio del formato XML **facturae**, cuando el destinatario sea una administración de la AGE (Administración General del Estado) y sus organismos públicos, este formato se adopta frecuentemente en España también para la facturación entre empresas privadas.

Por otro lado las administraciones autonómicas con políticas activas de impulso de la factura electrónica están adoptando también este formato de factura electrónica **facturae**. Entre las Comunidades Autónomas que han adoptado el formato **facturae** cabe citar las siguientes:

- Cataluña (e-Fact)
- País Vasco
- Comunidad Valenciana (Ge-Factura)
- La Rioja
- Castilla-La Mancha

A lo largo de este documento se pone énfasis en la facturación electrónica en la que se utiliza la firma electrónica según el formato **facturae** dado que se ha consolidado como el conjunto de mejores prácticas en la adopción de la facturación electrónica en España.

“La factura electrónica es un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la autenticidad de su origen y la integridad de su contenido”.

La factura electrónica dentro del proceso contable global

La factura no debe entenderse como un proceso aislado, sino como un elemento integrado dentro del conjunto de gestión financiera y del flujo de compras y ventas de una entidad.

Es sólo una de las fases del proceso de gestión de compras y ventas de la empresa, en el que con frecuencia nos encontramos la factura como uno de los últimos resultados tras el tránsito habitual de presupuesto, solicitudes de compra, aprobaciones, albaranes, apuntes contables o procesos de gestión de almacén.

Una buena gestión electrónica en todos los pasos

y documentos previos facilitará en gran medida la implantación de la factura electrónica y multiplicará exponencialmente los beneficios de la misma.

Por otro lado, acometer el proyecto de incorporar la factura electrónica a la gestión de una empresa, habitualmente implicará revisar el proceso de emisión y recepción de facturas y afectará a más áreas de gestión de las que puede parecer obvio.



Fig. 2. Workflow documental asociado a compras.

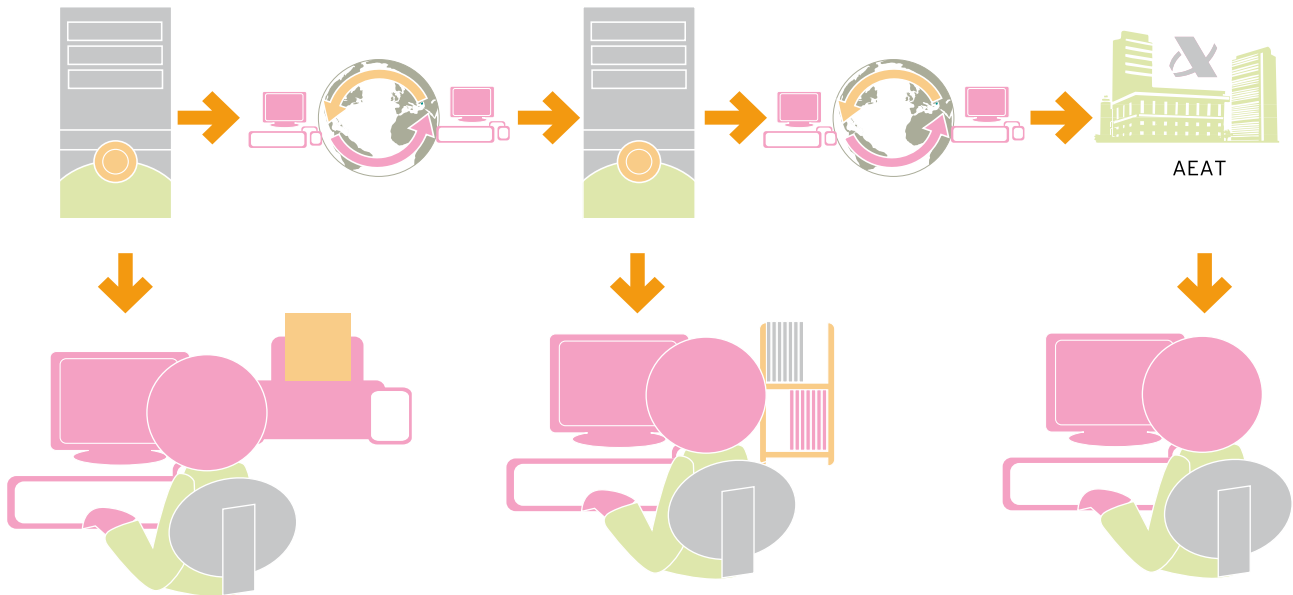


Fig. 3. Proceso simplificado de facturación electrónica.

La factura que se gestiona en un ordenador, se transmite a otro telemáticamente. Este la conserva de forma electrónica y desde él, de ser preciso, se pone a disposición de la Administración Tributaria por vía telemática. Los usuarios llevan a cabo toda la operativa en sus ordenadores.

Cómo funciona la factura electrónica

A grandes rasgos, el proceso de facturación electrónica lo formarían dos pasos básicos y diferenciados en todo sistema de facturación: emisión y recepción de facturas.

1. En la emisión, el emisor, con la conformidad del receptor, transmite a éste por medios telemáticos la factura electrónica (que frecuentemente incluye una firma electrónica) y conserva copia o matriz (la base de datos). Si se conserva la base de datos, no es necesario conservar las copias de los documentos electrónicos firmados.
2. El receptor recibe la factura en formato digital y la conserva en soporte informático para su futura consulta e impresión, si fuera necesario. Al ser la factura un documento firmado electrónicamente, debe guardar la información relativa a la comprobación de la validez de la firma electrónica, o que permita comprobar esta validez transcurrido un tiempo.

De esta forma 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.

Ventajas, beneficios y ahorros de la factura electrónica

La factura electrónica genera grandes beneficios a las empresas que la utilizan, tanto del lado del emisor como del receptor. Existen muchas razones para adoptar la factura electrónica, que van desde los puramente económicos hasta los ecológicos.

Entre las ventajas de la gestión electrónica cabe mencionar:

- **Ahorro de costes:** tanto del lado del emisor como del receptor. Derivado de la supresión del papel, el abaratamiento de los medios de comunicación electrónicos (en contraposición a los medios tradicionales de envío postal), eliminación de los gastos de franqueo, gastos derivados de la introducción manual de datos.
- **Mejora de la eficiencia:** la liberación de tareas administrativas permite destinar los recursos humanos a aspectos productivos en las compañías.
- **Integración con ERPs:** desde el punto de vista del emisor continúa el proceso que ya se está realizando electrónicamente. Un simple clic desde el ERP y la factura es emitida y enviada. Desde el lado del receptor los datos se pueden introducir automáticamente en sus aplicaciones.
- **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 y actual.
 - **Reducción de tiempos de gestión:** la inmediatez del envío y recepción de facturas por medios telemáticos convierte este trámite en un elemento que deja de tener sentido. Además, permite solucionar las discrepancias en muy poco tiempo.
 - **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 acciones erróneas:** a través de sistemas de alertas que detectan discrepancias entre operaciones de contabilidad y facturación o en la aplicación de tipos erróneos.
 - **Uso eficaz de recursos financieros:** la adopción de la factura electrónica favorece el acceso a medios de financiación como el **factoring** o el **confirming**.
 - **Mejor aprovechamiento de la habilidad de los empleados,** que pueden dedicar su tiempo a tareas de mayor valor añadido para la empresa.
 - **Reducción de controversias** en la gestión de facturas entre emisor y receptor.
 - **Mejoras en la resolución de incidencias,** que disminuyen y se resuelven de forma más rápida.
 - **Reducción de plazos de cobro,** ya que la conformidad de las facturas se consigue con más celeridad.
 - **Mejoras en la negociación de los plazos de pago,** ya que la certeza en la aplicación de los plazos que no se ven afectados por demoras por incidencias, permite un cierto margen de maniobra adicional.
 - **Mejora de la relación comercial y de la imagen de la empresa,** como consecuencia de los efectos anteriores.
 - **Cumplimiento de obligaciones** cuando la facturación electrónica sea exigida en los procesos de licitación.

Se consigue, en definitiva, una mayor calidad de servicio que repercute a su vez en una mayor competitividad de la empresa.

“Existen muchas razones para adoptar la factura electrónica, que van desde los puramente económicos hasta los ecológicos”

Algunos datos

Una de las principales ventajas de la factura electrónica es el ahorro económico que tiene para las empresas que la utilizan. Y es que eliminar gastos relacionados con el uso de papel, tinta o impresión constituye una de sus grandes ventajas. Los siguientes cuadros reflejan los ahorros de la factura electrónica. Estos datos son estimaciones de ASIMELEC.

Emisión

Papel	Coste/ unidad	Factura electrónica	Coste/ Unidad
Impresión	0,12	Imputación de costes del proyecto	0,05
Envío (sobre, sello, correo certificado)	2,60	Servicios externos (tráfico, timestamping)	0,15
Tratamiento manual	0,35	Gestión (Dpto. Administración)	0,02
TOTAL:	3,07	TOTAL:	0,22

Ahorro por factura: 2,85 euros.

Recepción

Papel	Coste/ unidad	Factura electrónica	Coste/ unidad
Recepción y manipulación	0,07	Imputación de costes del proyecto	0,05
Grabación	0,15	Comprobación de factura y firma-e	0,13
Tratamiento manual	1,68	Gestión (Dpto. Administración)	0,05
Archivado (4 años)	1,67	Archivado (4 años)	0,48
TOTAL	3,57	TOTAL	0,71

Ahorro por factura: 2,86 euros.

Hay ahorros adicionales como consecuencia de gestiones posteriores. Por ejemplo, facturas que no aparecen o son difíciles de encontrar por estar mal archivadas, en fases de auditoría o inspección. Este problema no se da con los documentos electrónicos.

Cuánto cuesta un proyecto de factura electrónica

Es difícil contabilizar el precio de la implantación de una solución de facturación electrónica en sentido amplio, si bien podemos presumir que, a mayor grado de complejidad de la plataforma y mayor automatización, crecerá inevitablemente el coste de puesta en marcha, a la vez que se lograrán mayores ahorros por factura emitida/recibida.

Según lo anterior, el coste de la factura electrónica puede considerarse virtualmente nulo si empleamos elementos ya existentes en la empresa, tales como herramientas ofimáticas que permitan la firma electrónica, certificados digitales empleados en otros procesos de la empresa, o el DNI electrónico, y el correo electrónico. También están disponibles sin coste sencillas aplicaciones de facturación electrónica orientadas a PYMEs y profesionales independientes.

Por su parte, la creación de un entorno específico de facturación electrónica con desarrollos específicos e integración requerirá un mayor plazo de retorno de la inversión, que será recuperada a medio/largo plazo.

Como orientación, algunos sistemas de implantación sencilla, como aplicaciones tipo web para emitir facturas pueden costar unos 30 euros al mes. En otras ocasiones, los prestadores de estas soluciones pueden definir modelos de precio basados en el número de facturas emitidas con valores entre 10 y 20 céntimos de euro por factura. Estos sistemas serían adecuados para las PYMEs, si bien las grandes empresas se rigen por otros parámetros.

No suele indicarse, pero uno de los costes del proyecto es precisamente el de adaptación a la nueva forma de hacer las cosas, y la necesidad de mantener el sistema anterior de papel y el nuevo electrónico, durante un tiempo.

“A mayor grado de complejidad de la plataforma y mayor automatización, crecerá inevitablemente el coste de puesta en marcha, a la vez que se lograrán mayores ahorros por factura emitida/recibida”.

02.

Capítulo 2. Trabajar con la factura electrónica de manera fácil

Qué necesito para implantar la factura electrónica

Los requerimientos dependen en gran medida del alcance del proyecto, si bien siempre existen ciertos elementos básicos según se analicen desde el punto de vista del emisor o desde el del receptor.

Al diseñar el proyecto influyen los volúmenes de facturación y su distribución por interlocutores, por lo que conviene comenzar por la implantación con aquellas empresas con las que se consiga más ahorro o sea más sencilla la adopción.

Simplificando, puede afirmarse que el requisito básico del emisor es **firmar electrónicamente** la factura (requisito que puede ser cumplido por un servicio externo) y el del receptor es **verificar la factura y conservarla en su formato original** (lo que también se puede realizar por un servicio externo).

En una de las variantes más sencillas, el emisor de la factura puede firmar un correo electrónico y enviarlo con los datos de la factura, para lo que sólo es necesario una clave con su certificado electrónico reconocido (qualified certificate en inglés) expedido por un prestador de servicios de certificación que cumpla lo establecido por la Directiva 1999/93/CE de Firma Electrónica (la Ley 59/2003, en el caso de los prestadores españoles).

Existen soluciones gratuitas, como la "Gestión de facturación electrónica. 1.0" disponible en la sección de descargas de la página web: <http://www.facturae.es>.



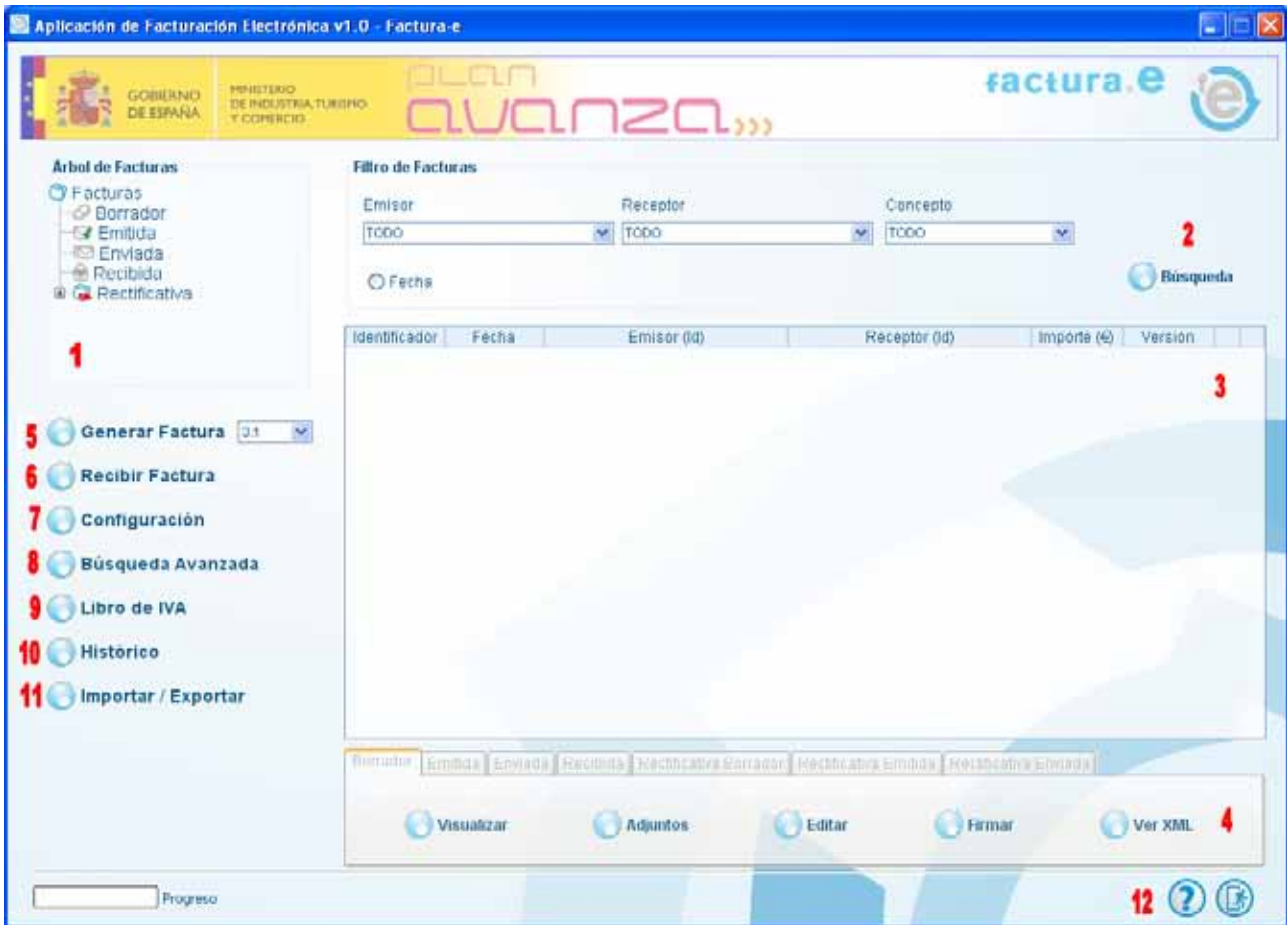


Fig. 4. Gestión de facturación electrónica.1.0.

Este programa basado en Java permite gestionar facturas en formato XML **facturae 3.0 y 3.1**, y realizar firmas electrónicas **XAdES-EPES** (según la norma TS 101 903).

También está disponible sin coste la extensión **OffInvoice** descargable desde Codeplex: <http://offinvoice.codeplex.com> que permite gestionar facturas electrónicas desde **Word 2010** o desde **Excel 2010** en entornos de **Windows 7**.

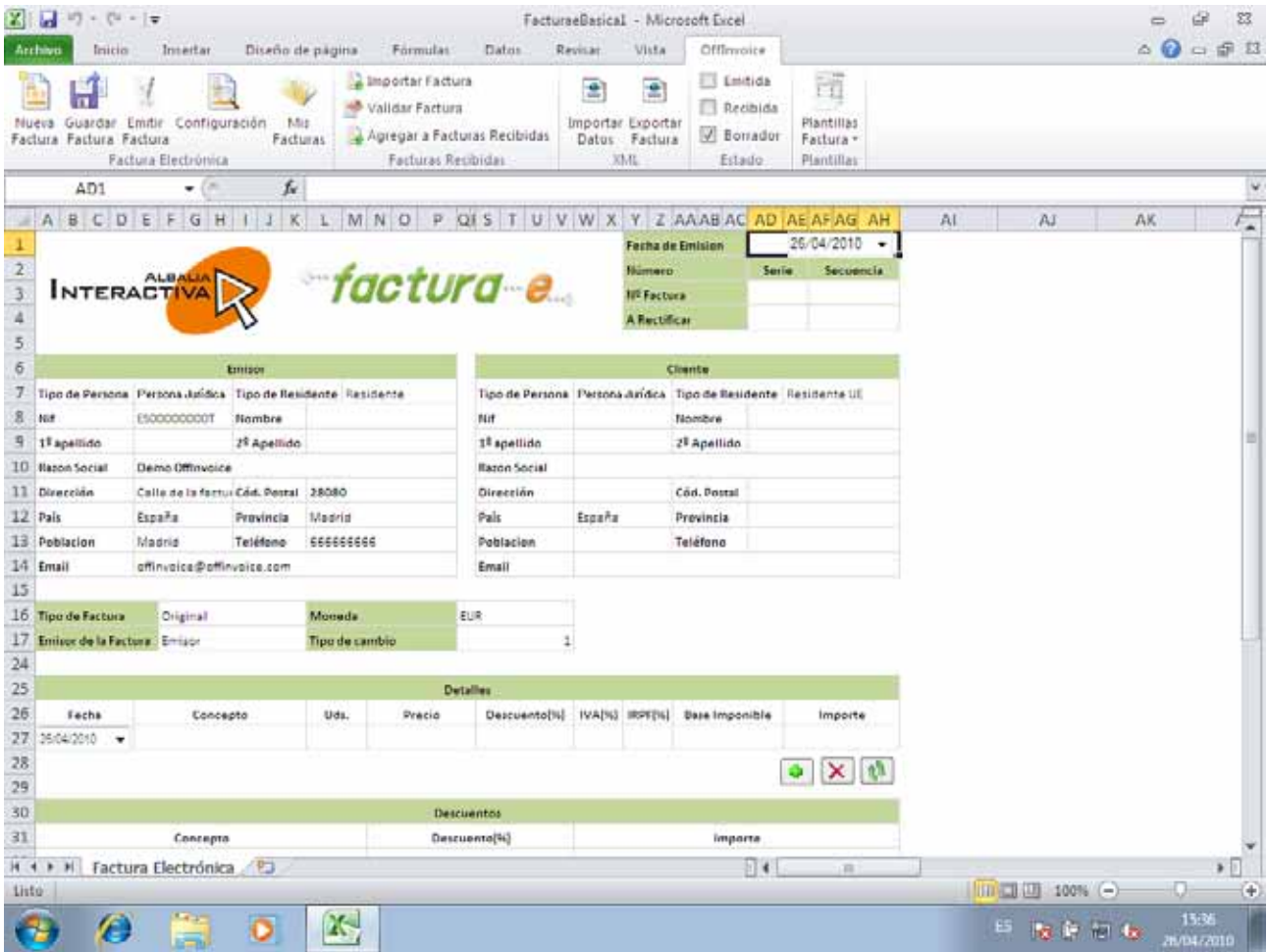


Fig. 5. Ejemplo de factura con Offinvoice en MS Excel 2010.

Este programa se maneja como un conjunto de menús adiciones de Word o Excel y permite gestionar facturas en formato XML **facturae 3.1** y **3.2**, en formato **UBL** (Universal Business Language) y en un prototipo (la especificación es incompleta) del formato **CII** (Cross Industry Invoice) Además permite realizar firmas electrónicas **XAdES-EPES** y **XAdES-XL** (según la norma TS 101 903).

Existe una versión anterior, denominada FactOffice, diseñada para Word 2007 disponible en <http://factoffice.codeplex.com>

Ambos programas permiten utilizar cualquier certificado electrónico, y, en particular el **DNI electrónico**.

Existen mecanismos intermedios, como las plataformas de facturación de terceros o la automatización de procesos clave (como la firma en "batch" o por lotes de facturas), donde se puede llegar a un grado de eficiencia bastante alto.

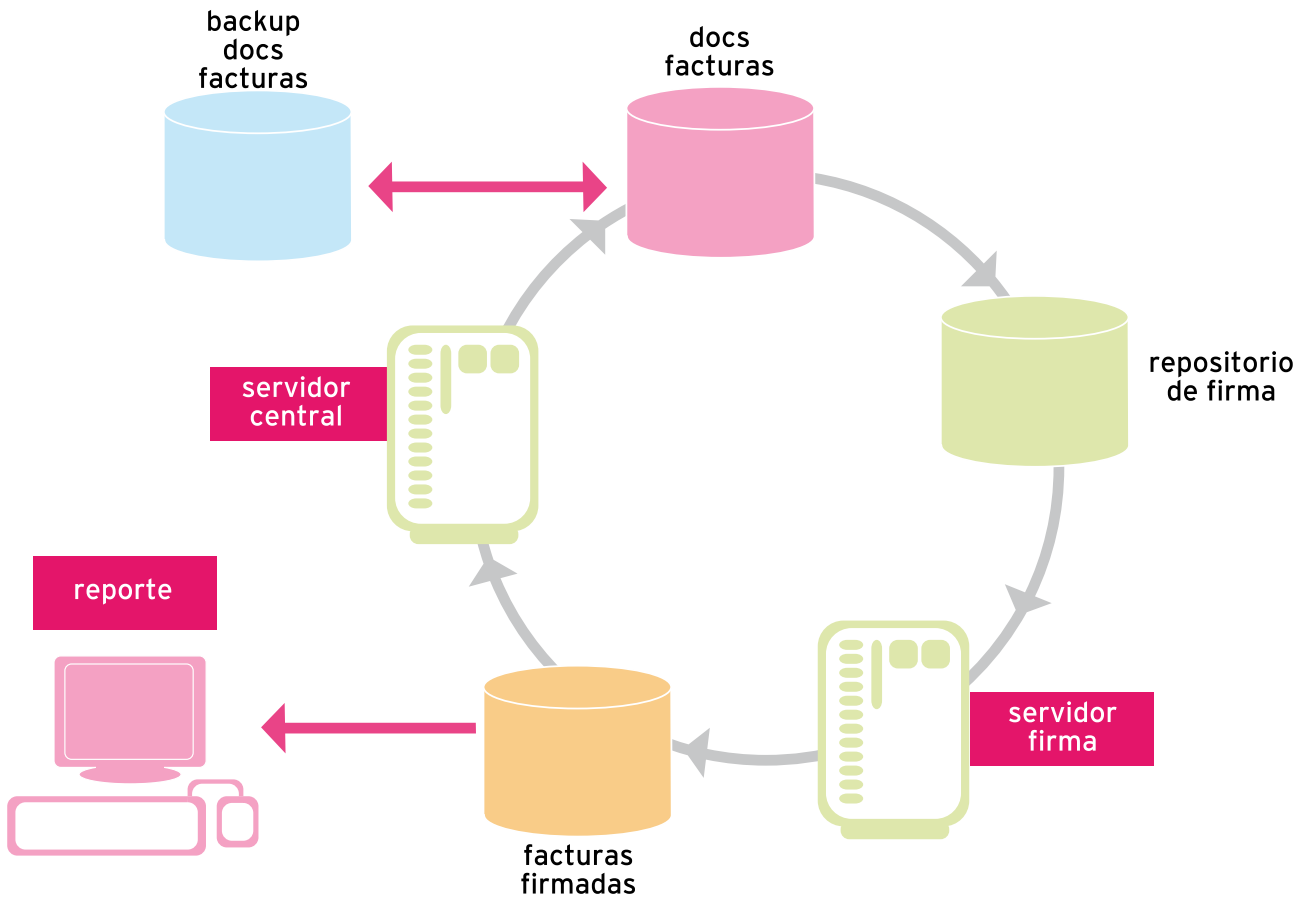


Fig. 6. Esquema de aplicación intermedia para la firma de facturas ya formadas.

Tras la generación de la factura en un formato adecuado, el servidor de firmas procesa automáticamente un lote de documentos sin ulterior intervención manual.

Cuando hablamos de desarrollos a medida o de integraciones complejas de productos estaremos ante lo que denominaremos proyectos avanzados de facturación electrónica.

Si decide empezar a emitir facturas firmadas

electrónicamente de manera sencilla para luego ir ampliando el alcance del proyecto, necesitará un programa de firma electrónica y un certificado expedido por un prestador de servicios de certificación.

“Es importante analizar si la empresa va a iniciar la implantación desde el punto de vista de emisor o desde el punto de vista de receptor de facturas”.

Requerimientos en la emisión de facturas electrónicas

A pesar de que la implantación de la factura electrónica implica necesariamente a ambas partes, muchos de los proyectos que se inician en España están siendo orientados a la posición de emisión de facturas.

Los proyectos de emisión de facturas suelen ser más sencillos de abordar, si bien tienen menos repercusión en el objetivo de la agilización de procesos de una entidad.

Para el emisor se exige

- Tener el consentimiento previo del receptor.
- Garantizar la autenticidad del origen y la integridad de las facturas, mediante el uso de la firma electrónica reconocida (qualified electronic signature en inglés).
- Almacenar copia de las facturas. Este requisito no es necesario si se puede reconstruir una factura a partir de la información guardada en la base de datos de la empresa (**matriz**).
- Las facturas almacenadas deben contener determinados elementos que faciliten su búsqueda, visualización e impresión en caso de inspección (acceso completo a los datos).

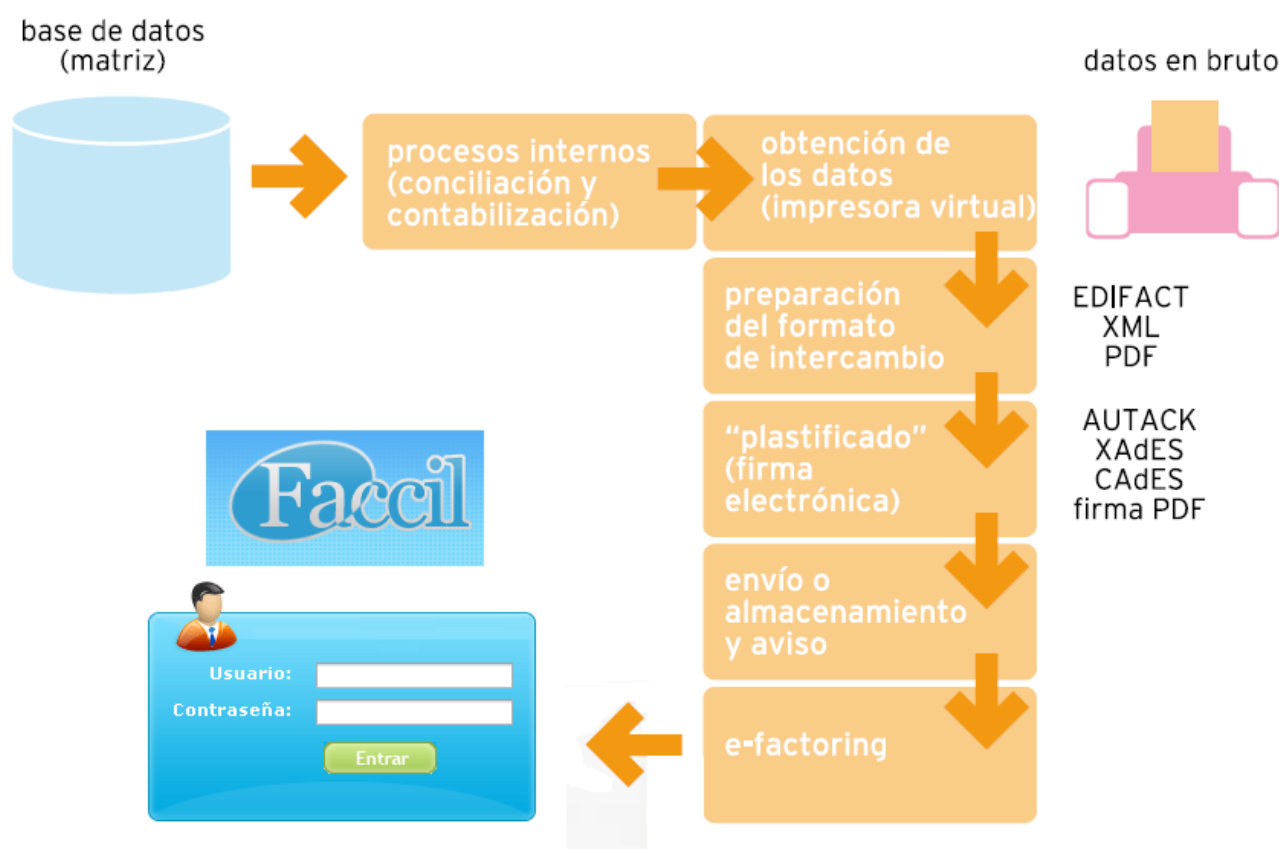


Fig. 7. Flujo base de emisión de facturas.

En la emisión, el proceso de gestión de facturas culmina en su impresión, o en la generación de los formatos de intercambio acordados para los destinatarios que las prefieren electrónicas. Según el formato de la factura, así será el formato de la firma electrónica. Tras el envío, la factura está en un formato que facilita la gestión de servicios de factoring con las entidades financieras.

“La gran mayoría de los proyectos que se inician en España están siendo orientados a la posición de emisión de facturas”.

Requerimientos en la recepción de factura electrónica

En los proyectos dirigidos a la optimización del proceso de recepción de facturas mediante la utilización de la factura electrónica, se busca habitualmente la integración con los ERPs o gestores de facturación internos.

La complejidad de este tipo de proyecto aumenta si se tiene que tratar un número indeterminado de formatos electrónicos junto con la recepción de facturas en papel.

Para disminuir la complejidad del proceso, se puede optar por la modalidad de auto-facturación, en la que el propio receptor controla el formato de recepción y garantiza la conciliación contable.

Otra posibilidad a considerar por las empresas receptoras es el uso de plataformas externas, que, bajo la modalidad de facturación por terceros, facilitarán todo el proceso de transformación de las facturas e incluso la digitalización certificada de los documentos recibidos en papel.

Para el receptor se exige

- Disponer del software necesario para la validación de la firma electrónica.
- Almacenar las facturas recibidas digitalmente (factura y firma) en su formato original.
- Las facturas almacenadas deben contener elementos que faciliten su búsqueda, visualización e impresión en caso de inspección (acceso completo a los datos).

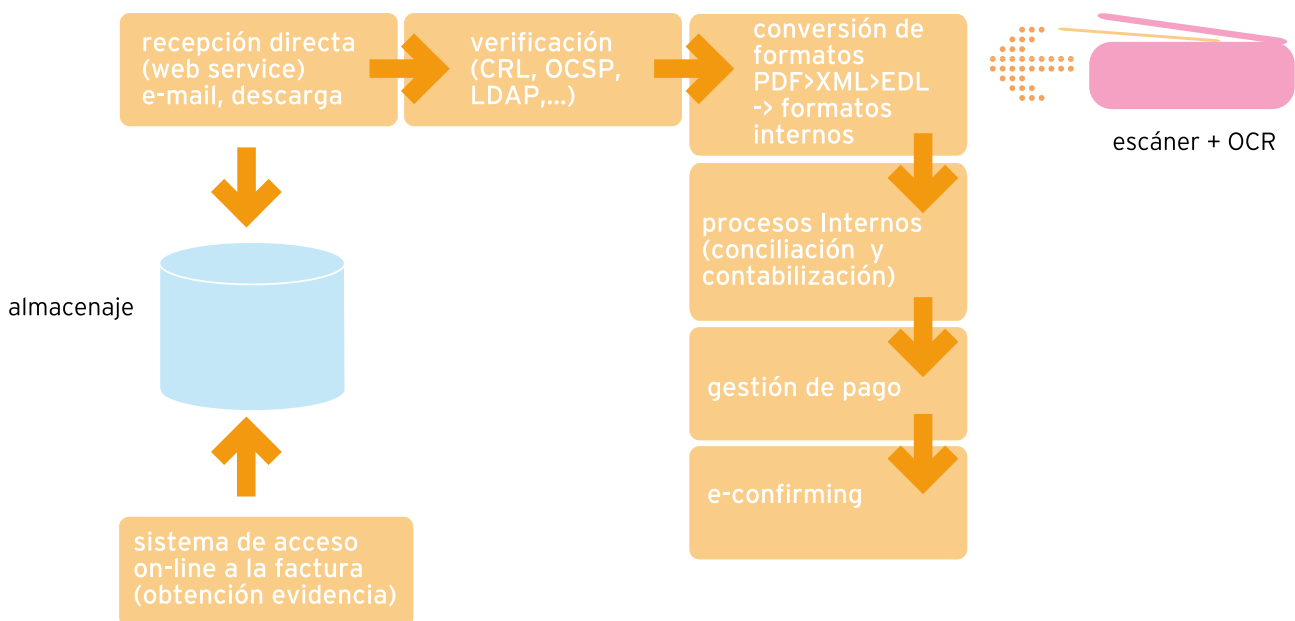


Fig. 8. Flujo base de recepción de facturas.

En la recepción, los dos elementos principales son el almacenamiento de la factura electrónica en su formato original y la verificación de su vigencia. Además será necesario adaptar el formato al que internamente maneja la aplicación de conciliación, para su contabilización y pago. Esta gestión puede acabar facilitando los servicios de confirming de entidades financieras.

“La complejidad de este tipo de proyecto radica en la necesidad de tratar con un número indeterminado de formatos electrónicos junto con la recepción de facturas en papel”.

La digitalización certificada definida en la Orden EHA/962/2007 permite transformar a formato electrónico las facturas recibidas en papel, para lo que los receptores no necesitan pedir permiso a nadie, aunque sí utilizar software homologado. Su objetivo es permitir conservar electrónicamente facturas recibidas en papel, de forma que se pueden destruir estas.

En la actualidad existen más de 30 sistemas de gestión documental homologados por la Agencia Tributaria para facilitar este proceso, que se considera un paso intermedio antes de llegar a implantar por completo la factura electrónica.

Una vez realizada la digitalización certificada de una factura, es posible destruir el documento en papel ya que el documento transformado tiene el carácter de "original".

Cómo se pueden hacer facturas electrónicas mediante plataformas de terceros

La posibilidad de delegar la ejecución material de la facturación, bien en los destinatarios de las operaciones (**autofactura**), bien en terceros mediante la contratación de sus servicios (**facturación por terceros**) se reconoce expresamente en el RD 1496/2003.

Independientemente del modelo adoptado, el responsable del cumplimiento de las obligaciones establecidas por la ley en relación a la facturación, es el empresario, profesional o **sujeto pasivo obligado a la expedición de la factura**. Lo que significa que, la delegación de la ejecución material de la facturación en terceros no exime de responsabilidad, por lo que los obligados tributarios deberán ser cuidadosos en la elección de su proveedor. La credibilidad del prestador de servicios es muy importante. (Ver artículos 5 y 19.3 del Real Decreto 1496/2003).

Para que revistan validez las opciones estudiadas deberán cumplirse los siguientes requisitos:

- Acuerdo previo documentado por escrito entre el obligado tributario emisor y la entidad que efectivamente gestione la expedición de la factura, ya sea un tercero o el obligado tributario receptor (autofactura). En el citado acuerdo constará de manera expresa la autorización del obligado tributario emisor y las operaciones comprendidas en el acuerdo.



- El empresario o profesional que delega la emisión de facturas en el destinatario de las mismas deberá aceptar o rechazar la emisión de cada factura concreta, para lo que dispondrá de quince (15) días desde la recepción de la copia o su acceso telemático a ella. El rechazo deberá ser expreso. Si se produce este rechazo, la factura se anula, o se tiene por no emitida. Por ello, es recomendable no asignar número a la factura hasta que se tenga la aceptación o hayan transcurrido quince (15) días. Para medir este tiempo, pueden utilizarse mecanismos de acuse de recibo, tales como por ejemplo la descarga de un fichero (un gráfico cualquiera o una versión reducida de la factura) en el e-mail enviado para notificar al vendedor sobre la disponibilidad de una factura para su aprobación.
- Estas facturas serán expedidas en nombre y por cuenta del empresario o profesional que haya realizado las operaciones que en ellos se documentan.

Para resolver el problema de los plazos y la indeterminación de la emisión de facturas, se recomienda que en el contrato, el obligado tributario emisor acepte explícitamente la emisión de facturas por el receptor, gestionando excepcionalmente las discrepancias que se pudieran detectar a través de las facturas rectificativas.

Cuando se usan servicios externos de facturación o se delega la gestión de facturas en algunos receptores, se debe asignar una serie específica por cada entidad que gestiona facturas por cuenta del obligado emisor.

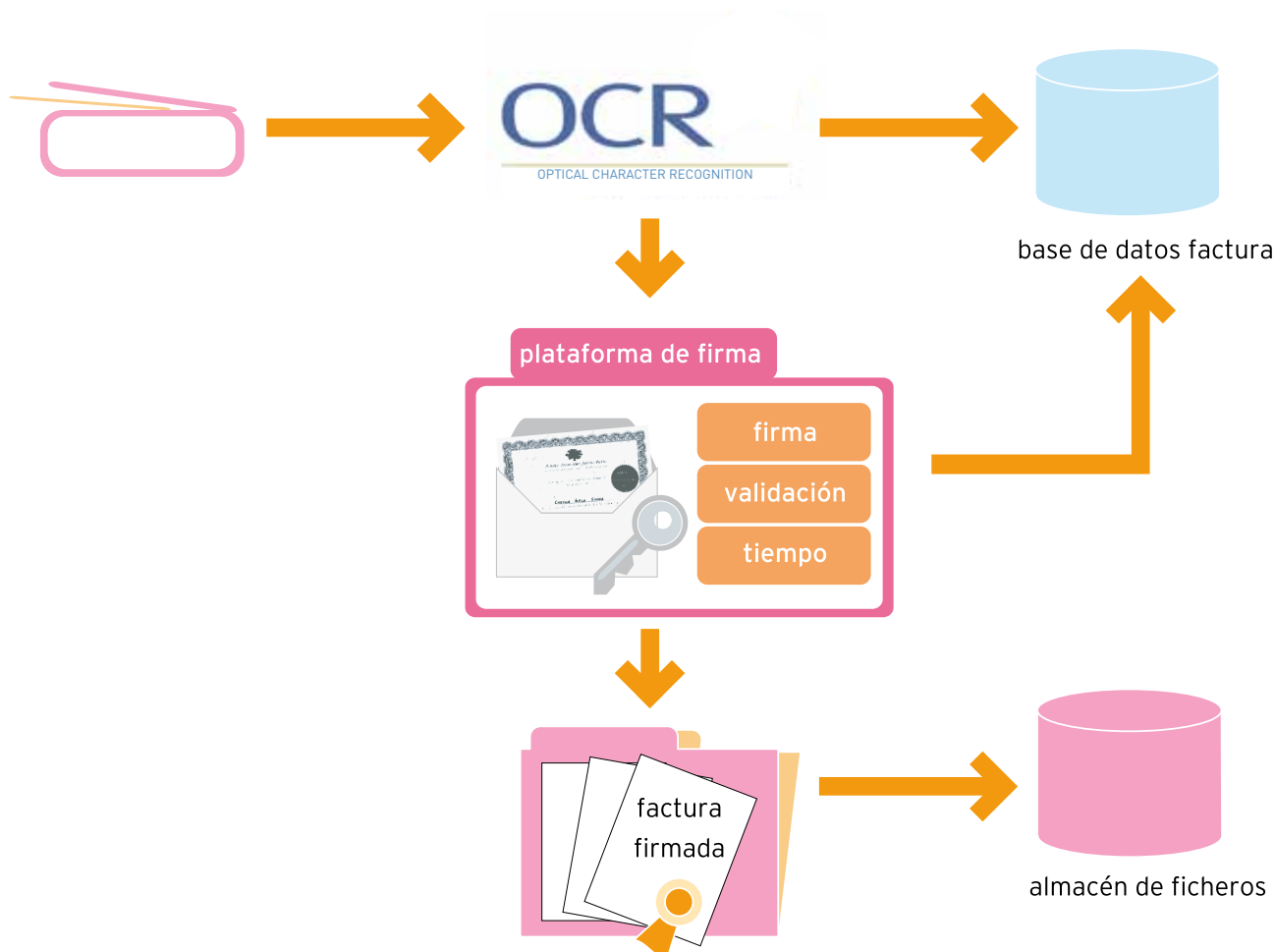


Fig.9. Esquema del proceso de digitalización certificada.

Tras la digitalización hay que firmar la factura. Un proceso complementario es la aplicación de sistemas OCR (reconocimiento de caracteres óptico) que permite extraer las palabras del documento con lo que se facilita la búsqueda posterior. En este ejemplo, se utiliza una modalidad de firma denominada "firma completa", que incluye información del momento de la verificación de validez del certificado y de la respuesta del prestador de servicios de certificación al consultar sobre dicha vigencia.

“La posibilidad de delegar la ejecución material de la facturación, bien en los destinatarios de las operaciones (autofactura), bien en terceros mediante la contratación de sus servicios (facturación por terceros) se reconoce expresamente en la normativa actual”.

Ejemplos de factura electrónica

Factura facturae

Aunque el usuario no necesita conocer la codificación interna de una factura electrónica, en ocasiones surge la curiosidad: ¿qué aspecto tiene por dentro un fichero de factura?

Aquí hay un ejemplo:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <fe:Facturae xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:fe="http://www.facturae.es/Facturae/2009/v3.2/Facturae">
- <FileHeader>
  <SchemaVersion>3.2</SchemaVersion>
  <Modality>I</Modality>
  <InvoiceIssuerType>EM</InvoiceIssuerType>
- <Batch>
  <BatchIdentifier>000000000B18</BatchIdentifier>
  <InvoicesCount>1</InvoicesCount>
- <TotalInvoicesAmount>
  <TotalAmount>63.13</TotalAmount>
</TotalInvoicesAmount>
- <TotalOutstandingAmount>
  <TotalAmount>63.13</TotalAmount>
</TotalOutstandingAmount>
- <TotalExecutableAmount>
  <TotalAmount>63.13</TotalAmount>
</TotalExecutableAmount>
  <InvoiceCurrencyCode>EUR</InvoiceCurrencyCode>
</Batch>
</FileHeader>
- <Parties>
- <SellerParty>
- <TaxIdentification>
  <PersonTypeCode>J</PersonTypeCode>
  <ResidenceTypeCode>R</ResidenceTypeCode>
  <TaxIdentificationNumber>A82735122</TaxIdentificationNumber>
</TaxIdentification>
- <LegalEntity>
  <CorporateName>Company Comp SA</CorporateName>
  <TradeName>Comp</TradeName>
```

```
- <RegistrationData>
  <Book>1</Book>
  <RegisterOfCompaniesLocation>12AP22</RegisterOfCompaniesLocation>
  <Sheet>3</Sheet>
  <Folio>15</Folio>
  <Section>2</Section>
  <Volume>12</Volume>
  <AdditionalRegistrationData>Sin datos</AdditionalRegistrationData>
</RegistrationData>
- <AddressInSpain>
  <Address>C/ Mayour 33 15º E</Address>
  <PostCode>28001</PostCode>
  <Town>Argamasilla de Alba</Town>
  <Province>Ciudad Real</Province>
  <CountryCode>ESP</CountryCode>
</AddressInSpain>
- <ContactDetails>
  <Telephone>917776665</Telephone>
  <TeleFax>917776666</TeleFax>
  <WebAddress>www.facturae.es</WebAddress>
  <ElectronicMail>facturae@mityc.es</ElectronicMail>
  <ContactPersons>Fernando</ContactPersons>
  <CnoCnae>28000</CnoCnae>
  <INETownCode>2134AAB</INETownCode>
  <AdditionalContactDetails>Otros datos</AdditionalContactDetails>
</ContactDetails>
</LegalEntity>
</SellerParty>
```

Fig. 10. Cabecera de un fichero de factura en formato facturae con firma electrónica XAdES-XL.

La visualización se logra mediante una plantilla de transformación XSLT (Extensible Stylesheet Language Transformations) y mediante una hoja de estilo CSS (Cascading Style Sheet), como la que está disponible en el portal facturae.es. Al aplicarla, se le da un aspecto concreto a la factura, pero podría ser otro aplicando una hoja de estilo diferente. En ocasiones, esto puede ser interesante cuando una persona tiene que revisar facturas, ya que se puede dar un mismo aspecto a las facturas de todos los proveedores.



FACTURA

Fecha de emisión:	26/04/2010	
Número:	Serie	Secuencia
Factura:	electronica	120

Emisor	
Razón Social:	demo facil
Dirección:	Alameda Fácil 1
CP:	28080 Madrid
Provincia:	Madrid
País:	España
NIF:	00000000T

Cliente	
Razón Social:	Joaquin
Dirección:	Calle sdfsgs 2
CP:	22222 Toledo
Provincia:	Toledo
País:	España
NIF:	03909546Y

Detalles								
Fecha	Concepto	Unidades	Precio	% dto	% IVA	% IRPF	Base Imponible	Importe €
2010-04-26	Tuercas	100	0,25	10,00	16,00	0,00	22,50	26,10
2010-04-26	Tomillos	100	0,25	10,00	16,00	0,00	22,50	26,10

Descuentos Generales		
Concepto	Descuento	Importe

Suplidos	
Fecha	Importe

Condiciones de pago	
Forma de pago:	Al contado
Vencimiento:	26/04/2010
Importe:	52,20

Totales	
Importe Total Bruto	45,00
Total Base imponible	45,00
Base Imponible (IVA 16%)	45,00
Cuota (IVA 16%)	7,20
Total Factura	52,20
TOTAL A PAGAR	52,20

Fig. 11. Presentación de una factura XML facturae en pantalla una vez aplicadas las hojas de transformación y de estilo.

Una factura XML se puede visualizar de formas diferentes según la plantilla (hoja de estilo) aplicada. Por ejemplo, el receptor puede aplicar su propia plantilla para facilitar la revisión de muchas facturas ya que los apartados esenciales de las facturas se posicionarán en la misma zona de la imagen.

Uso de aplicaciones en internet (“Software as a Service” o “computación en la nube”)

Las plataformas de terceros quizás son la opción más práctica para una pequeña o mediana empresa. Generalmente, se paga una cuota mensual por un servicio al que se accede de forma remota por internet, encargándose la tercera empresa de dotar de legalidad a sus facturas mediante la aplicación de su firma electrónica. En este caso la empresa que emite las facturas no tiene que

preocuparse de la obtención de los certificados digitales, porque de ello se encarga la empresa que presta el servicio. Algunos de los prestadores de servicios de facturación, no obstante, dan la opción de usar los certificados de la empresa, si dispone de ellos.

En estas plataformas se suele emplear la modalidad de facturación por terceros y en la mayoría de los casos incorporan un sencillo ERP válido para gestionar la facturación de una pequeña empresa.

The screenshot shows the Faccil web application interface for creating a new invoice. The interface is in Spanish and includes a navigation menu at the top with options: Facturas, Clientes, Productos, Configuración, and Validación de Facturas. The main content area is titled 'Nueva Factura' and contains a form for entering invoice details. The form fields include: Cliente (dropdown), Serie (dropdown), Fecha emisión (2010-04-25), Forma de pago (dropdown), IBAN (text), Vencimiento (dropdown), and Fecha vencimiento (2010-04-26). Below the form is a table for items with columns: Devenge, Código, Producto, Cantidad, PVP, Descuento, Neto, IVA, DDPF, and Total. There are also sections for 'Descuentos Generales' and 'Suplidos'. The status of the invoice is 'Nuevo'. The footer includes logos for INTERACTIVA, Faccil, factura-e, and LEAD, along with the text 'Faccil ©2009 | Nota Legal | Condiciones Generales'.

Fig. 12. Formación de la factura a través de un formulario.

En este caso se usa el servicio Faccil, uno de los muchos que existen en internet. También las entidades financieras, cuando prestan servicios de facturación, lo hacen con la modalidad de facturación por terceros, por lo que el aspecto de la pantalla es muy parecido a este.

Las facturas se confeccionan a través de formularios. Las facturas están en estado de borrador hasta que se decide que están completas y listas para emitir.

03.

Capítulo 3. Proyectos avanzados de factura electrónica

Identificación de proyectos avanzados

Los proyectos avanzados de factura electrónica implican una cierta complejidad en la implantación y habitualmente requerirán para su diseño e implementación la participación de varios departamentos en la empresa (informática, administración, facturación, compras, ...)

Ejemplos típicos de proyectos avanzados:

Consideraremos genéricamente que un proyecto de facturación electrónica es avanzado en los siguientes casos:

- Cuando se diseña un producto específico, orientado específicamente a las necesidades del usuario.
- Cuando se realiza una integración de una plataforma o producto genérico en los sistemas de información del usuario.
- Cuando se realizan modificaciones sobre elementos disponibles en la empresa, como la integración de la firma electrónica en los ERPs.

El nivel de dificultad y la duración de este tipo de proyectos variará en función de una serie de ele-

mentos clave como son la capacidad tecnológica y de desarrollo de la entidad, el grado de implicación de los participantes, la disposición de elementos claves en los sistemas de facturación electrónica (ERPs, certificados digitales, ...), la adaptabilidad de los elementos anteriores o la formación de los usuarios afectados.

En la mayoría de las ocasiones es aconsejable contar con entidades terceras, consultoras y desarrolladoras de software, que aportarán a la empresa su experiencia en proyectos de este tipo y cubrirán aquellas áreas a las que la entidad no puede llegar por sí misma. La actividad del experto puede abarcar diferentes aspectos:

- Consultoría y asesoramiento tecnológico
- Asesoría legal
- Asesoría fiscal
- Desarrollo e implantación
- Formación
- Sistemas y comunicaciones

En un proyecto de facturación electrónica avanzado es importante también delimitar claramente al inicio del proyecto cuál es el alcance que queremos darle al proyecto, es decir, tomar la decisión sobre los objetivos críticos, recomendables o innecesarios. Por ejemplo, una empresa puede plantearse realizar un proyecto de emisión y recepción dirigido a todas las empresas con las que se relaciona o, por el contrario, sólo aspira a resolver la facturación más compleja con aquellos clientes / proveedores estratégicos. De forma similar, puede decidir si abordar un proyecto completo (emisión / recepción) o por el contrario enfocarlo en cualquiera de los dos sentidos en función del mayor peso de alguno de los elementos.

Desde un punto de vista práctico, sería aconsejable comenzar desarrollando un proyecto según el peso de la facturación (emisión / recepción) sobre aquellos clientes con los que se tenga una mayor relación, para posteriormente ir completando el proyecto en función de los recursos disponibles. De esta forma, se resuelven de forma ágil las necesidades más apremiantes de la empresa, sin dejar de lado las posibles vías de crecimiento posterior.

Por último, es recomendable realizar un proyecto modular, que permita el crecimiento posterior de la plataforma y la reutilización de elementos para otros proyectos.

“En la mayoría de las ocasiones es aconsejable contar con entidades terceras, que aportarán a la empresa su experiencia en proyectos de este tipo y cubrirán aquellas áreas a las que la entidad no puede llegar por sí misma”.

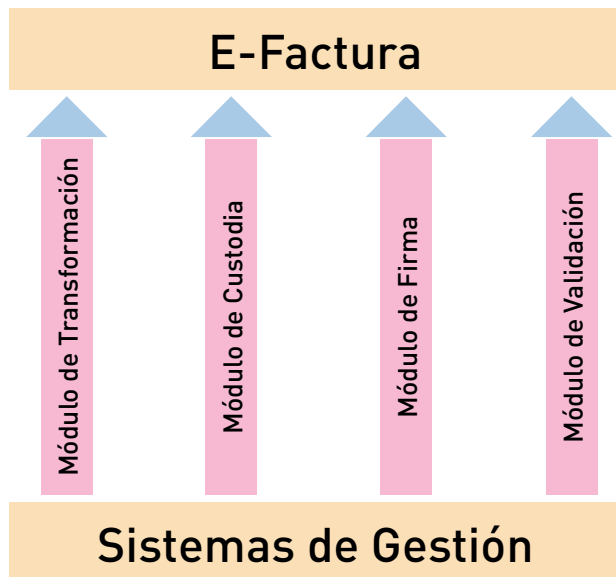


Fig. 13. Pilares básicos de la e-factura.

- **Módulo de transformación:**
Realiza modificaciones entre formatos de entrada y de salida.
- **Módulo de custodia:**
Método de almacenamiento de la factura original (generada o recibida).
- **Módulo de firma:**
Permite realizar firmas electrónicas en las facturas en aquellos casos en que el emisor no tenga la capacidad de firma.
- **Módulo de validación:**
Comprueba la corrección de las facturas recibidas y la validez de la firma electrónica.

El énfasis en la custodia o en la firma depende del rol de la entidad como emisor o receptor de facturas. Sin embargo, en ocasiones todos los módulos entran en juego. Por ejemplo, en las modalidades de autofacturación y facturación por terceros. En la autofacturación es el destinatario el que firma electrónicamente. En la facturación por terceros, un tercero firma electrónicamente la factura por cuenta del emisor y custodia la factura electrónica por cuenta del destinatario.

Proyectos orientados a la emisión de facturas

El objetivo principal de un proyecto de emisión de facturas suele ser lograr una reducción de costes derivada de la operativa manual de emisión de facturas: impresión, ensobrado, envío, ... pero también son objetivos relevantes la optimización de los recursos disponibles, la minimización de los tiempos de cobro o la fiabilidad en los métodos de conciliación contable.

Este es el tipo de proyecto más frecuente y el más sencillo de puesta en marcha, ya que por lo general, la empresa que emite es la que controla los formatos y el medio de emisión de la factura, sobre todo en aquellos casos en los que el proveedor tenga una posición de fuerza sobre sus clientes. No obstante lo anterior, en la mayoría de situaciones será necesario realizar conversiones de

formatos para garantizar la interoperabilidad con determinadas empresas.

La parte más compleja en los proyectos de emisión suele ser el proceso de firma electrónica, ya que implica la integración de las claves y certificados en la plataforma y el desarrollo de la aplicación de firma, máxime cuando se opta por emplear una firma electrónica (no exigida legalmente) con todos los elementos de validación que permitan su posterior verificación al receptor de forma fiable y perdurable en el tiempo, para lo cual nos podremos apoyar en **Prestadores de Servicios de Sellado de Tiempo (TSA)** y **Prestadores de Servicios de Validación (VA)**.

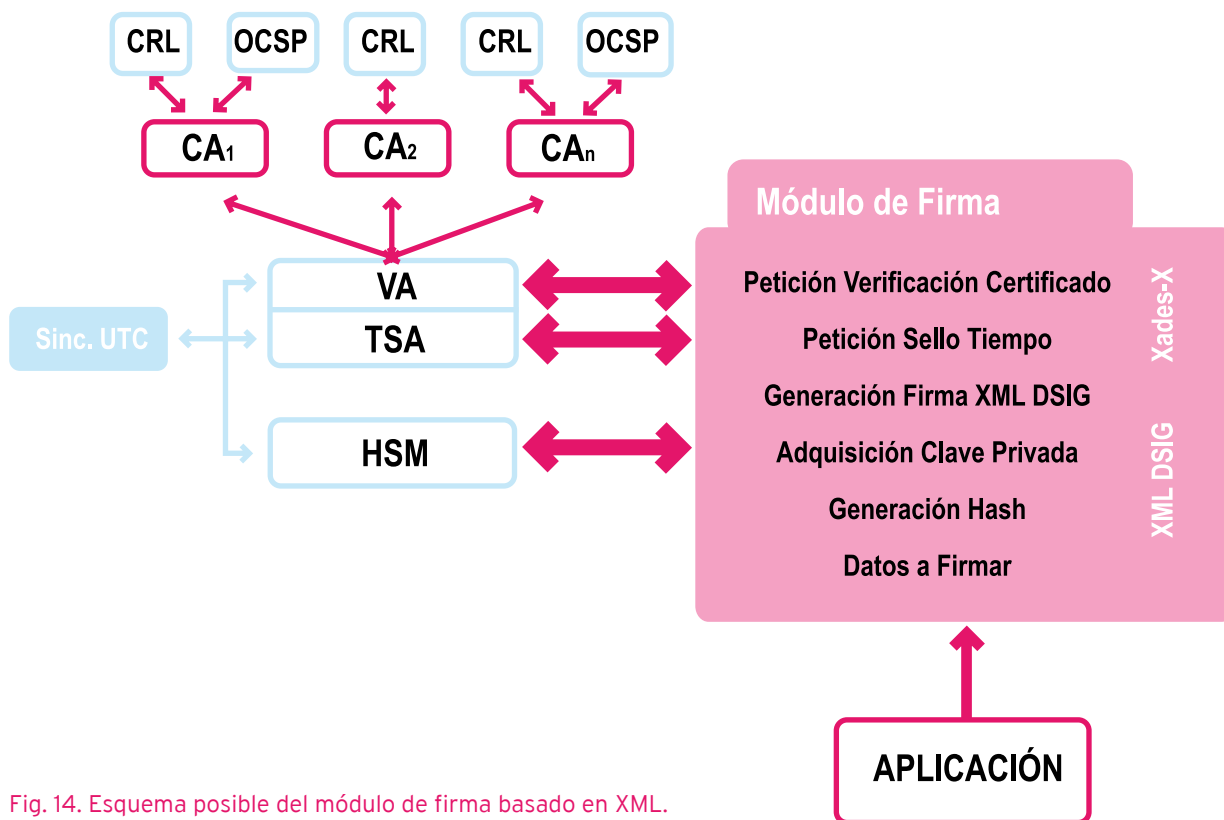


Fig. 14. Esquema posible del módulo de firma basado en XML.

Esta modalidad contempla la firma completa **ES-XL** descrita en la norma **TS 101 903**. Si la firma completa se forma en el lado del firmante, el tercero que confía en el certificado no debe preocuparse de conocer las peculiaridades del PSC (prestador de servicios de certificación) que expidió el certificado en lo relativo a los servicios de validación.

“La parte más compleja en los proyectos de emisión suele ser el proceso de firma electrónica”.

Aunque esta modalidad no es exigible desde un punto de vista normativo, libera al receptor del problema de validar firmas electrónicas en las que se haya empleado un certificado expedido por un prestador de servicios de certificación cuya gestión de los certificados revocados no sea fácilmente accesible para el receptor.

Proyectos orientados a la recepción de facturas

Si en el caso de la emisión decíamos que la parte más compleja era la de la firma electrónica de las facturas, en este caso, el elemento diferenciador es la validación, tanto del formato de los documentos facturas como de los certificados con los que estas han sido firmadas.

En el caso de la verificación de los formatos de las facturas, es necesario conocer el tipo de datos que se reciben para posteriormente convertirlo al formato interno de la empresa y poder tratarlo en las aplicaciones (generalmente el ERP). Evidentemente, los formatos estructurados como el XML facilitan enormemente la labor de conversión.

Para la validación de firmas electrónicas de las facturas, deberemos tener en cuenta dos elementos principales: el formato de firma empleado (XML, CMS, ...) y el certificado con el cual se ha firmado la factura. Respecto al primero, deberemos identificar el formato de firma para saber “parsear” esta firma y extraer los elementos necesarios (sujeto firmante, emisor del certificado, validez temporal, localización de la información de revocación, ...), una vez extraída la información

del certificado deberemos comprobar que el certificado estaba vigente en el momento de la firma y que el mismo no ha sido revocado, para lo cual podremos servirnos de la propia información contenida en el certificado, o valernos de elementos externos. En la actualidad se cuenta con elementos facilitadores de la labor de validación de firmas electrónicas, como es el caso de las Autoridades de Validación.

Afortunadamente, se van perfilando estándares tanto en el formato del propio documento factura como en la firma electrónica asociada, dirigidos

mayoritariamente hacia XML: **facturae, UBL, CII**, y en cuanto a la firma, XAdES,... Una vez realizados los procesos de validación y conversión, el receptor deberá integrar los datos obtenidos en su propio sistema, sin olvidar que debe custodiar la factura tal y como fue recibida, al considerarse esta como original a efectos fiscales.

Por último, como se ha comentado con anterioridad, debemos tener en cuenta la iniciativa de la Agencia Estatal de Administración Tributaria, para digitalizar y securizar las facturas recibidas en formato papel.

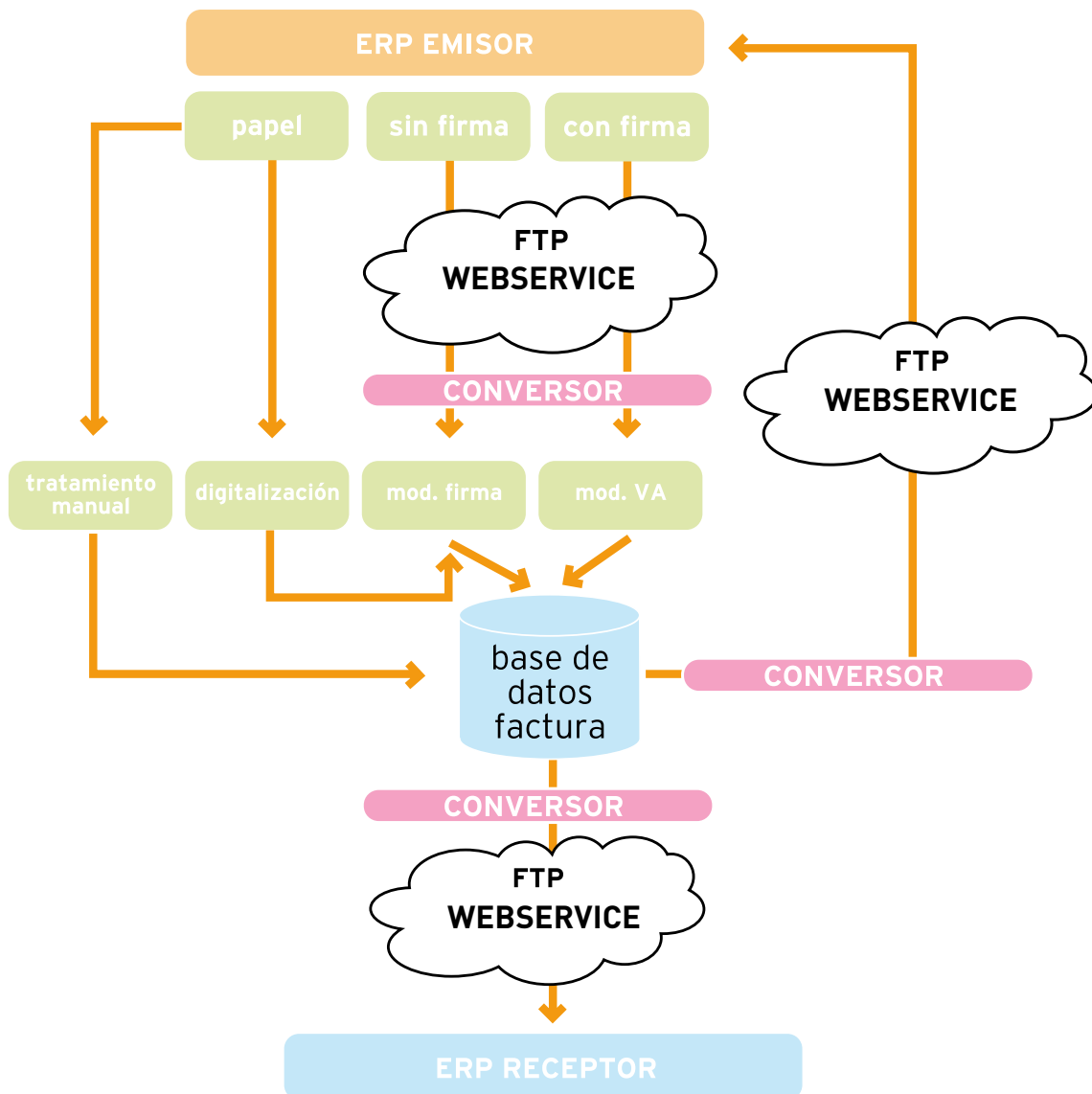


Fig. 15. Esquema de tratamiento e integración de facturas.

El uso de diferentes sistemas de transmisión debe ser tenido en cuenta en el proyecto, junto con los formatos de factura y los de firma.

“El elemento diferenciador es la validación, tanto del formato de los documentos facturas como de los certificados con los que aquellas han sido firmadas”.

Preparación del proyecto

Normalmente hay que tener en cuenta una pequeña lista de comprobación, para cerciorarnos de que satisfacemos todos los requisitos.

Elementos a recordar al abordar un proyecto de factura electrónica:

- Especificación del flujo de facturación
 - Diseño del flujo documental
 - Identificación de los roles implicados
 - Definición de los requisitos legales
 - Gestión de la integración con proveedores y clientes
 - Integración con los sistemas de la empresa
- **Especificación del flujo de facturación:** análisis de las características de los proveedores/clientes para determinar cómo los incorporamos al proyecto, y de los formatos en que emitimos/recibimos las facturas.
 - **Diseño del flujo documental:** para identificar ineficiencias en el proceso y facilitar la implantación de sistemas automatizados de workflow.
 - **Identificación de los roles implicados:** es básico identificar los recursos humanos internos y externos de la organización implicados en el proyecto, así como las excepciones.
 - **Definición de los requisitos legales:** definir aquellos aspectos de la normativa vigente que puedan afectar al proyecto.
 - **Gestión de la integración con proveedores y clientes:** tratar con proveedores y clientes todos aquellos aspectos que afecten a la funcionalidad, usabilidad, compatibilidad de formatos, ...
 - **Integración con los sistemas de la empresa:** lógicamente el sistema de facturación electrónica deberá estar integrado con los sistemas de la empresa: ERP, sistemas de facturación, CRM y sistemas de gestión de pagos.

Facturación electrónica a las Administraciones Públicas

Las administraciones públicas, en aplicación de la Ley 11/2007 de Acceso electrónico de los ciudadanos a los servicios públicos, deben estar en disposición de recibir facturas electrónicas siempre que sus suministradores lo soliciten. Sin embargo, esto no se traduce en una obligación para las empresas de facturarles electrónicamente.

La norma que sí impone obligaciones de facturación electrónica a las empresas suministradoras del sector público estatal es la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público. También lo establece la Ley 56/2007, de 28 de diciembre, de Medidas de impulso de la sociedad de la información, que además impone actuaciones de dinamización del uso de la factura electrónica dirigidas al resto de la actividad productiva del país, que se realizarán favoreciendo la colaboración entre el Ministerio de Industria, Turismo y Comercio y el Ministerio de Economía y Hacienda, y entre estos y las Comunidades Autónomas.

Los ministerios citados han colaborado en el despliegue del portal *facturae* (<http://www.facturae.es>) y en el desarrollo de la 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, que establece el formato de factura electrónica que se envía a una administración pública.

Asimismo, el Ministerio de Industria, Turismo y Comercio, desde su Subdirección General de Tecnologías de la Información y de las Comunicaciones, ha llevado a cabo una serie de desarrollos que facilitan la integración de la factura electrónica en las PYMEs, así como herramientas que permiten la verificación de los documentos firmados, garantizando así la autenticidad e integridad del proceso de facturación electrónica.

Además de este esfuerzo, las Administraciones Públicas europeas están colaborando desde hace tiempo en la definición de los criterios de interoperabilidad que sin renuncia a aspectos de soberanía sean deseables en la contratación pública y en otras actividades de desarrollo de las Administraciones Públicas. Entre los desarrollos más relevantes están los del Proyecto Peppol (Pan-European Public Procurement Online). Este proyecto tiene como objetivo establecer una solución piloto a nivel europeo que, junto a las soluciones nacionales, facilite una contratación pública electrónica interoperable a través de Europa.

Desde el punto de vista de la normalización, cabe destacar dos iniciativas de CEN (Comité Europeo de Normalización).

Una de ellas es CEN/ISSS Business Interoperability Interfaces for Public eprocurement in Europe Workshop (BII), que, sobre la base de UBL, define los mensajes necesario en base, entre otras referencias, a la ontología definida sobre CODICE (Componentes y Documentos Interoperables para la Contratación Electrónica). CODICE es un desarrollo impulsado por la Dirección General de Patrimonio del Estado dependiente del Ministerio de Economía y Hacienda de España.

La otra iniciativa de CEN es CEN Workshop on eInvoicing, que ya ha iniciado la fase 3, tras publicar en sus fases anteriores relevantes documentos y estudios de aplicación de la normativa de factura electrónica en toda Europa.



04.



Capítulo 4. Interacción con la factura papel

Cómo se conservan electrónicamente facturas recibidas en papel

Aunque normativamente se prevé la conservación electrónica de facturas, por la condición de que las facturas deban estar disponibles para la inspección tributaria en el formato original en el que fueron recibidas, hasta muy recientemente se entendía que dicha conservación electrónica sólo aplicaba a las facturas remitidas electrónicamente.

En estos momentos la Orden EHA/962/2007 define la forma de gestionar electrónicamente las facturas recibidas en papel gracias al concepto de **digitalización certificada**. Se trata de un proceso en que, partiendo de una factura en papel, se genera una imagen digital firmada electrónicamente a la que se le aplica la presunción de tener el mismo valor probatorio que la factura original, mayor, incluso que el de una compulsión electrónica, permitiendo por ello destruir la propia factura original en papel.

Para que se dé por buena la presunción descrita, será preciso utilizar dispositivos homologados (que deberán superar una auditoría para obtener la homologación).

Para garantizar que los documentos así digitalizados cumplen de forma íntegra las condiciones de autenticidad, se recomienda utilizar la modalidad de firma electrónica **ES-X-L**, también llamada **firma completa**, ya que quien deba verificar la firma no debe preocuparse de encontrar el mecanismo de comprobación de validez, que puede ser diferente para cada prestador. Debe tenerse en cuenta que sólo en España existen más de 20 sistemas de certificación, cada uno de los cuales tiene su propio mecanismo de verificación.

Si se emplea un sistema OCR (Optical Character Recognition), el sistema puede reconocer letras y números y superponerlos en una capa del fichero, de forma que se simplifica la indexación y la búsqueda de documentos. Si además la factura se ha impreso según una plantilla acordada, el OCR permitirá codificar la factura en el formato estándar **facturae** u otro, facilitando también la inserción del contenido de la factura en el sistema informático y su tratamiento más o menos automatizado.

Por este motivo se recomienda la adopción de modelos de factura concretos por parte de los emisores. Así, incluso cuando se emite una factura en papel, se puede estar facilitando la labor al receptor.

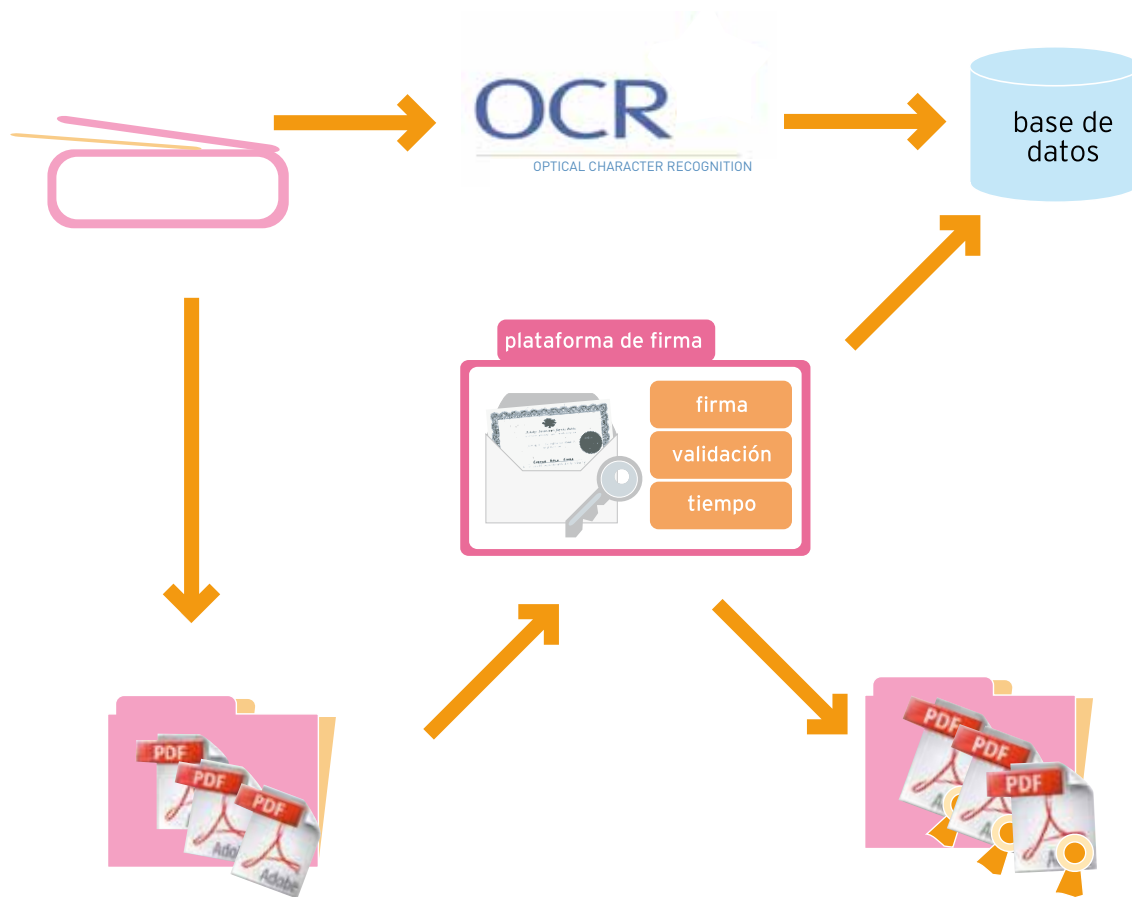


Fig. 16 - Proceso de digitalización certificada.

El receptor de la factura en papel no necesita autorización para digitalizar las facturas con el concepto de "digitalización certificada", siempre que utilice un software homologado por la Agencia Tributaria y un certificado electrónico con el que se firman electrónicamente los documentos digitalizados. Es frecuente el uso del formato PDF para las digitalizaciones, por lo que es fácil leer las facturas digitalizadas y comprobar los metadatos y las firmas electrónicas con el software gratuito Adobe Reader.

Cómo se conservan en papel facturas recibidas electrónicamente

Aunque existe la posibilidad de almacenar facturas electrónicas en papel mediante un código de barras, es posible otro mecanismo alternativo.

Cuando sea un tercero que actúa en nombre y por cuenta de los obligados tributarios, el emisor o el receptor de facturas electrónicas podrá poner a disposición de sus clientes aplicaciones informáticas que gestionen un repositorio de facturas y documentos sustitutos emitidos o recibidos, según corresponda, junto con la firma electrónica generada o verificada (según corresponda al rol de

emisor o de receptor de la factura), proporcionando un código seguro de verificación del documento. Este código permitirá el acceso al documento asociado existente en el repositorio (por ejemplo, a través de un acceso web) y garantizará, al que accede, el cumplimiento de los requisitos legales de la factura electrónica. En este supuesto, un documento impreso en papel con este código es válido, como sistema de conservación en papel de la factura electrónica, siempre que se mantenga el mencionado repositorio en el que se encuentra el documento y su firma electrónica, exista un mecanismo de verificación de la firma en el mismo y se pueda acceder de forma completa al documento mediante dicho código electrónico de autenticación. Así lo expresa el artículo 6 de la Orden EHA/962/2007.

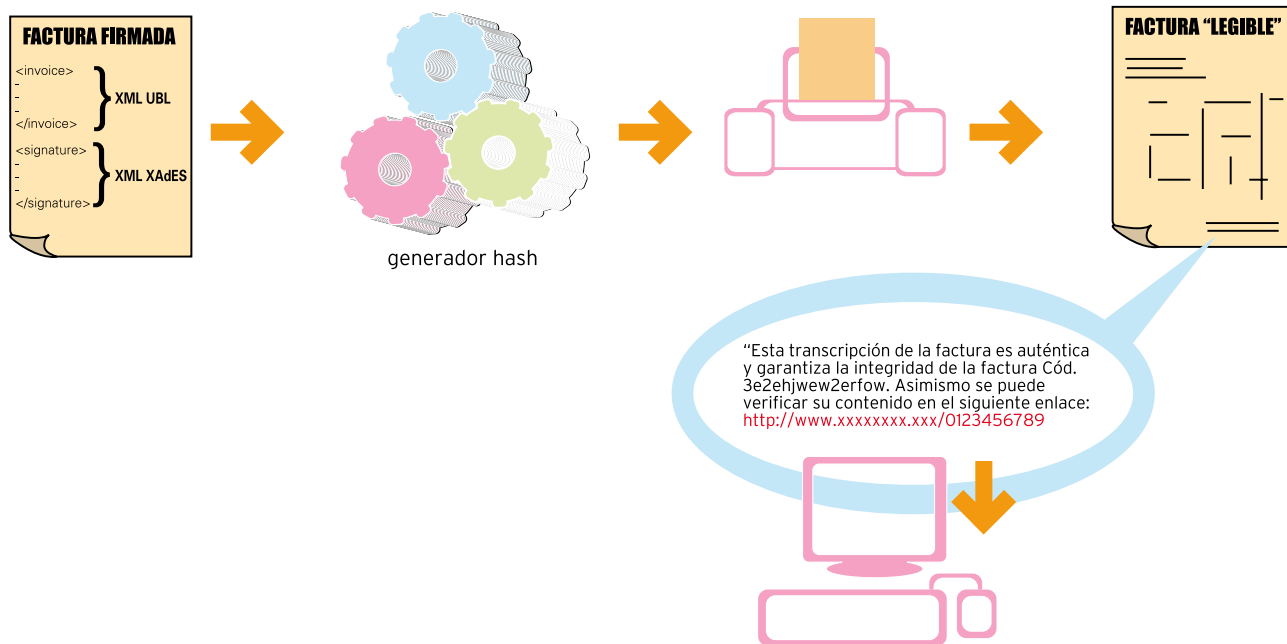


Fig. 17. Ejemplo de esquema de generación de código de recuperación de facturas.

Con los datos de la factura electrónica se genera un código identificador único susceptible de ser introducido en la copia papel de la factura para su posterior localización y recuperación.

"Aunque existe la posibilidad de almacenar facturas electrónicas en papel mediante un código de barras, es posible otro mecanismo alternativo".



05.

Capítulo 5. Formatos de factura y firma electrónica

Formato de la factura electrónica

El formato contenedor de la factura, esto es, aquel fichero donde se almacenan los datos que conforman la factura antes de aplicarles la firma electrónica, no es relevante desde el punto de vista legal si no se factura a una entidad pública. Podría tratarse de un fichero PDF, un archivo RTF, un documento Excel, texto plano, HTML, XML, etc. Cualquier formato empleado es válido siempre que posteriormente sea firmado electrónicamente para dotarlo de validez legal.

En España, cuando el destinatario sea una administración de la Administración General del Estado, existe la obligación de codificar la factura en formato XML **facturae**. Según la disposición final segunda de la Orden PRE/2971/2007, este formato se adecuará, transcurridos dos años desde la publicación de la norma, al formato **UBL (Universal Business Language)** o, en su caso, al formato que establezcan los organismos de normalización de la Unión Europea CEN (Comité Europeo de Normalización) o CENELEC (Comité Europeo de Normalización Electrotécnica), de forma que se permita la interoperabilidad de las facturas emitidas por cualquiera de los Estados miembros de la Unión Europea.

En la actualidad existe cierto consenso internacional para adoptar la futura especificación UN/CEFACT CII (Cross Industry Invoice).



```

<Invoice
xmlns:qdt="urn:oasis:names:specification:ubl:schema:xsd:QualifiedDatatypes-2"
xmlns:udt="urn:un:unece:uncefact:data:draft:UnqualifiedDataTypesSchemaModule:2"
xmlns:cbc="urn:oasis:names:specification:ubl:schema:xsd:CommonBasicComponents-2"
xmlns:cac="urn:oasis:names:specification:ubl:schema:xsd:CommonAggregateComponents-2"
xmlns:stat="urn:oasis:names:specification:ubl:schema:xsd:DocumentStatusCode-1.0"
xmlns:ccts="urn:oasis:names:specification:ubl:schema:xsd:CoreComponentParameters-2"
xmlns="urn:oasis:names:specification:ubl:schema:xsd:Invoice-2">
  <cbc:UBLVersionID>2.0</cbc:UBLVersionID>
  <cbc:ID>E-0000001</cbc:ID>
  <cbc:CopyIndicator>>false</cbc:CopyIndicator>
  <cbc:IssueDate>2010-01-13</cbc:IssueDate>
  <cbc:InvoiceTypeCode>Comercial</cbc:InvoiceTypeCode>
  <cbc:DocumentCurrencyCode>EUR</cbc:DocumentCurrencyCode>
  <cac:Signature>
    <cbc:ID>UBL_Signature_1</cbc:ID>
    <cac:SignatoryParty>
      <cac:PartyIdentification>
        <cbc:ID>ESB84009240</cbc:ID>
      </cac:PartyIdentification>
      <cac:PartyName>
        <cbc:Name>Demo Facturae</cbc:Name>
      </cac:PartyName>
      <cac:PartyLegalEntity>
        <cbc:RegistrationName>Demo Facturae</cbc:RegistrationName>
        <cbc:CompanyID>ESB84009240</cbc:CompanyID>
        <cac:RegistrationAddress>
          <cbc:StreetName>Calle de la Factura Electronica, 1</cbc:StreetName>
          <cbc:BuildingNumber />
          <cbc:CityName>Madrid</cbc:CityName>
          <cbc:PostalZone>28001</cbc:PostalZone>
          <cbc:CountrySubentity>Madrid</cbc:CountrySubentity>
          <cac:Country>
            <cbc:IdentificationCode>ESP</cbc:IdentificationCode>
          </cac:Country>
        </cac:RegistrationAddress>
      </cac:PartyLegalEntity>
    </cac:SignatoryParty>

```

Fig. 18. Extracto de factura en XML (formato UBL) con firma electrónica. Puede encontrar más información sobre este formato en <http://www.oasis-open.org/committees/ubl/>.

Formato de firma

Formatos de firma especiales: firma fechada y validada

Además de los tipos de firma **simple**, **avanzada** y **reconocida** (qualified electronic signature en inglés), que establecen tanto la Directiva como la Ley de Firma Electrónica, desde el punto de vista técnico, se han definido en el marco de ETSI (European Telecommunications Standards Institute) los subtipos de firma electrónica avanzada que son esenciales para facilitar su uso en diferentes contextos.

Los tipos de firma de relevancia legal son los siguientes:

- **Simple.** Son datos que puedan ser usados para identificar al firmante (autenticidad)
- **Avanzada.** Además de identificar al firmante permite garantizar la integridad del documento.
- **Reconocida.** Es la firma avanzada, amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante) y realizada con un dispositivo seguro de creación de firma. En ocasiones, esta firma se denomina cualificada por traducción del término inglés qualified que aparece en la Directiva europea de firma electrónica.

Por otro lado, la firma avanzada puede incluir más o menos información, relativa al momento de creación o a la validez de los certificados. La más sencilla es la **básica**, que recoge los elementos esenciales de la firma electrónica: el resumen del documento firmado (hash), el certificado del firmante asociado a la clave privada con la que se firma, y el propio resultado de aplicar la clave privada al resumen, que es la firma electrónica propiamente dicha.

La firma **fechada** añade a la firma básica información temporal sobre el momento de la firma o de su verificación, y la firma **validada** añade a la firma fechada información sobre la vigencia del certificado empleado en el momento de la firma o de su verificación.

Cuando la firma electrónica se codifica en XML, estas modalidades de firma están recogidas en la norma TS 101 903, en sus vertientes XAdES-BES, XAdES-T y XAdES-XL, aunque existen más variantes.

La firma validada se denomina también firma completa, porque incluye todos los elementos que permiten comprobar que el certificado utilizado por el firmante estaba vigente en el momento de la firma, y permite su almacenamiento a largo plazo.

La ventaja de codificar la firma en formato XAdES-XL por parte del firmante es que se exonera al receptor del problema de validar el certificado utilizado, porque en la firma ya se incluyen todos los elementos que garantizan su validez en el momento de la firma.

Las firmas electrónicas utilizadas en facturación electrónica suelen ser las avanzadas y reconocidas, y, en el caso de facturas, en las modalidades XAdES-BES y XAdES-XL.

Firmas XML

Las firmas XML se utilizan cuando las propias facturas se codifican en XML, aunque pueden aplicarse a cualquier tipo de documento, con independencia de su formato.

Dentro de la firma electrónica en formato XML, existen diferentes subtipos de formatos, dentro de los cuales destaca el XML Advanced Electronic Signatures (XAdES).

En toda firma XML, existen 3 modalidades de firma:

- **Enveloped**, en el que la firma se añade al final del documento XML como un elemento más.
- **Enveloping**, en el que el documento se incluye dentro de la firma en la que se referencia lo firmado como objeto insertado en la firma.
- **Detached**, en el que la firma y el documento se separan en dos archivos, la URL donde se encuentra el documento puede aparecer en la propia firma.

```

<ds:Signature >
  <ds:SignedInfo/>
  <ds:SignatureValue/>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate/>
    </ds:X509Data>
  </ds:KeyInfo>
  <ds:Object>
    <xades:QualifyingProperties>
      <xades:SignedProperties>
        <xades:SignedSignatureProperties>
          <xades:SigningTime />
          <xades:SigningCertificate/> ?
          <xades:SignaturePolicyIdentifier/>
          <xades:SignerRole/> ?
        </xades:SignedSignatureProperties>
      </xades:SignedProperties>
      <xades:UnsignedProperties>
        <xades: UnsignedSignatureProperties>
          <xades: SignatureTimeStamp /> *
          <xades: CompleteCertificateRefs/>
          <xades: CompleteRevocationRefs/>
          (<SigAndRefsTimeStamp> * |
           <RefsOnlyTimeStamp> *)
          <xades: CertificateValues>
          <xades: RevocationValues/>
        </xades: UnsignedSignatureProperties>
      </xades:UnsignedProperties>
    </xades:QualifyingProperties>
  </ds:Object>
</ds:Signature>

```

Fig. 19. Firma XML (XAdES-XL) de la política de firma facturae 3.1.

A pesar de que los datos relativos tanto al sellado de tiempo como a la revocación del certificado pueden ser de gran utilidad y aportar un gran valor añadido al proceso de firma, éstos no son obligatorios para dotar de validez a una factura electrónica.

Anexo

Anexo I. Introducción a la firma electrónica y a la certificación electrónica

PSC y CA

En las siguientes páginas se utilizan dos términos que frecuentemente se usan como sinónimos pero que no lo son. Prestador de servicios de certificación (PSC) es un término legal, que se define en la Directiva 93/1999 y en la ley 59/2003, mientras que Autoridad de Certificación (AC) es un concepto técnico expresamente recogido en la recomendación X.509 de la UIT-T. El término PSC es más amplio, puesto que incluye a las AC que "expiden certificados electrónicos", y también a aquellos que "prestan otros servicios en relación con la firma electrónica", por ejemplo AV (Autoridad de Validación), AR (Autoridad de Registro), AST (Autoridad de Sellado Temporal). Con frecuencia se usan sus términos equivalentes en inglés: CSP (Certification Service provider), CA (Certification Authority), VA (Validation Authority), RA (registration Authority) y TSA (Time Stamping Authority).

La firma manuscrita

La firma manuscrita permite certificar el reconocimiento o conformidad sobre un documento por parte del firmante, de forma que tiene una gran importancia desde el punto de vista legal. Aunque existen diferentes formas de mostrar o demostrar conformidad con diferentes actuaciones, o de cerrar acuerdos entre personas o empresas, la firma manuscrita tiene un reconocimiento particularmente alto.

La firma manuscrita tiene las siguientes propiedades:

- Sólo puede ser realizada por una persona
- La puede comprobar cualquier persona, con la referencia de una muestra

El problema del reconocimiento de firma se resuelve, cuando ésta es manuscrita, mediante la comparación con una muestra (la del carné de identidad, la de la tarjeta de crédito).

Algo que es tan fácil de hacer y comprobar en el mundo real, no es tan sencillo en el mundo virtual. Requiere el uso de la **criptografía** y el empleo de propiedades matemáticas de los mensajes codificados.

Criptografía

El objetivo básico de la criptografía es encontrar sistemas que permitan hacer llegar determinada información considerada secreta, desde un lugar origen a otro destino, de forma tan segura que, si el mensaje es interceptado, un atacante no pueda reconocer el mensaje.

Uno de los objetivos de la criptografía moderna es encontrar algoritmos basados en principios matemáticos (como la imposibilidad de tratamiento computacional de determinados problemas complejos) que, siendo públicos (es decir, supuestamente conocidos por un criptoanalista atacante) permitan garantizar la inviolabilidad de los mensajes protegidos por ellos, al menos durante el tiempo en que pueda ser útil el conocimiento de la información protegida. Asimismo, no debe ser posible obtener las claves a partir del conocimiento de fragmentos cifrados y en claro del mensaje.

Cifrado simétrico

La característica principal de la criptografía simétrica es que, utilizando el mismo algoritmo y la misma clave, permite obtener el texto cifrado a partir del texto en claro y viceversa. Por este motivo, puesto que el algoritmo es público, es necesario mantener el secreto de la clave entre las partes que intervienen.

El cifrado simétrico es el más fácil de entender, porque se parece a la forma en que guardamos las cosas en la vida real. Veamos un ejemplo:

Supongamos que tenemos una caja con una cerradura. Si hacemos una sola copia de la llave y se la damos a nuestro interlocutor, disponemos de un mecanismo para intercambiar objetos o mensajes de forma confidencial y segura con él.

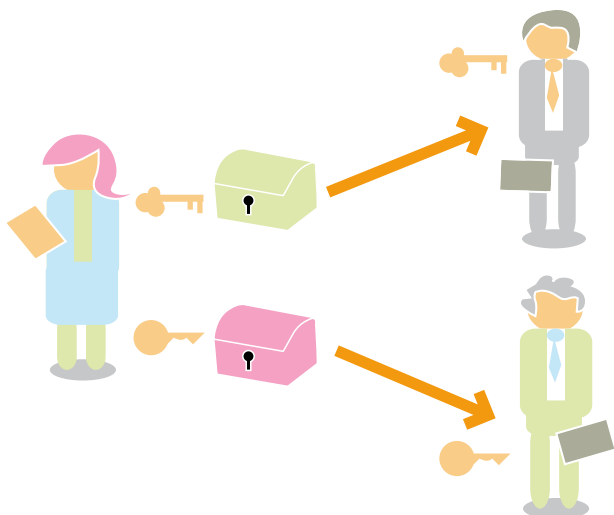


Fig. 20. *Compartición de claves simétricas.*

La clave que permite intercambiar información entre Alicia y Borja debe de ser diferente de la que comparten Alicia y Carlos.

De esta forma se puede comprobar que el envío lo hemos hecho nosotros porque somos los únicos que hemos podido introducir el documento (el uso de la caja actúa como firma) y además sabemos que nadie más puede conocer su contenido mientras viaja (uso como sobre seguro).

El mayor problema aparece cuando deseamos que un conjunto numeroso de interlocutores puedan mantener comunicaciones entre ellos. En este caso son necesarias muchas cajas y el doble de llaves.

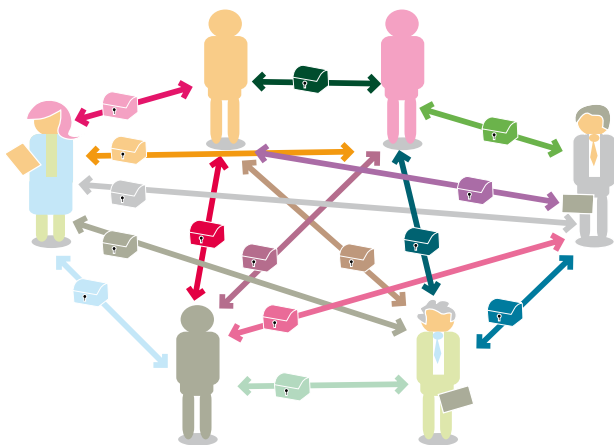


Fig. 21. *Problema de multiplicidad de intervinientes y llaves.*

No es practicable un sistema en el que haya que gestionar claves para cada dos personas

No pueden tenerse cajas y llaves iguales para interlocutores distintos, ya que ello conllevaría el riesgo de suplantación o de pérdida del secreto en el mensaje.

Cifrado asimétrico

Existe la posibilidad de encontrar algún sistema que utilice claves **distintas** para cifrar y descifrar un mensaje, de forma que el conocimiento de la clave de cifrado no permita el descifrado del mensaje e, inversamente, que el conocimiento del texto cifrado y de la clave de descifrado no diga nada acerca de la clave de cifrado.

Este concepto propuesto por Hellman y Diffie en 1.976 tiene uno de los exponentes más difundidos en el algoritmo de Rivest, Shamir y Adleman (RSA), basado en la intratabilidad computacional de la factorización en los números primos que los componen, de grandes números compuestos.

En los algoritmos con parejas de claves, llamados también asimétricos o de clave pública, una de las claves se mantiene secreta, mientras que la otra se hace libremente disponible: pública.

El cifrado asimétrico es difícil de entender, y, a veces, incluso difícil de creer. Para intentar explicarlo, sin recurrir a las matemáticas, recurriremos de nuevo a un símil de cajas y de llaves.

En este caso, no utilizamos cajas normales, sino "cajas de mago".

Supongamos que tengo una caja de doble fondo, cuyo anterior propietario era un mago, con una tapa que se abre de dos formas distintas con diferentes llaves. La propiedad de la caja es que lo que se introduce cuando se abre con una llave pasa a un compartimento al que solo se puede acceder si se utiliza la otra llave. En esto, ambas llaves son equivalentes, es decir, lo que se introduce usando una llave sólo puede recuperarse utilizando la otra.

Si una de las llaves la guardo de la forma más segura de que soy capaz, y de la otra hago copias que reparto ampliamente o que difundo a través de un medio público, cualquiera que tenga una de esas llaves podrá entregarme sólo a mí un objeto sin que los demás lo conozcan. Sólo yo seré capaz de recoger el envío. En ese caso, la caja se utiliza como **sobre seguro**.



La caja de mago con dos llaves

Fig. 22. Caja de mago: una sola llave de entrada y muchas copias de la llave de salida.

La llave de entrada es la PRIVADA, y la de salida, con múltiples copias es la PÚBLICA.

Por otro lado, si decido demostrar que sólo yo he tenido acceso a determinado dato u objeto, puedo introducirlo con mi llave en la caja. Cualquiera que abra la caja y encuentre el objeto, sabe que sólo yo lo he podido introducir allí. En este caso, la caja es la herramienta que me permite realizar mi **firma electrónica**.

Si cada persona dispone de una caja como la mía y reparte las llaves públicas a las demás, todos disponemos de un sistema para enviarnos mensajes de forma segura o para firmar envíos. En el caso de 1000 personas, necesitamos 1000 cajas y cada uno tenemos nuestra clave privada y las claves públicas de las otras 999.

Para poder comparar, hay que pensar que con el sistema de cifrado simétrico, con cajas convencionales, serían necesarias 499.500 cajas y el doble de llaves (Combinaciones de 1.000 elementos tomados de dos en dos).

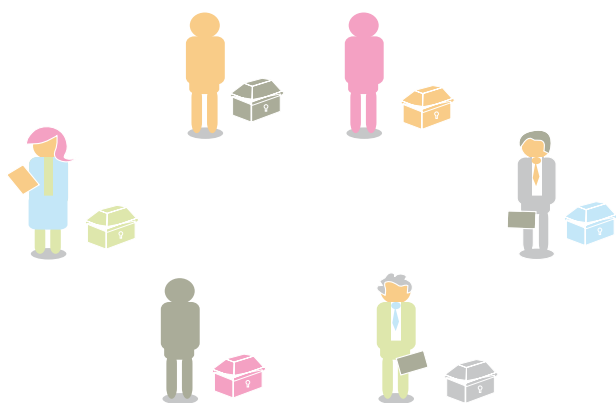
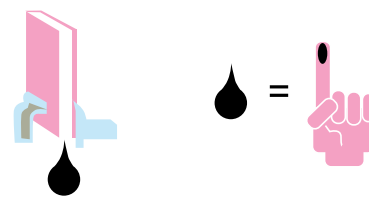


Fig. 23. Analogía de múltiples cajas y claves.

Ya no es necesario compartir llaves por cada dos usuarios, como con el sistema de clave simétrica, sino que cada usuario tiene su pareja de claves pública-privada.

Con principios equivalentes, la firma electrónica se basa en los sistemas criptográficos de clave pública. En estos sistemas se tiene un algoritmo que toma un texto en claro y lo cifra con una clave. El texto cifrado se restituye al texto original mediante otra clave distinta y vinculada a la de cifrado. Si la clave de cifrado sólo la tiene una persona y la de descifrado la conoce todo el mundo, lo que cifre esa persona podrá ser utilizado como su firma electrónica, ya que sólo ella la puede realizar y en cambio todo el mundo la puede reconocer.

Dando un paso más: si tomamos un documento electrónico y le aplicamos un algoritmo tal que nos permita obtener un código corto que dependa del contenido del documento (algo así como la esencia del documento, su huella dactilar, tal que si cambia cualquier carácter del documento, cambia el resultado) y ciframos el código corto con la clave privada, entonces obtenemos una firma electrónica que permite comprobar si se han realizado modificaciones sobre el documento.



Obtención de MAC* El MAC* es la huella del documento

Fig. 24. Analogía del código de autenticación de mensaje como huella dactilar de un documento.

El "hash" o "MAC" es una función resumen que calcula un valor dependiente del documento sobre el que se calcula, y que es diferente para diferentes documentos, por pequeña que sea su diferencia.

Frecuentemente, a este código se le denomina función HASH o MAC (Message Authentication Code), y se calcula en el momento de la firma, y también cuando se desea realizar su comprobación.

El resultado del algoritmo y el de descifrado de la firma electrónica deben coincidir: es el código corto que permite comprobar que nadie ha modificado el documento que se utilizó como base cuando se llevó a cabo la firma electrónica.

Aparentemente, ha quedado resuelto el problema de realizar y comprobar la firma electrónica, pero todavía es necesario un elemento fundamental: el **prestador de servicios de certificación**.

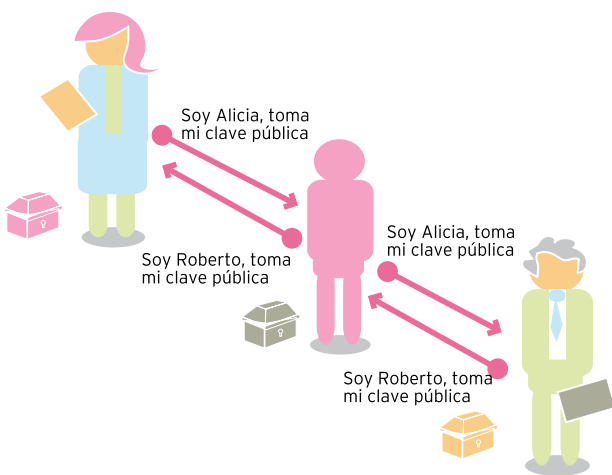


Fig. 25. Problema "Man in the middle".

Hay que resolver este problema aunque sea más teórico que real.

Para ver su necesidad, podemos plantearnos el caso en el que dos personajes, Alicia y Roberto, se intercambian sus claves públicas mediante un sistema de comunicaciones.

Es posible que se produzca la interceptación de los mensajes y que tanto Alicia como Roberto queden confundidos acerca de sus identidades y claves. Una vez intercambiadas las claves a través de este atacante, sería posible para él descodificar y recodificar los mensajes sin que Alicia ni Roberto se percataran de que todos sus mensajes son conocidos y suplantados por el atacante.

Prestador de servicios de certificación

Para evitar la interceptación de los mensajes por parte de un interlocutor ilegítimo que se inserta en el circuito de intercambio de claves, se cuenta con una entidad reconocida por parte de los participantes denominada prestador de servicios de certificación.

El prestador de servicios de certificación recibe la petición de un participante para que emita un certificado que garantice que su clave pública es precisamente la suya, para lo cual realiza las indagaciones necesarias que permitan confirmar la identidad del peticionario. Cuando tiene certeza de esta identidad, emite un certificado en el que

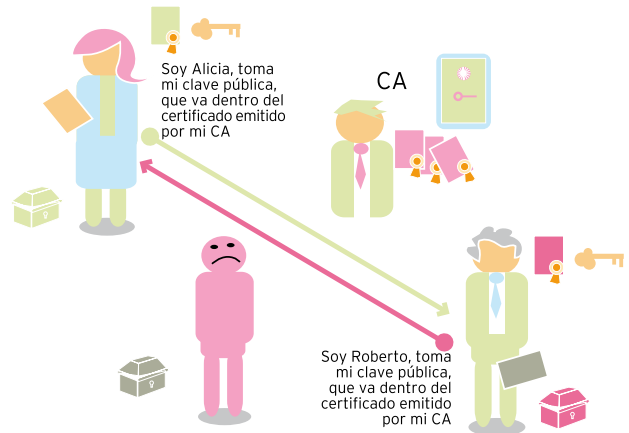


Fig. 26. Función de las Autoridades de Certificación.

Ya no es posible el ataque de "hombre en el medio" porque no puede tener acceso a la clave privada de la Autoridad de Certificación, y por tanto, no puede falsificar los certificados.

se recogen los datos de identificación e inseparablemente la clave pública del peticionario. En el certificado, todos estos datos van cifrados con la clave privada del prestador de servicios de certificación.

Dado que la clave pública del prestador de servicios de certificación es conocida por todos los interlocutores, cualquiera es capaz de extraer los datos del certificado. Sin embargo, nadie es capaz de suplantar al prestador de servicios de certificación emitiendo certificados falsos, ya que carece de su clave privada.

Una vez que Alicia y Roberto cuenten con sus respectivos certificados, ya no intercambiarán las claves a través del medio de transmisión, sino que intercambiarán sus certificados. Volviendo al símil de las cajas, el prestador de servicios de certificación comunica su clave pública a través de los periódicos (seguimos con un símil) y proporciona pruebas de que es una entidad de confianza por lo que sus certificados pueden ser considerados válidos. Utiliza su caja, cifrada con su llave privada, para proporcionar la información sobre la identidad que se certifica. Entre la información proporcionada está la clave pública asociada a la identidad del certificado.

A partir del certificado, es posible, por tanto, obtener la clave pública de nuestro interlocutor y, a partir de allí reconocer su firma o tener la posibilidad de enviarle mensajes confidenciales.

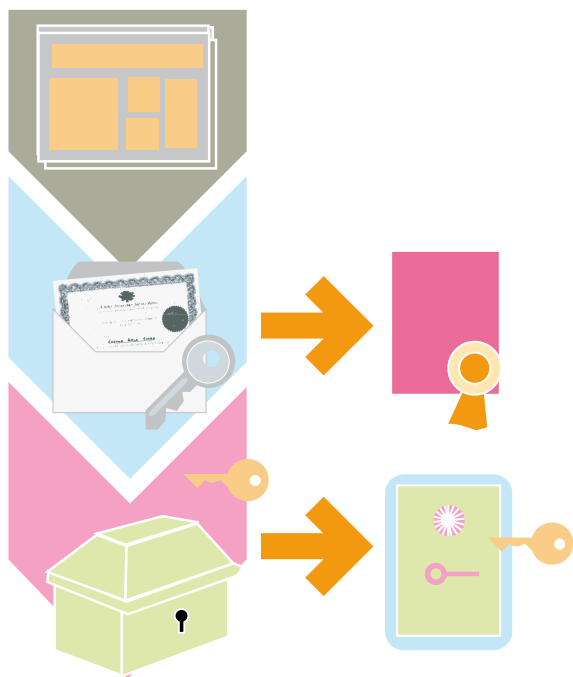


Fig 27 - Analogía de las claves gestionadas por los prestadores de servicios de certificación (PSC).

La clave pública del PSC está ampliamente disponible (como si se publicara en un periódico). Con su clave privada, se firman los certificados de los usuarios. Los certificados son documentos públicos (que incluyen su clave pública) que se vinculan con la clave privada del usuario (con el símil de la caja de mago), que éste debe custodiar diligentemente (lo que se ilustra con el símil de la caja fuerte).

Cuando un participante comunica a otro su certificado, indica el prestador de servicios de certificación utilizado. La llave pública del prestador de servicios de certificación debe ser conocida por todos y es la única que necesita ser conocida previamente. Habitualmente está incorporada al software de realización y verificación de firmas electrónicas, o es posible obtenerla a partir de sistemas de difusión públicos, tales como servidores web.

Por lo dicho hasta ahora, vemos que el prestador de servicios de certificación debe ser una entidad de confianza (trusted third party), conocida ampliamente, cuya política de certificación incluya cláusulas aceptables por los diferentes interlocutores, que permita, entre otras cosas, la Verificación de identidad, que dé información sobre uso y validez de los certificados y que realice gestión de certificados revocados (para impedir que claves privadas expuestas puedan tener vigencia) y ofrezca la lista de certificados expedidos.

Dado que en una red existe más de un prestador de servicios de certificación, la selección de los prestadores de servicios de certificación adecuados para cada uso vendrá dada por las características de su política de certificación, o por el reconocimiento de alguna de ellas por parte de entidades que aceptan sus certificados. Se están desarrollando sistemas jerárquicos en los cuales todas las autoridades de certificación que pertenezcan a una jerarquía dada puedan realizar certificaciones mutuas.

Los parámetros que definen a un prestador de servicios de certificación son su dirección de red (nombre distinguido) y su clave pública. Además es necesario especificar en su identificación: entidad emisora del certificado, departamento u organización responsable de la custodia de la clave privada, y ubicación (ciudad, país). También son valorables aspectos como identificativo fiscal o referencia registral.

Entidad de registro

Puesto que al realizar la comprobación de la identidad del usuario en la primera certificación es necesario realizar unas actividades especiales, el prestador de servicios de certificación lleva asociada una Entidad de registro.

Esta entidad de registro mantiene información sobre los aspectos relevantes del registro y sobre los procedimientos de identificación utilizados, así como la vinculación del registro con la identidad que garantiza el prestador de servicios de certificación.

Además de este tipo de entidades de registro, existen otras, que demuestran la realización en el tiempo de determinados actos electrónicos: certificaciones en presencia de un fedatario (como en el caso de contratos firmados ante notario), certificaciones de acreditación respecto a la capacidad suficiente para obrar o para representar a terceros, registro de contratos o transmisiones patrimoniales. En la normativa actual de administración electrónica se les denomina sede electrónica y uno de sus precedentes fue el sistema de anotaciones en cuenta, que se utiliza en el mercado de valores.

Algunas de estas entidades tienen actividades independientes y adicionales a las de los prestadores de servicios de certificación, que se centran en la autenticación de los intervinientes y las funciones derivadas.

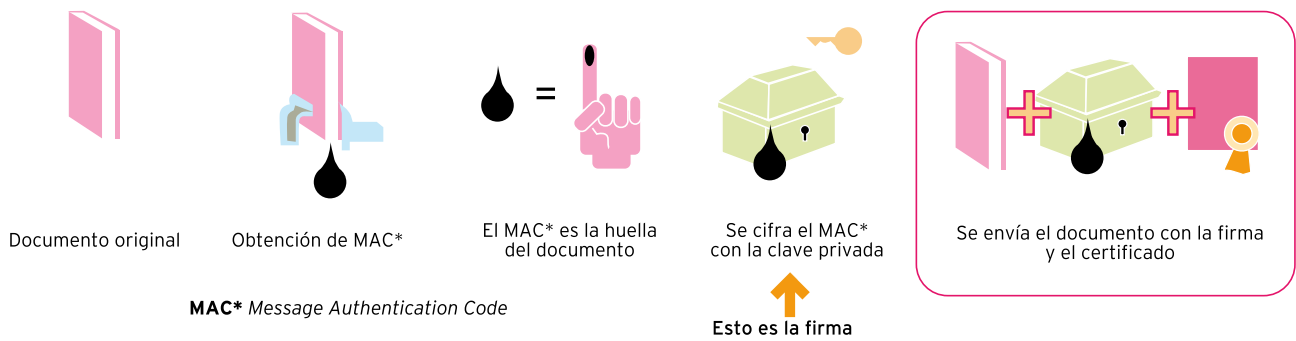


Fig. 28. Símil de firma electrónica.

Se aplica la función resumen sobre el documento (que obtiene algo semejante a la huella dactilar del documento) y se cifra con la llave privada del firmante, se envía el documento, el certificado y el resultado de la operación anterior, que es la firma electrónica. La firma electrónica es diferente para cada documento, firmado por un mismo usuario y para el mismo documento, si lo firman distintos usuarios.

El esquema completo

Con todos los elementos descritos, ya es posible tener una idea sobre la forma en que se realizan los diferentes procesos de firma, verificación,...

Realización de la firma

Partimos del documento original al que se le calcula el hash (o MAC "Message Authentication Code"), función resumen unidireccional, que lo identifica unívocamente. El resultado de aplicar esta función se cifra con la clave privada del titular del certificado (siguiendo con el símil, se introduce en la "caja de mago"). Lo que se envía al destinatario es el conjunto formado por el **documento**, el **hash (o MAC) firmado** y el **certificado**.

Comprobación de la firma

El receptor recibe el conjunto formado por el **documento**, el **hash firmado** y el **certificado**. A partir del certificado, podemos extraer la clave pública del remitente. Con dicha clave pública podemos abrir la "caja de mago" y por tanto obtener el **hash** que se calculó en origen. Dado que disponemos del documento, podemos calcular su **hash** por nuestra cuenta. Al comparar los dos "hashes", el que se calculó en origen y el que se calculó en destino, ambos deben coincidir. En caso de que no coincidan, esto quiere decir que o bien el documento o bien el "**hash firmado**" han tenido alguna incidencia en la transmisión que afecta a su contenido, y por tanto, la firma no es válida.

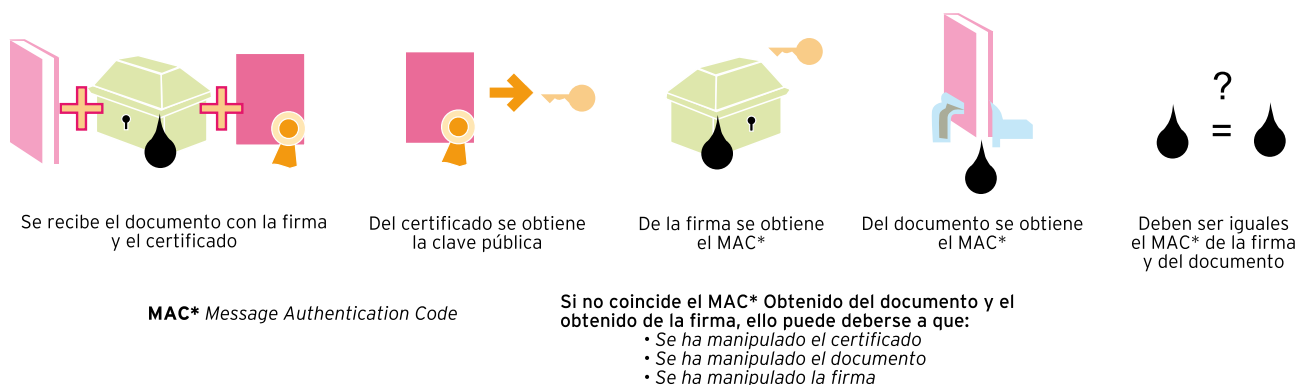


Fig. 29. Verificación de la firma electrónica.

Del certificado se obtiene la clave pública del firmante con lo que se puede descifrar la firma para obtener el resultado de la función resumen aplicada por el firmante. Además, aplicando el mismo algoritmo sobre el documento, se calcula de nuevo la función resumen. Ambos valores, el original y el obtenido en destino, deben ser iguales.

Funciones de Seguridad

Un sistema de firma electrónica permite cumplir las siguientes funciones de seguridad:

- **Integridad,**
- **Identificación del firmante (atribuibilidad),**
- **Prueba de conformidad con lo firmado (pres-tación del consentimiento),**
- **Momento de la firma**

Además existen otros principios de seguridad que igualmente se satisfacen, según las características del certificado y del protocolo empleado, como disponibilidad, auditabilidad, fiabilidad, confidencialidad, detección de mensajes faltantes en una secuencia, acuse de recibo, poder bastante para el acto y evidencia legal.

Integridad

No es posible que el contenido del mensaje sufra ninguna modificación accidental o intencionada, una vez firmado.

Identificación del firmante

Es posible saber quién es el emisor del mensaje y sus atributos principales.

Prueba de conformidad con lo firmado

El firmante está de acuerdo con el contenido del documento o se vincula con él de alguna forma (como autor, como revisor, dándose por enterado, etc).

Momento de la firma

Si la firma se lleva a cabo de forma correcta, incorporando información temporal fehaciente, es posible saber que el documento existía antes de un momento dado, que es el que se indica como momento de la firma.

Custodia de claves y dispositivos seguros de creación de firma

Un aspecto importante en un entorno de facturación electrónica que emplee certificados digitales es el referido a la custodia de la clave privada asociada a la clave pública y al certificado empleado para la firma de facturas.

Lo que comúnmente conocemos como certificado digital, consta en realidad de tres elementos importantes:

1. La clave privada: se trata de una clave generada de forma aleatoria a partir de unos algoritmos matemáticos de una determinada longitud. En la actualidad se suele emplear para claves personales el algoritmo RSA y claves de 1024 bits. Esta clave debe ser conocida y manejada únicamente por el usuario de esta.
2. La clave pública: esta clave está generada en base a la anterior, si bien resulta extremadamente complejo inferir la clave privada una vez conocida esta clave pública. El objetivo de esta clave es permitir su intercambio, por lo cual su naturaleza es pública.
3. La clave pública generada se incorpora, junto con los datos del usuario del certificado (nombre, DNI, empresa, ...) a un documento formado en base al estándar X509 v.3. Este documento es firmado por un prestador de servicios de certificación, que de esta manera certifica la autenticidad de todos los datos contenidos en él. Este documento firmado por el prestador de servicios de certificación es el certificado digital propiamente dicho.

La seguridad del sistema de firmas radica, por tanto, en la protección de la clave privada. Esta clave puede ser almacenada de diferentes formas:

1. Almacén en claro: La clave privada se almacena en el disco sin ninguna protección, salvo, en su caso, la protección habitual para ficheros sensibles.
2. Almacén en repositorios especiales: Microsoft dispone de un gestor de claves y certificados propio, el cual te permite proteger la clave privada con una contraseña. El principal problema radica en la dependencia a una plataforma y la escasa seguridad del proceso.
3. Almacén PKCS#12 / PEM: se trata de archivos contenedores de la clave privada, la clave pública y el certificado. La clave privada puede ser protegida por contraseña.
4. Almacén en tarjetas de memoria: algunas tarjetas chip de memoria permiten el almacén y recuperación de claves y certificados. Su principal ventaja es su portabilidad y su desventaja es que las operaciones criptográficas se realizan fuera de la tarjeta.
5. Almacén en tokens criptográficos: las tarjetas

criptográficas dotan de la misma portabilidad que la tarjeta de memoria con el añadido de que las operaciones criptográficas se realizan en la propia tarjeta, por lo que la clave privada nunca sale de la misma.

6. Almacén en HSM (Hardware Security Module): el hardware criptográfico otorga la misma funcionalidad que los tokens pero están optimizados para realizar procesos en batch (por lotes). Es recomendable su uso cuando se realicen muchas operaciones criptográficas y se quiera dotar al sistema de una gran seguridad. Además puede acompañarse de aceleradores criptográficos que optimicen su funcionalidad.

Para la utilización de las claves de firma se recomienda en términos absolutos el uso de algún hardware criptográfico HSM, por su mayor eficiencia (en términos de velocidad y seguridad) frente a la alternativa de almacenamiento software.



Fig. 30. El DNI electrónico es considerado un dispositivo seguro de creación de firma.

No obstante, dependerá del alcance del proyecto la decisión respecto al medio a emplear, si bien debemos tener en cuenta que la ley de firma electrónica exige la utilización de dispositivos seguros de creación de firma para la generación de firmas reconocidas.

Anexo



Anexo II. Marco jurídico de la firma y de la factura electrónica

Validez legal de la factura electrónica

La factura electrónica es plenamente legal en toda Europa. Las normas aplicables son fundamentalmente las siguientes¹

- 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.
- Directiva 2006/112/CE del Consejo, de 28 de noviembre de 2006, relativa al sistema común del impuesto sobre el valor añadido. Está aprobado el texto de la futura norma que modificará esta directiva y que deberá ser traspuesto a los ordenamientos jurídicos nacionales antes del 1 de enero de 2013.
- Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.
- Ley 58/2003, de 17 de diciembre, General Tributaria.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

¹ Puede encontrar y descargar la legislación española en el portal web del Boletín Oficial del Estado (http://www.boe.es/aeboe/consultas/bases_datos/iberlex.php), la legislación de la Unión Europea en el portal Eur-Lex (<http://eur-lex.europa.eu/es/index.htm>) y la regulación específica de los departamentos ministeriales en la sección de legislación del portal O60 (<http://legislacion.O60.es/>). También puede acceder a un repertorio legislativo, entre otras informaciones relativas a factura electrónica, en el portal web sobre factura electrónica del Gobierno de España: <http://www.facturae.es/es-ES/Documentacion/Normativa/Paginas/FacturaElectronica.aspx>

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
- Ley 53/2002, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Ley 30/2007, de 30 de octubre, de Contratos del Sector Público.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- 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.
- 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.
- Real Decreto 87/2005, de 31 de enero, por el que se modifican el Reglamento del Impuesto sobre el Valor Añadido, aprobado por Real Decreto 1624/1992, de 29 de diciembre, el Reglamento de los Impuestos Especiales, aprobado por Real Decreto 1165/1995, de 7 de julio, y el Reglamento por el que se regulan las obligaciones de facturación, aprobado por Real Decreto 1496/2003, de 28 de noviembre.
- Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto 2126/2008, de 26 de diciembre, por el que se modifican el Reglamento del Impuesto sobre el Valor Añadido, aprobado por el Real Decreto 1624/1992, de 29 de diciembre, así como el Reglamento General de

las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos, aprobado por el Real Decreto 1065/2007, de 27 de julio.

- 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.
- 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.
- 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.

Las diputaciones forales con capacidad normativa propia han publicado normativa equivalente, aplicable en territorio foral, prácticamente idéntica a la aplicable en territorio común.

Las empresas españolas tienen la obligación legal de expedir y entregar facturas o documentos sustitutos, en los casos permitidos por la ley, en relación con todas las operaciones comerciales que realicen en el desarrollo de su actividad.

Este deber legal va acompañado, en su caso, de la obligación de cumplimiento de la normativa vigente aplicable a la factura electrónica, en particular los Art.6 y 7 del Reglamento por el que se

regulan las obligaciones de facturación aprobado por el RD 1496/2003, que señala como requisitos obligatorios mínimos, que han de contener tanto las facturas que se emitan como sus copias, los siguientes datos:

- **Número de la factura y, en su caso, serie.** El uso de series diferentes añade una gran flexibilidad a las diferentes modalidades de facturación, entre las que se podrían identificar la autofacturación y la facturación por terceros.
- **Fecha de expedición.** En algunos casos esta fecha coincidirá con la de entrega del bien o de prestación de servicio, pero cuando no coincida, no puede superar el plazo previsto por la normativa.
- **Nombre y apellidos, o razón social,** tanto del obligado a expedir la factura como del destinatario de la misma.
- La factura habrá de consignar la denominación social de la forma que esté registrada, es decir, para su validez, la factura deberá contener el nombre **completo** registrado en la escritura de constitución inscrita en el Registro Mercantil, no revistiendo validez los nombres comerciales ni las posibles abreviaturas, salvo las que debido a limitaciones técnicas no permitan hacer constar el nombre completo y sean de común uso aceptadas (tales como S.A., S.L., SC, etc.).
- **Número de Identificación Fiscal (NIF).** En consideración a la Directiva 2001/115/CE las empresas antepondrán las letras ES al CIF otorgado por la Administración Tributaria (en base al estándar internacional ISO-3166 alfa2, que sirve para identificar al Estado miembro que haya atribuido el Número de identificación fiscal).
- **Domicilio fiscal** de los obligados tributarios, tanto emisor como destinatario. No tiene por qué coincidir con el lugar en el que se hace la entrega de bienes y servicios. El lugar en el que se hace la entrega puede figurar en la factura, pero no es un requisito esencial para su validez.
- **Descripción de operaciones.** Señalando, de forma destacada, la **fecha** de entrega del bien o de la prestación del servicio.
- En el supuesto de que para dar cumplimiento a este requisito se haga uso de la información contenida en albaranes, este hecho habrá de ser mencionado en la respectiva factura, haciendo referencia de manera inequívoca al correspondiente albarán, el cual deberá conservarse debidamente anexo a la factura. Esto es así debido a la calificación del albarán

como soporte documental de las operaciones realizadas, es decir, tendrá la consideración de parte integrante de la factura a la que se adjunte y estará sometido a las mismas obligaciones de conservación que la referida factura.

- Si el destinatario de la factura fuera empresario o profesional, podrán agruparse en una sola factura todas las operaciones llevadas a cabo en distintas fechas de un mes natural.
- Igualmente, podrá realizarse la agrupación señalada en una única factura las distintas operaciones realizadas con el mismo proveedor cuando el obligado a la expedición sea el sujeto pasivo del impuesto (IVA).
- Tipo o **tipos impositivos** aplicables a las operaciones. O mención expresa de la causa de exención o no sujeción, en su caso.
- La **cuota** repercutida.

Cabe recordar que la nueva normativa europea será más flexible a la hora de permitir diferentes mecanismos que garanticen la autenticidad e integridad de la factura electrónica.

Aspectos legales de la firma electrónica

Una norma que afecta a la implementación de la factura electrónica es la Ley 59/2003 de firma electrónica en la que se recoge la equiparación de la firma electrónica reconocida (*qualified signature*, en inglés) a la manuscrita y establece que no puede negarse el reconocimiento legal de cualquier firma electrónica, incluso de las modalidades simple o avanzada, por el hecho de presentarse en formato electrónico. Esta Ley constituye la transposición de la Directiva 1999/93,

Las variantes técnicas de realización de firma electrónica son muy amplias. En la Directiva 2006/112 que regula la factura electrónica a nivel europeo, se exige cuando se emplea firma electrónica, que ésta sea avanzada pudiendo exigir los países miembros el uso de firma reconocida (*qualified signature*, en inglés), lo que es el caso de España. El nuevo texto que modificará la directiva contempla la firma electrónica avanzada en el sentido del punto 2 del artículo 2 de la 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, basada en un certificado reconocido y creada mediante un dispositivo seguro de creación de firma, en el sentido de los puntos 6 y 10 de

la Directiva 1999/93/CE.

En la realización de la factura electrónica, la forma más sencilla de dotar de validez jurídica al documento electrónico que la contiene, consiste en incorporarle una firma electrónica. El artículo 18 del Real Decreto 1496/2003 establece expresamente que será válida una firma electrónica **avanzada** de acuerdo con lo dispuesto en el artículo 2.2 de la **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, **basada en un certificado reconocido** y creada mediante un **dispositivo seguro de creación de firmas**, de acuerdo con lo dispuesto en los apartados 6 y 10 del artículo 2 de la mencionada Directiva.

Es decir, cualquier certificado reconocido (o cualificado si se utiliza la traducción directa de la Directiva) es válido. La propia cualidad del certificado se establece en normas técnicas que emanan de la Directiva. En particular se indica que este tipo de certificados se expide a **personas físicas**.

El certificado reconocido otorga a la firma el nivel mayor de valor jurídico en la jerarquía establecida por la Ley 59/2003, de Firma Electrónica.

La **firma electrónica (simple)** es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante (de los datos a los que se asocia).

La **firma electrónica avanzada** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control. Es decir, que está llevada a cabo con criptografía de clave pública y con el respaldo de un certificado electrónico.

La **firma electrónica reconocida** es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Frecuentemente a la firma electrónica reconocida

se la denomina también cualificada, a partir de la definición de certificado cualificado de la directiva que acabó traducéndose como “reconocido”.

Como ejemplo, podemos indicar que una firma gráfica digitalizada, incorporada a un documento, puede ser considerada firma electrónica **simple**. También tiene la consideración de firma electrónica simple la identificación de un usuario mediante identificativo de usuario y clave (o password), o mediante un PIN, como en el caso de las tarjetas de crédito.

Una variante de firma electrónica **avanzada** es la que emplea criptografía de clave pública, y un código de verificación del contenido del documento, como por ejemplo la que se utiliza en el correo electrónico. En este caso, aunque el certificado utilizado no se haya obtenido tras un proceso riguroso de verificación de identidad, se siguen cumpliendo los supuestos básicos que exige la norma. El uso de sistemas criptográficos como PGP también cumple estos requisitos.

Cuando la identidad se comprueba de forma rigurosa, se cumple uno de los requisitos formales del **certificado reconocido**, aunque no es el único. Por eso, en ocasiones pueden establecerse subniveles de firma electrónica **avanzada** según el rigor del prestador de servicios de certificación (o de sus entidades de inscripción - autoridades de registro) al expedir el certificado (i.- identidad alegada, ii.- dirección de e-mail verificada, iii.- datos verificados indirectamente por vinculación con otros, iv.- datos verificados indirectamente por relación preexistente, v.- aportación de documentos y evidencias de forma no presencial).

Cuando se realiza verificación presencial de los datos del firmante y se cumplen otros requisitos formales, el prestador de servicios de certificación está en disposición de emitir certificados reconocidos, que son los que, junto con los dispositivos seguros de creación de firma, dan lugar a la firma electrónica **reconocida**.

La regla general es utilizar en lo posible **certificados personales** (para que sean aceptados en toda Europa).

De entre estos, deben preferirse aquellos que en su codificación incluyan una referencia a la empresa en la que la persona presta sus servicios. Mejor todavía es emplear certificados de representante que se hayan obtenido en base a un poder notarial

que restrinja su uso a firma de facturas.

La Ley 59/2003, de 19 de diciembre, de firma electrónica regula de manera expresa los certificados electrónicos de personas jurídicas en su artículo 7.

En el tráfico jurídico, aunque a través de una ficción, se reconoce personalidad jurídica y capacidad de obrar a las personas jurídicas, el ejercicio de tales potestades sólo puede ser efectivo mediante la intervención de una persona física que actúa en representación de la entidad, según se indica en el artículo 35 y siguientes del Código Civil.

Pero la Ley de firma electrónica introduce una novedad, la posibilidad de que las personas jurídicas firmen por sí mismas quedando de esta forma vinculadas en sus operaciones realizadas mediante el uso de medios telemáticos.

Para que ello sea posible y revista validez, es necesario que los datos de creación de firma sean custodiados por la persona física solicitante, cuyos datos van insertos en el certificado electrónico, que asume las responsabilidades previstas en la ley.

La intervención de los representantes de las personas jurídicas es un claro ejemplo de la llamada representación necesaria. La misma deriva de la celebración del otorgamiento de un documento público, el cual reconoce a un sujeto, persona física, determinado como representante legal de una persona jurídica determinada.

Pues bien, la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, regula los certificados de representantes (artículos 11.4, 13.3 y 23.2), cuyo contenido deberá tener mención expresa del documento público acreditativo de las facultades del firmante.

El régimen jurídico aplicable a este tipo de certificados es análogo al señalado para la representación propiamente dicha por la legislación común.

Los certificados de representante son idóneos para el uso y desarrollo de sistemas de facturación electrónica.

La Orden EHA/962/2007 aclara que cualquier otra firma electrónica avanzada, basada en un certificado reconocido (de cualquier prestador de

servicios de certificación comunitario, con arreglo a su normativa nacional, derivada de la Directiva 1999/93) y generada mediante un dispositivo seguro de firma (lo que el artículo 3.3 de la Ley 59/2003, de firma electrónica, denomina firma electrónica reconocida) es plenamente válida.

En virtud de la **Orden HAC/1181/2003** son válidos los certificados recogidos en portal web de la Agencia Estatal de Administración Tributaria (<http://www.agenciatributaria.es>), donde se pueden encontrar las entidades emisoras de certificados electrónicos (http://www.agenciatributaria.es/wps/portal/DetalleContenido?&content=c60501ae9dc89010VgnVCM1000004ef01e0aRCRD&channel=6c1ce5e17736e110VgnVCM1000004ef01e0a___&ver=L&site=56d8237c0bc1ff00VgnVCM100000d7005a80___&idioma=es_ES).

A partir del 20 de marzo de 2004, con la entrada en vigor la Ley 59/2003 de Firma Electrónica, corresponde al Ministerio de Industria, Turismo y Comercio, el censo de prestadores de servicios de certificación. El listado se obtiene buscando en el portal web del Ministerio de Industria, Turismo y Comercio (www.mityc.es), donde se pueden encontrar los prestadores de servicios de certifica-

ción de firma electrónica" (<http://www.mityc.es/dgdsi/es-ES/Servicios/FirmaElectronica/Paginas/Prestadores.aspx>).

Además, es válido cualquier certificado que esté codificado con la indicación de que es cualificado según las normas **TS 101 862** y **RFC 3739** (perfil de certificado reconocido), lo que presupone que el PSC cumple las siguientes normas:

- **TS 101 456.** Requisitos de política para PSC que expiden certificados reconocidos.
- **TS 102 042.** Requisitos de política para PSC que expiden certificados de clave pública.

Es decir, por referencia expresa del Real Decreto 1496/2003, y el artículo 4 de la Orden EHA 962/2007 son adecuados los certificados expedidos por cualquier prestador que se ajuste al marco normativo que se deriva de la **Directiva 1999/93/CE**.

En función del artículo 11 de esta Directiva, es posible identificar los PSC que operan en Europa buscando en el portal web de la Comisión Europea en la página de "Notification procedure Article 11 of Directive 1999/93/CE" (http://ec.europa.eu/information_society/policy/esignature/eu_legislation/notification/index_en.htm).

Anexo



Anexo III. Enlaces de interés

- Portal de factura electrónica del Gobierno de España (Ministerio de Economía y Hacienda, y Ministerio de Industria, Turismo y Comercio):
<http://www.facturae.es/>
- Portal de firma electrónica del Ministerio de Industria, Turismo y Comercio:
<http://www.mityc.es/dgdsi/es-ES/Servicios/FirmaElectronica/>
- Portal del DNI electrónico del Ministerio del Interior:
<http://www.dnielectronico.es>
- Información sobre el formato UBL en OASIS:
<http://www.oasis-open.org/committees/ubl/>
- Información sobre UN/CEFACT:
<http://www.unece.org/cefact/>
- Información sobre las especificaciones de CEN BII (Business Interoperability Interfaces for Public procurement in Europe):
<http://spec.cenbii.eu/>
http://www.cen.eu/CEN/sectors/sectors/iss/activity/Pages/ws_bii.aspx
- Información sobre CEN Workshop on eInvoicing:
http://www.cen.eu/CEN/sectors/sectors/iss/activity/Pages/einvoicing_2.aspx
- Portal con información sobre los sistemas de facturación en Europa desarrollado por CEN/CENELEC:
<http://www.e-invoice-gateway.net/>
- Información sobre factura electrónica en el Portal de la Comisión Europea:
http://ec.europa.eu/internal_market/payments/einvoicing/index_en.htm