FACTURA electrónica

Economía Sostenible

GOBIERNO DE ESPAÑA MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

plan avanza 2

asimelec ASOCIACIÓN MULTISECTORIAL DE EMPRESAS DE TECNOLOGÍAS DE LA INFORMACIÓN, COMUNICACIONES Y ELECTRÓNICA

Electronic invoicing

Version 2010

FACTURA
electrónica

www.planavanza.es

www.mityc.es

www.red.es

www.asimelec.es

Publication by:

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

© ASIMELEC
Orense nº 62, 28020, Madrid.

Texts: Julián Inza

Coordination: red.es

Image and Design: Virginia Zabala

Layout and production: Scan96, s.l.
and Leaders Comunicación

Pictures: age FOTOSTOCK

Economía
Sostenible

GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

plan avanza2

asimelec
ASOCIACIÓN MULTISECTORIAL DE EMPRESAS DE TECNOLOGÍAS DE LA
INFORMACIÓN, COMUNICACIONES Y ELECTRÓNICA

Table of Contents

Introduction

This is the second important review of the electronic invoicing guide, which was produced in 2006 as an ASIMELEC and Red.es initiative as the first in the collection of the Red.es Plan Avanza Guides

The first review was published in early 2008, including the most important of the many new developments that took place in 2007.

Having achieved the initial goals of laying the foundations for understanding electronic invoicing, and given the international setting in which interoperability is starting to take on greater importance, this second version will simplify some of the aspects addressed in previous editions, highlighting best practices that have already been consolidated.

Due to the simplification of the document, information on EDI (Electronic Data Interchange) systems is not included on this occasion, but anyone interested in this may refer to previous versions, which are available online. As of today, EDI is still the system of choice in environments such as commercial retail and the automotive industry.

The manual is mainly aimed at the Spanish market, and describes the electronic invoice management system most commonly-used in Spain. The electronic signature has become very widely used in Spanish electronic invoicing systems, and for this reason many of the points in this document cover "good practices" that could be useful at a European level in cases where the parties prefer to use this security measure. Therefore, this third version has been translated into English.

The previous editions were available in printed form and as a PDF. More than 10,000 printed copies were distributed, and more than 500,000 PDF versions of it were downloaded. Meanwhile, the technological advances implemented by companies and their suppliers have had a considerable impact on the adoption of electronic invoicing in Spain, which is currently one of the strongest countries in Europe in terms of penetration of this technology, with a large number of solutions of all kinds, from cost-free solutions for small and medium-sized companies, to sophisticated ones for large companies and public bodies.

This edition has also been affected by two significant events: firstly, the publication of the Final Report by the European Commission's Expert Group on Electronic Invoicing, which identified some barriers, the elimination of which may boost the adoption of electronic invoicing in Europe, and secondly, during the Spanish Presidency of the EU, the adoption on 16 March 2010 of the agreed text on the reform of Directive 112/2006, containing the main proposals issued by the Expert Group, and which is expected to be transposed into national legislations by 1 January, 2013.

With the obligatory establishment of electronic invoicing for the public sector enshrined in Law 30/2007 and Law 56/2007, there is no doubt that the level of adoption will be more considerable still in years to come.

01.

Chapter 1. The ABC of electronic invoicing

What's an invoice

An invoice is a document certifying the delivery of a product or the provision of a service, showing the date of accrual and the amount payable in consideration for the product or service provided.

The invoice contains the issuer's and recipient's details, a description of the products and services provided, unit prices, total prices, discounts and taxes.

It is considered to be fiscal proof of delivery of a product or provision of a service affecting the tax-paying issuer (the seller) and the tax-paying recipient (the purchaser). The original should be kept by the recipient. Generally, the issuer of the invoice keeps a copy or the original (database) recording the issuance, in which case the recipient does not have to keep invoice copies.

A properly drawn-up invoice is the only tax receipt that gives the recipient the right to claim a tax refund (VAT). This is not the case for documents that substitute invoices, such as receipts or tickets.

In Europe, invoicing rules are governed by Directive 2006/112/CE, with amendments to be included in the next version already having been agreed upon. These amendments are intended to harmonize legal requirements throughout the entire EU in order to achieve a higher level of interoperability, which will encourage electronic invoicing to take off and become more deeply rooted.

Invoices can be:

- **Standard invoices:** stating the supply transaction.
- **Amendment invoices:** showing corrections to one or more previous invoices, or product returns, packaging and packing or volume extra fees.
- **Summary invoices:** showing a group of invoices for a specific period.

There are also the following variations:

- **Pro-forma:** an invoice which states an offer, showing the exact form that the invoice will take after the product has been supplied. It has no value for accounting purposes or as a receipt.
- **Copy:** states the transaction for the issuer, with the same details as the original invoice. It should be marked as a copy so that it can be distinguished from the original.
- **Duplicate:** stating the transaction for the recipient, in the event of loss of the original. It is issued by the same issuer who issued the original and has the same details as the original. It should be marked as a duplicate so that it can be distinguished from the original, especially in the event that the original is found.

It is interesting to note that traditional credit notes are not provided for in the regulations, even though their function can be covered by amendment invoices. Both documents can be identified provided that they indicate that they are amendment invoices and, optionally, for information purposes, the credit note, and the quantities on them are stated correctly.

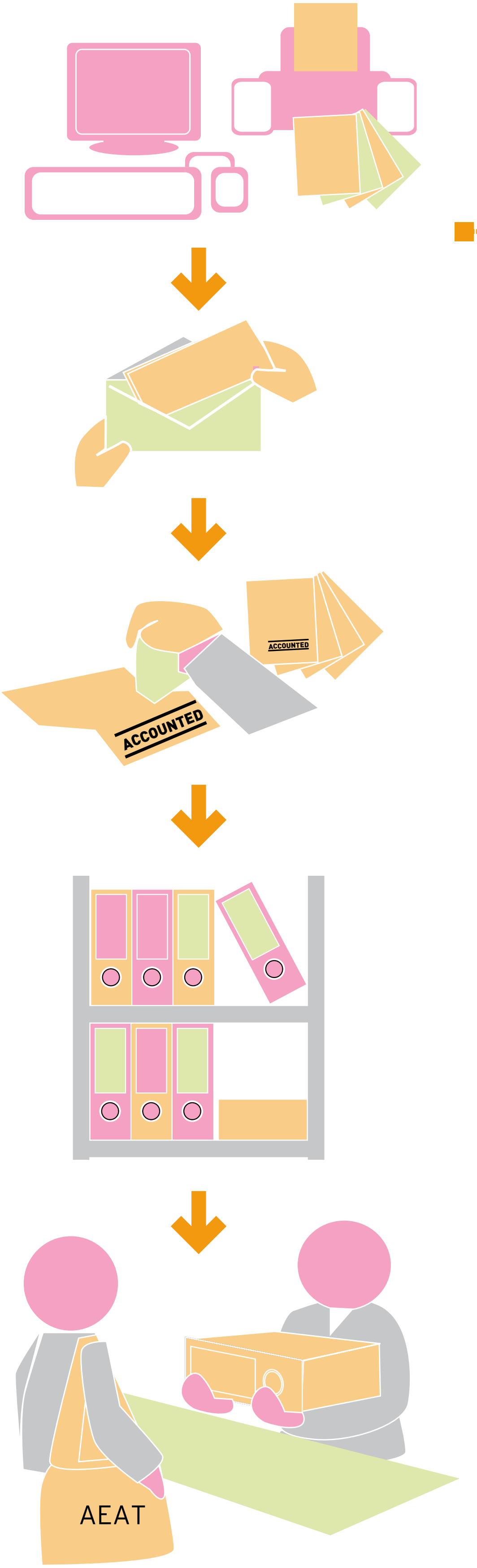


Fig 1. General traditional paper-based invoicing procedure.

The invoice can be printed from computer files, folded, put into an envelope and stamped. It is sent by postal mail or courier, and is received by the recipient, who carries out the account reconciliation, accounting and payment processes. It is then filed and made available for auditing or tax inspections, which are based on the value of the document in paper format.

> *"A properly drawn-up invoice is the only tax receipt that gives the recipient the right to claim a tax refund (VAT)".*

What is the electronic invoice?

Electronic invoicing is the transfer of invoices or equivalent documents from issuer to recipient electronically (computer files) and telematically (from one computer to the other), these being electronically signed using recognized (or qualified) certificates, which have the same legal validity as paper-based invoices.

A specific definition can be found in Article 1 of Law 56/2007: "The electronic invoice is an electronic document which fulfils all the legal and enforceable requirements for invoicing, and which also guarantees the authenticity of its origin and the integrity of its contents".

Even though there are several mechanisms for guaranteeing the authenticity of origin, content integrity and legibility of both paper and electronic invoices from the moment of issue to the end of the invoice retention period, the electronic signature is the most commonly-used form of electronic invoicing in Spain.

In relation to this, the agreed text for the future amendment of Article 233 of Directive 112/2006, states that:

1. The authenticity of origin, content integrity and legibility of an invoice, whether in paper or in electronic format, shall be ensured from the moment it is issued until the end of the invoice-retention period. Each taxable person or company shall determine how to ensure the authenticity of the invoice's origin, content integrity and legibility. This can be done by using management controls that create a reliable audit trail between the invoice and supply of goods or services.

"Authenticity of the origin" shall mean assurance of the identity of the supplier or the issuer of the invoice. "Integrity of content" shall mean that the content required has not been altered, in accordance with the provisions of this Directive.

2. Aside from the type of business controls described in the second subparagraph of section 1, the following are examples of technologies that ensure the authenticity of origin and content integrity of an electronic invoice:

- *advanced electronic signature in relation to point (2) of Article 2 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999, on a Community framework for electronic signatures, which are based on a qualified certificate and which are created by a secure signature creation device, within the sense of points (6) and (10) of Article 2 of Directive 1999/93/EC.*
- *electronic data interchange (EDI), as defined in Article 2 of Commission Recommendation 1994/820/EC of 19 October 1994, relating to the legal aspects regarding electronic data interchange, if the agreement on the exchange provides for the use of procedures that guarantee authenticity of origin and integrity of data.*

This means that, following the period for transposition of the Directive (1 January 2013), Spanish legislation will provide for the possibility of electronic invoices being exchanged between companies without any official requirement, although the requirements currently in place in cases where the recipient is a public administration will probably be maintained.

In Spain, the adoption of electronic invoicing as a widespread mechanism to guarantee the authenticity and integrity of electronic invoicing has been boosted by the spread of the electronic DNI national ID card (with more than 15 million units issued), and the broad availability of electronic certificates from numerous certification service providers, as well as by the availability of free software that makes it possible to electronically generate and sign the electronic invoices sent, as well as to verify them if they are being received.

The invoicing process is crucial for every company, and culminates in the purchase-sale process. Although the relationship between companies has traditionally been based on the exchange of paper-based documents, this entails using large amounts of resources and performing many tasks manually. In a context where the Internet is quickly becoming universal, more and more companies are deciding to streamline their processes in order to improve efficiency and reduce costs.

This is why progress has been made on the adoption of electronic invoicing, regulated by the Invoicing Regulation published in Royal Decree 1496/2003, as amended by Royal Decree 87/2005.

The Electronic Invoicing Regulation was completed with the publication of Order EHA/962/2007, of 10 April, which developed certain provisions on telematic invoicing and electronic invoice retention, contained in Royal Decree 1496/2003, of 28 November, which approved the regulations governing invoicing obligations.

The terms electronic invoice, telematic invoice and digital invoice are interchangeable, even though the name most commonly used in the regulation is electronically-transferred invoice (remisión electrónica) or transferred via electronic means (remisión por medios electrónicos). Usually, the term digital invoice (factura digital) is used for the type of electronic invoice using a digital signature to guarantee the authenticity and the integrity of the invoice.

Electronic invoices can be issued in different formats (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg or txt, among others), provided that the relevant legally-required contents are included and the authenticity and integrity requirements are met, for example by incorporating the qualified electronic signature.

However, following the publication of Order **PRE/2971/2007**, which established the obligatory use of the XML **facturae** format in cases where the recipient is a central government administration or public body, this format has also been frequently adopted in Spain for invoicing between private companies.

Meanwhile, Spanish regional administrations with active policies to promote electronic invoicing are also adopting this "**facturae**" electronic invoice format. These are some of the Autonomous Regions that have adopted the facturae format:

- Catalonia (e-Fact)
- Basque Country
- Valencia (Ge-Factura)
- La Rioja
- Castilla-La Mancha

Throughout this document, focus is placed primarily on the kind of electronic invoicing that uses the electronic signature according to the facturae format, given that this has become consolidated as best practice in Spain for implementing electronic invoicing.

“The electronic invoice is an electronic document which fulfils the legal and enforceable requirements for invoices, and which also ensures the authenticity of their origin and the integrity of their content”.

Electronic invoicing as part of the global accounting process

Electronic invoicing should not be considered as an isolated process, but rather as an integral element within an entity’s financial management and flow of purchases and sales.

It is just one of the stages in a company’s purchase and sale management process, with the invoice often being one of the final results following on from the exchange of budget estimates, purchase requests, approvals, delivery notes, accounting entries and stock management processes.

Good electronic management at all stages and prior documentation will considerably facilitate implementation of the electronic invoicing system and will lead to an exponential increase in its advantages.

However, incorporating electronic invoicing within a company’s management system will usually entail a review of invoice issuing and reception processes, and will affect more management areas than may at first be expected.

How an electronic invoice works

Generally speaking, the electronic invoicing process comprises two basic and differentiated processes in all invoicing management systems – the issuance and receipt of invoices.

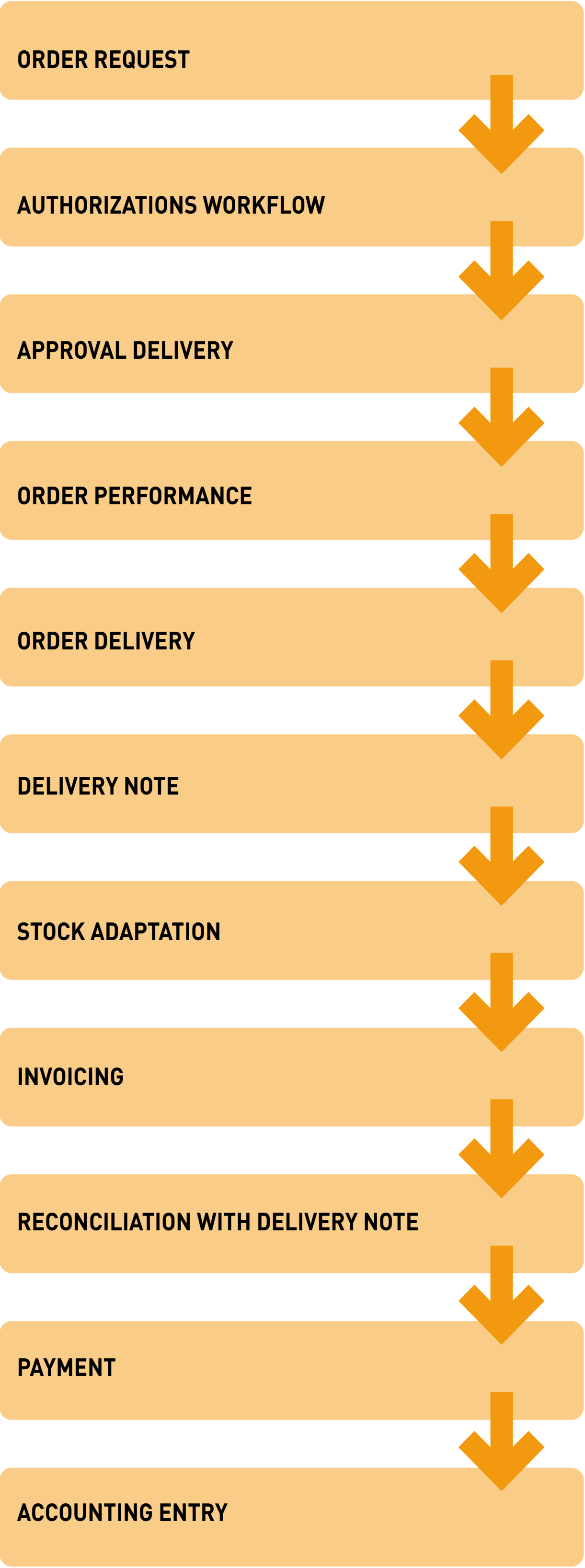


Fig. 2. Purchase-related document workflow

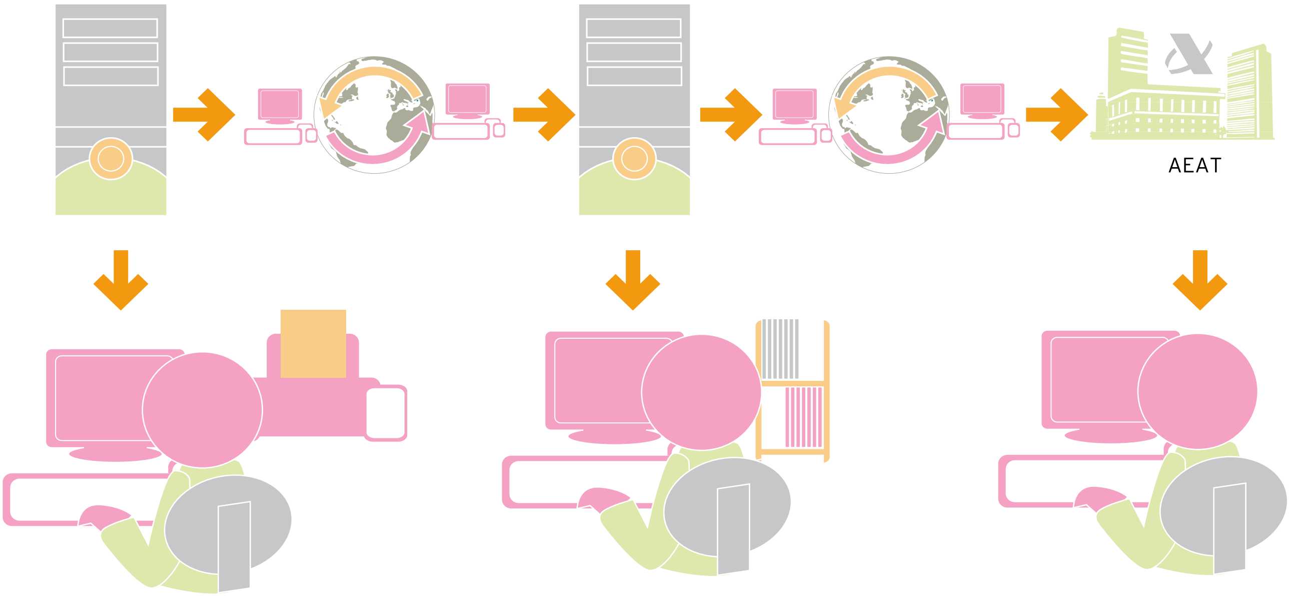


Fig. 3. Simplified electronic invoicing process.

Invoicing is managed on a computer and transferred to another computer electronically. This computer stores the invoice electronically and, where necessary, submits it to the Tax Agency electronically. Users carry out the whole operation from their computers.

At the issuance stage, the issuer, with the recipient's approval, transfers the electronic invoice to the recipient telematically (often including use of the electronic signature), and keeps a copy or the original (database). If retained in the database, it is not necessary to keep copies of the electronically-signed documents.

The recipient receives the invoice in digital format and keeps it in this format for future reference or printing, if necessary. Given that the invoice is an electronically signed document, the recipient should keep the information that verifies the validity of the electronic signature or that will enable this validity to be proved after a certain length of time.

This means it is no longer necessary to print the invoice in order for it to be legally and fiscally valid, and the entire process (issuance, distribution and retention) can be directly carried out using the electronic file generated by the issuer.

Advantages, benefits and savings with electronic invoicing

Electronic invoicing has great benefits for the companies that use it, both as issuers and recipients. There are many reasons for using electronic invoicing, ranging from the purely economic to the environmental.

The following are some of the most important advantages:

- **Cost saving:** both for the issuer and for the recipient, as a result of eliminating paper, the reduced prices of electronic communication (in comparison with traditional postage), elimination of postal costs and expenses incurred in manual data entry, etc.

- **Efficiency improvement:** releasing human resources from administrative tasks makes it possible for these to be focused on productive aspects of the business.

- **Integration with ERPs:** for the issuer, the electronic process they are already carrying out continues. The invoice is issued and sent with just one click from the ERP. For the recipient, the data can be automatically introduced into their applications.

- **Cash management optimization:** automation makes it possible to balance accounting entries and to compare documents (delivery note/invoice), while also minimizing human error.

- **Real-time access to information:** makes it possible to verify the status of the invoice and all its related information (errors, rectifications, payment collections, delivery of goods, delivery notes, etc.), accurately and on a real-time basis.

- **Reduction in handling times:** the immediacy in the dispatch and delivery of electronic invoices reduces admin to an absolute minimum and makes it possible to resolve any discrepancies in a short time.

- **Quick decision-making:** the immediacy of communications makes it possible to take decisions, such as on financing needs, in a shorter period of time.

- **Automated administration and accounting:** the integration of business systems means that all data entry and accounting operations require a much lesser degree of human involvement.

- **Monitoring of erroneous actions:** through alert systems that detect discrepancies between accounting and invoicing operations or the application of erroneous rates.

- **Efficient use of financial resources:** the adoption of electronic invoicing facilitates access to means of financing such as factoring or confirming.

- **Better use of employees' skills,** enabling them to devote their time to tasks with greater added value for the company.

- **Reduction in disputes arising from the handling** of invoices between issuer and recipient.

- **Improvement in problem resolution,** reducing them and resolving them more quickly.

- **Reduction of payment collection** periods, given that the payment of invoices is achieved more quickly.

- **Improvements in the negotiation of payment deadlines,** given that the certainty in the application of payment deadlines not affected by delays arising from problems allows a certain margin for additional manoeuvre.

- **Improvement of the company's commercial relationship** and image, as a result of the foregoing effects.

Performance of obligations, when electronic invoicing is required in tender proceedings.
In short, a higher quality in the service is achieved, resulting in higher business competitiveness.

"There are many reasons for adopting electronic invoicing, ranging from the purely economic to the environmental".

Some figures

One of the main advantages of electronic invoicing is the economic savings for companies that use it.

In fact, eliminating the costs associated with using paper, ink and printing is a great advantage. The following charts show the savings to be made by using electronic invoicing. These figures are ASIMELEC estimates.

Issue

PAPER	Cost/ Unit	ELECTRONIC INVOICING	Cost/ Unit
Printing	0,12	Project cost allocation	0,05
Sending (envelope, stamp)	2,60	External services (traffic, timestamping)	0,15
Manual processing	0,35	Management (Administration Dept.)	0,02
TOTAL	3,07	TOTAL:	0,22

Saving per invoice: 2,85

Receiving

PAPER	Cost/ Unit	ELECTRONIC INVOICING	Cost/ Unit
Reception and manipulation	0,07	Project cost allocation	0,05
Data entry	0,15	Invoice and e-signature verification	0,13
Manual processing	1,68	Management (Administration Dept.)	0,05
Archiving (4 years)	1,67	Archiving (4 years)	0,48
TOTAL	3,57	TOTAL	0,71

Saving per invoice: 2,86

There are additional savings to be made as a result of subsequent processes – for example in the case of invoices that do not turn up or are hard to find because they have not been properly filed, during audits or inspections. Such problems do not arise with electronic documents.

How much is the cost of electronic invoicing?

It is hard to estimate the price of implementing an electronic invoicing solution in general terms, although it can be taken that, the more complex the platform and the greater its level of automation, the greater the implementation costs will be, while bigger savings will also be achieved with every invoice issued or received.

Based on the foregoing, the cost of electronic invoicing can be considered to be virtually nil if use is made of elements already existing in the company, such as office suite tools that permit the use of electronic signatures, digital certificates used in other business processes, or the electronic DNI (national ID card), and e-mail. Simple, cost-free electronic invoicing applications are also available for small and medium-sized companies and independent professionals.

Meanwhile, creating a specific environment for electronic invoicing, with specific developments and integration, will require a longer time period before a return can be seen on the investment, which will be recovered over the medium/long term.

As a guide, some easy-to-implement systems, such as web-based applications for issuing invoices, can cost about 30 euros per month. On some occasions, the providers of these solutions may set pricing systems based on the number of invoices issued, ranging from 10 to 20 cents per invoice. These systems are appropriate for small and medium-sized companies, while large companies are governed by other parameters.

Although it is rarely mentioned, one of the costs involved in implementing electronic invoicing relates to adapting to the new way of doing things, and the need to retain both the previous paper-based system and the new electronic one for a certain period of time.

> *"The more complex the platform and the greater its level of automation, the higher the implementation costs will be, while bigger savings will also be achieved with every invoice issued or received".*

02.

Chapter 2. Working easily with the electronic invoice

What do I need to implement electronic invoice?

The requirements largely depend on the scope of the project, although there are always certain basic elements affecting the issuer or the recipient.

When a project is designed, both the invoicing volumes and their distribution between the parties are important, so it is advisable to start implementation with those companies with which it will be possible to make the greatest savings, or where adopting the system will be easiest.

More simply put, the basic requirement of the issuer is to **sign the invoice electronically** (a requirement which may be provided by an external service), while the recipient's requirement is to check the invoice and keep it in its original format (which can also be carried out by an external service).

In one of the simplest variations, the issuer of the invoice can sign an e-mail and send it with the invoice details, which only requires a key and a qualified electronic certificate issued by a certification service provider that complies with the provisions of Directive **1999/93/ EC** on electronic signatures (Law 59/2003, for Spanish providers).

There are cost-free solutions, such as 'Gestión de facturación electrónica.1.0', available in the download section in the website http://www.facturae.es

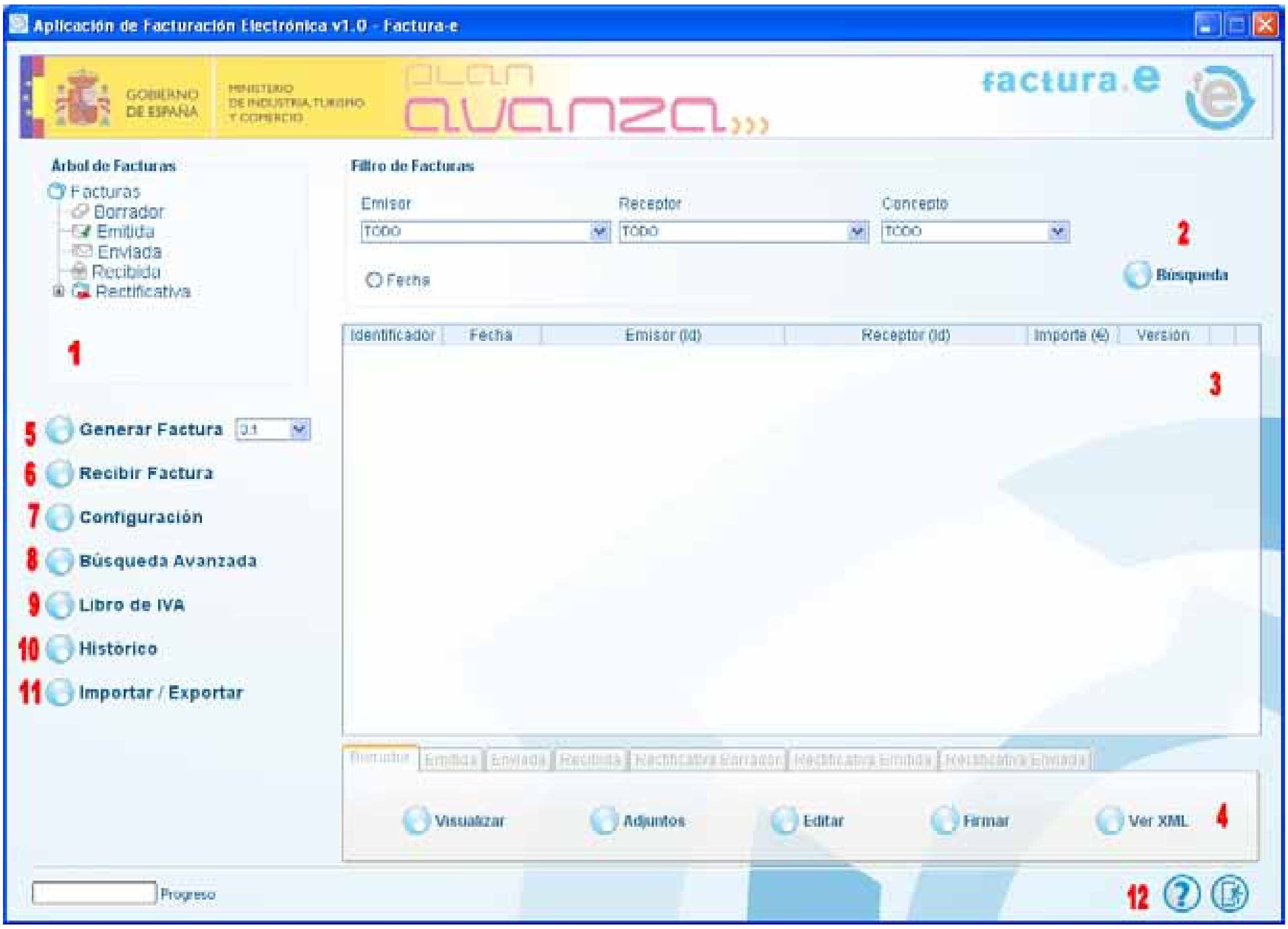
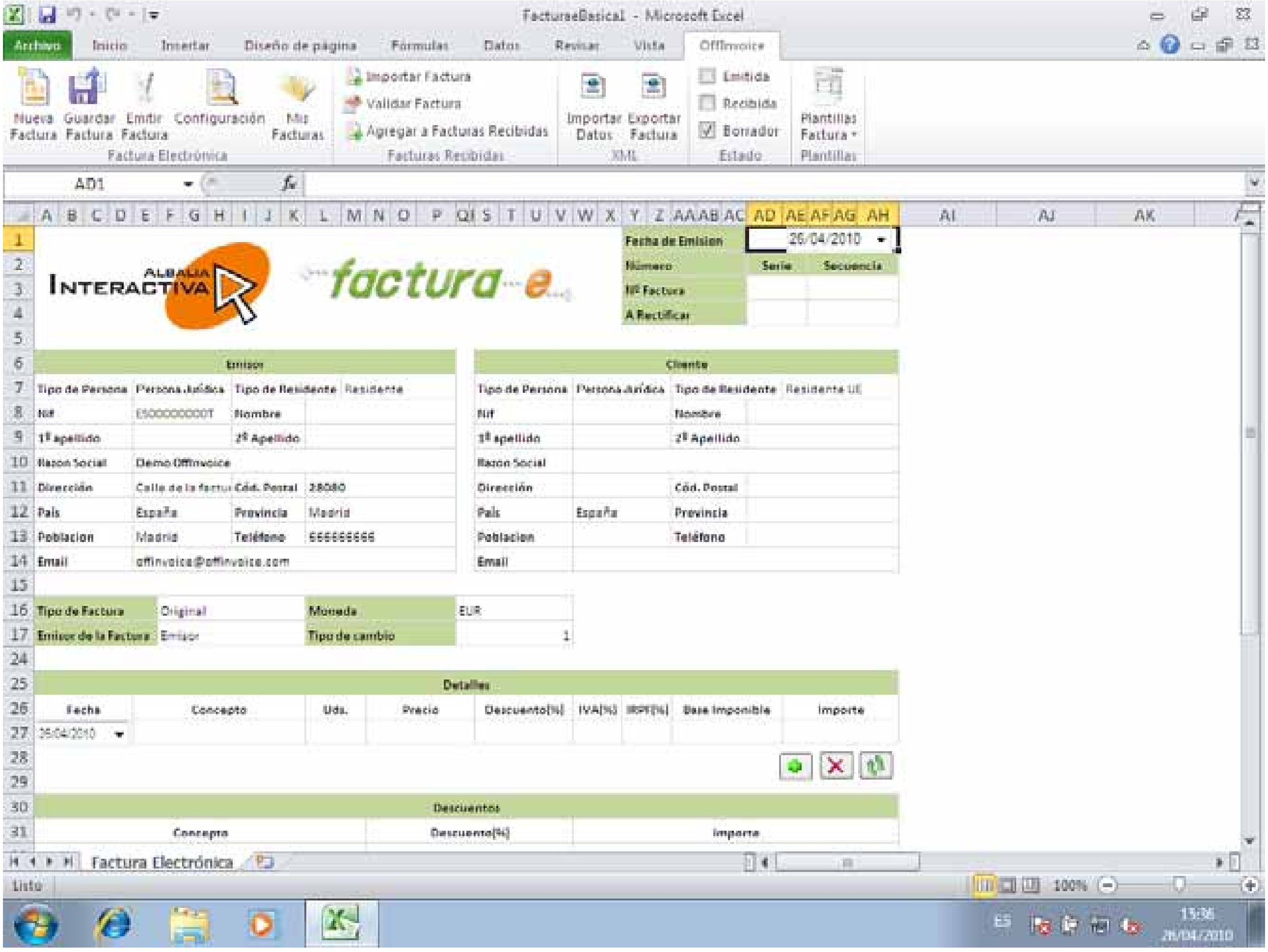


Fig. 4. Electronic invoicing management 1.0

This Java-based programme makes it possible to manage invoices in XML **facturae 3.0 and 3.1.** formats and to use **XAdES-EPES** electronic signatures (in line with standard TS 101 903)

The **OffInvoice** extension is also available, free of charge, downloadable from Codeflex: http://offinvoice.codeplex.com, which makes it possible to process electronic invoices using **Word 2010 or Excel 2010**, in Windows 7 operating systems.



Fecha de Emision	26/04/2010	
Número	Serie	Secuencia
Nº Factura		
A Rectificar		

Emisor			
Tipo de Persona	Persona Jurídica	Tipo de Residente	Residente
Nif	ES00000000T	Nombre	
1º apellido		2º Apellido	
Razon Social	Demo Offinvoice		
Dirección	Calle de la factu	Cód. Postal	28080
País	España	Provincia	Madrid
Poblacion	Madrid	Teléfono	666666666
Email	offinvoice@offinvoice.com		

Cliente			
Tipo de Persona	Persona Jurídica	Tipo de Residente	Residente UE
Nif		Nombre	
1º apellido		2º Apellido	
Razon Social			
Dirección		Cód. Postal	
País	España	Provincia	
Poblacion		Teléfono	
Email			

Tipo de Factura	Original	Moneda	EUR
Emisor de la Factura	Emisor	Tipo de cambio	1

Detalles

Fecha	Concepto	Uds.	Precio	Descuento(%)	IVA(%)	IRPF(%)	Base Imponible	Importe
26/04/2010								

Descuentos

Concepto	Descuento(%)	Importe

Fig. 5. Sample of invoice with Offinvoice in MS Excel 2010

This programme is operated as a set of additional Word and Excel menus, and makes it possible to process invoices in XML **facturae 3.1 and 3.2 formats and in UBL** (Universal Business Language) format, and in a **CII** (Cross Industry Invoice) prototype format (the specification is not complete). It also makes it possible to use the **XAdES-EPES and XAdES-XL** electronic signatures (in line with the standard TS 101 903).

There is a previous version, called FactOffice, designed for Word 2007, available at http://factoffice.codeplex.com

Any kind of electronic certificate can be used with both of these programmes, particularly **the electronic DNI (Spanish National Identity Card).**

Intermediate mechanisms, such as third-party invoicing platforms or for automation of key processes (such as invoice batch signing), can achieve a fairly high level of efficiency.

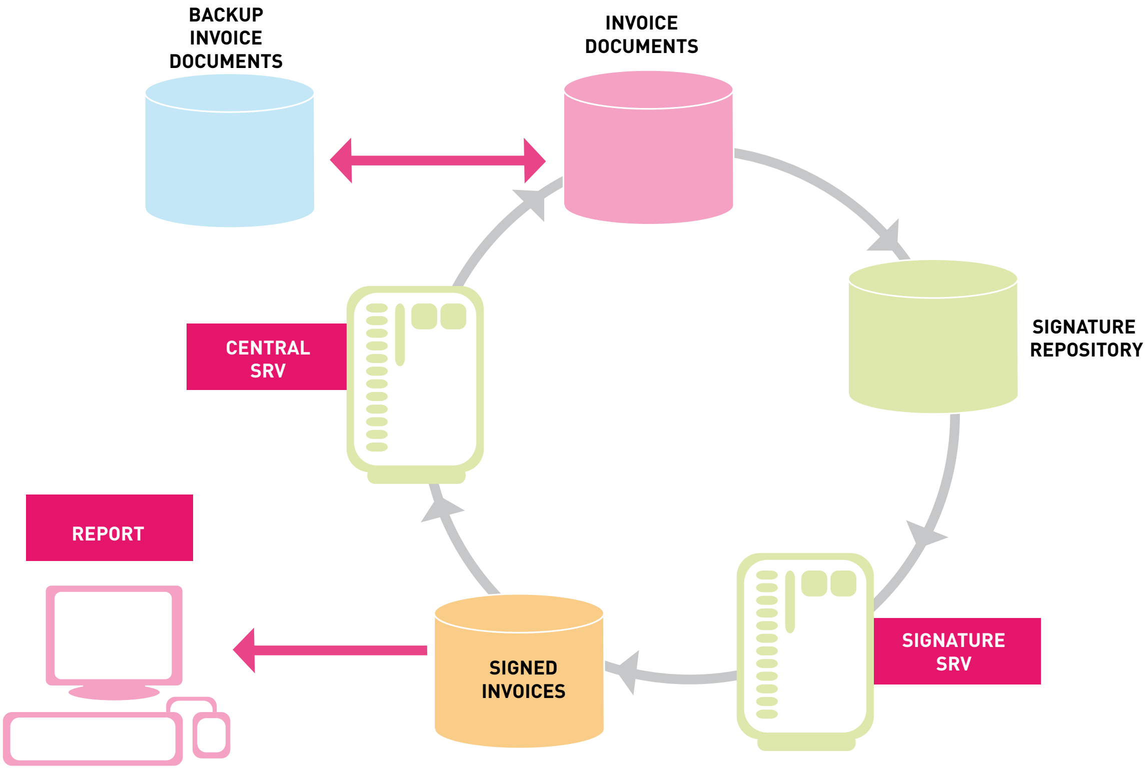


Fig. 6. Chart showing intermediate application for signing invoices that have already been created.

Upon generation of the invoice in a suitable format, the signature server automatically processes a batch of documents without any further manual intervention.

Customized developments or complex product integrations are advanced electronic invoicing projects.

If you decide to start to issue electronically-signed invoices in a simple way before later expanding the scope of the project, you will need an electronic signing programme and a certificate issued by a certification service.

"It is important to look at whether the company is going to start implementation from the perspective of an issuer or a recipient".

Requirements for issuing electronic Invoices

Despite the fact that implementing electronic invoicing necessarily involves both parties, the issuer and the recipient, the vast majority of projects initiated in Spain involve the issuing of invoices.

Invoice issuance projects may be easier to carry out, even though they have a smaller impact on the goal of speeding up an entity's processes.

The requirements for the **issuer** are

- To obtain the prior consent of the recipient.
- To guarantee the authenticity of the origin and integrity of invoices, by using the qualified electronic signature.
- To retain a copy of the invoices. This requirement is not necessary if an invoice can be reconstructed from the information saved in the company's database (original).
- Saved invoices must contain specific elements that make it easier to search for them, view them and print them in the event of an inspection (full access to data).

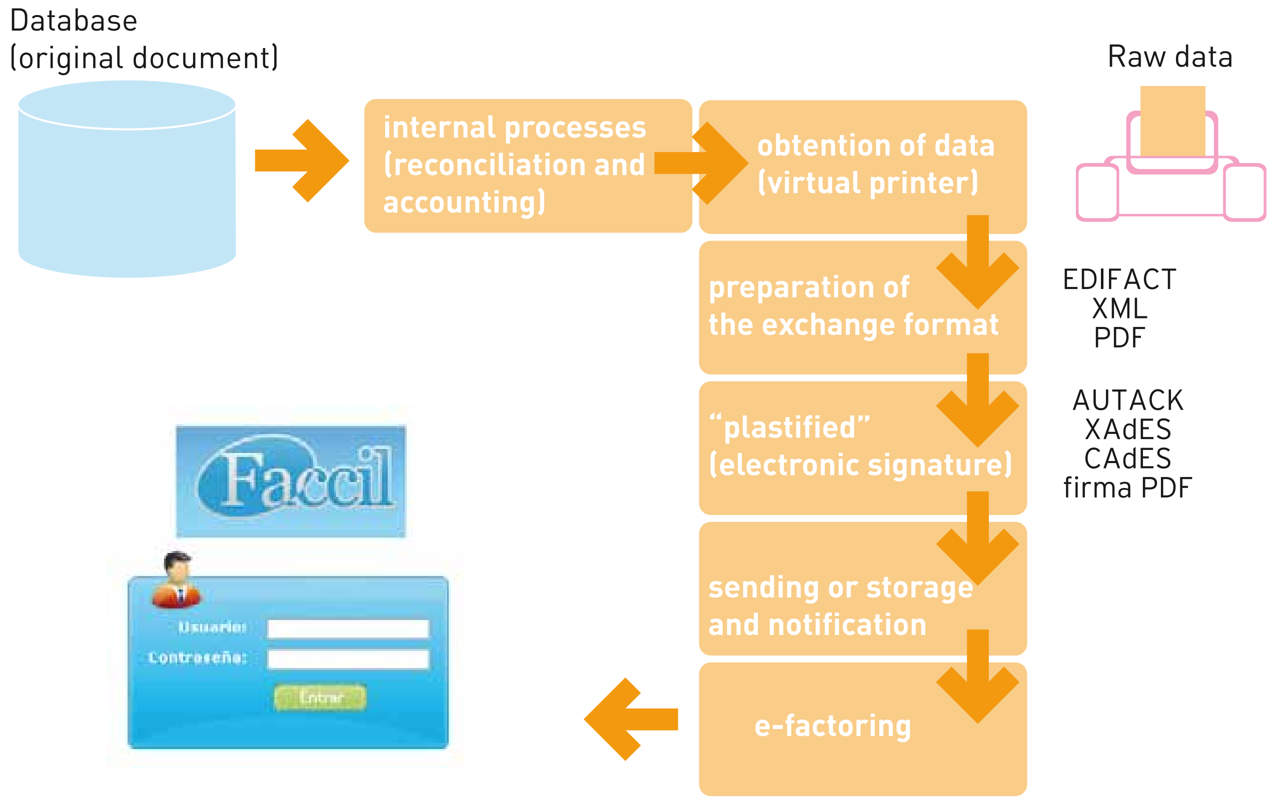

Database
(original document)
internal processes (reconciliation and accounting)
obtention of data (virtual printer)
Raw data
preparation of the exchange format
EDIFACT
XML
PDF
"plastified" (electronic signature)
AUTACK
XAdES
CAdES
firma PDF
sending or storage and notification
e-factoring
Faccil
Usuario:
Contraseña:
Entrar

Fig. 7. Basic flow of invoice issuing process

The invoice issuing process ends in it being printed, or in the generation of the exchange formats agreed on for recipients who prefer them in electronic format. The invoice format will determine the format of the electronic signature. After sending, the invoice is in a format that facilitates the management of factoring services with financial institutions.

"The vast majority of projects initiated in Spain focus on issuing invoices".

Requirements in the reception of electronic invoices

Integration with ERPs or internal invoicing managers is usually pursued in projects aimed at optimizing invoice reception through use of the electronic invoice.

The complexity of this type of project stems from the need to deal with an indeterminate number of electronic formats as well as receiving paper-based invoices.

In order to reduce the complexity of the process, the self-invoicing option can be pursued, a modality in which the recipient itself controls the reception format and guarantees the accounting reconciliation.

Another possibility that could be considered by recipient companies is to use external platforms, which, under the third party invoicing modality, facilitate the whole invoice conversion process, and even the certified digitalization of paper-based documents.

The requirements for the **recipient** are:

- To have the necessary software to validate the electronic signature.
- To store the received invoices digitally (invoice and signature) in their original format.
- Stored invoices should contain elements that make it easier to search for them, view them and print them in the event of an inspection (full access to data).

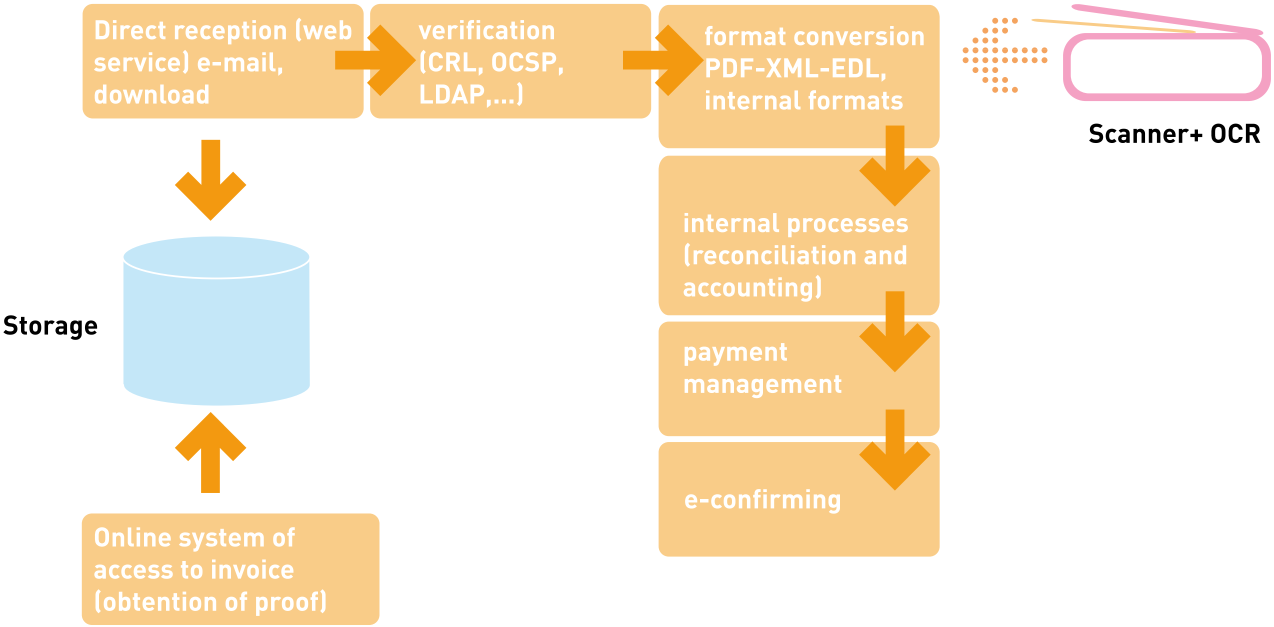

Direct reception (web service) e-mail, download
verification (CRL, OCSP, LDAP,...)
format conversion PDF-XML-EDL, internal formats
Scanner+ OCR
internal processes (reconciliation and accounting)
payment management
e-confirming
Storage
Online system of access to invoice (obtention of proof)

Fig. 8. Basic flow in the invoice receipt process

In the reception process, the two main elements are the storage of the electronic invoice in its original format, and verification of its validity. It is also necessary to adapt the format to the one that the reconciliation application uses internally, so that it can be accounted and paid. This procedure can end up facilitating the confirming services for financial institutions.

> *"The complexity of this type of project stems from the need to deal with an indeterminate number of electronic formats as well as receiving paper-based invoices".*

Certified digitalization, as defined in Order EHA/962/2007, makes it possible to convert paper-based invoices into an electronic format, and recipients do not need to ask for permission to do this, although they must use authorized software. The purpose of this is to enable the electronic storage of paper-based invoices, so that these can be destroyed.

Currently, there are more than 30 document management systems approved by the Spanish Tax Agency to facilitate this process, which is considered an intermediate step before full implementation of electronic invoicing.

Once the certified digitalization of an invoice has been carried out, the paper document can be destroyed, given that the converted document can now be viewed as the "original".

How to make electronic invoices on third-party platforms.

The possibility to delegate material invoicing, either to the recipients of transactions (**self-invoicing**), or to third parties, by hiring their services (**third-party invoicing**), is expressly provided for in Royal Decree 1496/2003.

Regardless of the model used, the party responsible for compliance with the legal obligations on invoicing is the business owner, professional or person **responsible for issuing the invoice**. This means that delegating the material issuance of invoices does not remove responsibility, and, therefore, taxable people should take care in their choice of supplier. The credibility of the service provider is very important. (See Articles 5 and 19.3 of Royal Decree 1496/2003).

For these options to be valid, the following requirements should be fulfilled:

- Prior documented **written** agreement between the issuing taxable person and the entity that effectively manages the invoicing, whether this is a third party or the recipient taxpayer (self-invoicing). This agreement must contain the express authorization of the issuing taxpayer and the transactions included in the agreement.
- The businss owner or professional delegating the recipients to issue the invoices should accept or reject the issue of each specific invoice, within fifteen (15) days **of receiving** the copy or electronically accessing it. If it is rejected, this should be done explicitly. If it is rejected, the invoice will be **annulled**, or **considered to be unissued.** Therefore, it is advisable not to assign a number to the invoice until approval has been received or fifteen (15) days have passed. Receipt acknowledgement systems could be used in order to measure this time period, for example by downloading a file (any kind of chart, or a small version of the invoice) into the e-mail sent to notify the seller that an invoice is awaiting approval.
- These invoices can be issued in the name of and on behalf of the business owner or professional who has carried out the transactions documented in them.

In order to solve the problem of deadlines and uncertainty in the issuing of invoices, it is advisable that, in the agreement, the issuing taxable person expressly gives consent to the issue of invoices by the recipient, dealing with any discrepancies that may arise exceptionally by means of amendment invoices.

When external invoicing services are used or the invoicing management is delegated to some recipients, a specific series should be assigned for every entity that manages invoices on behalf of the issuing taxable person.

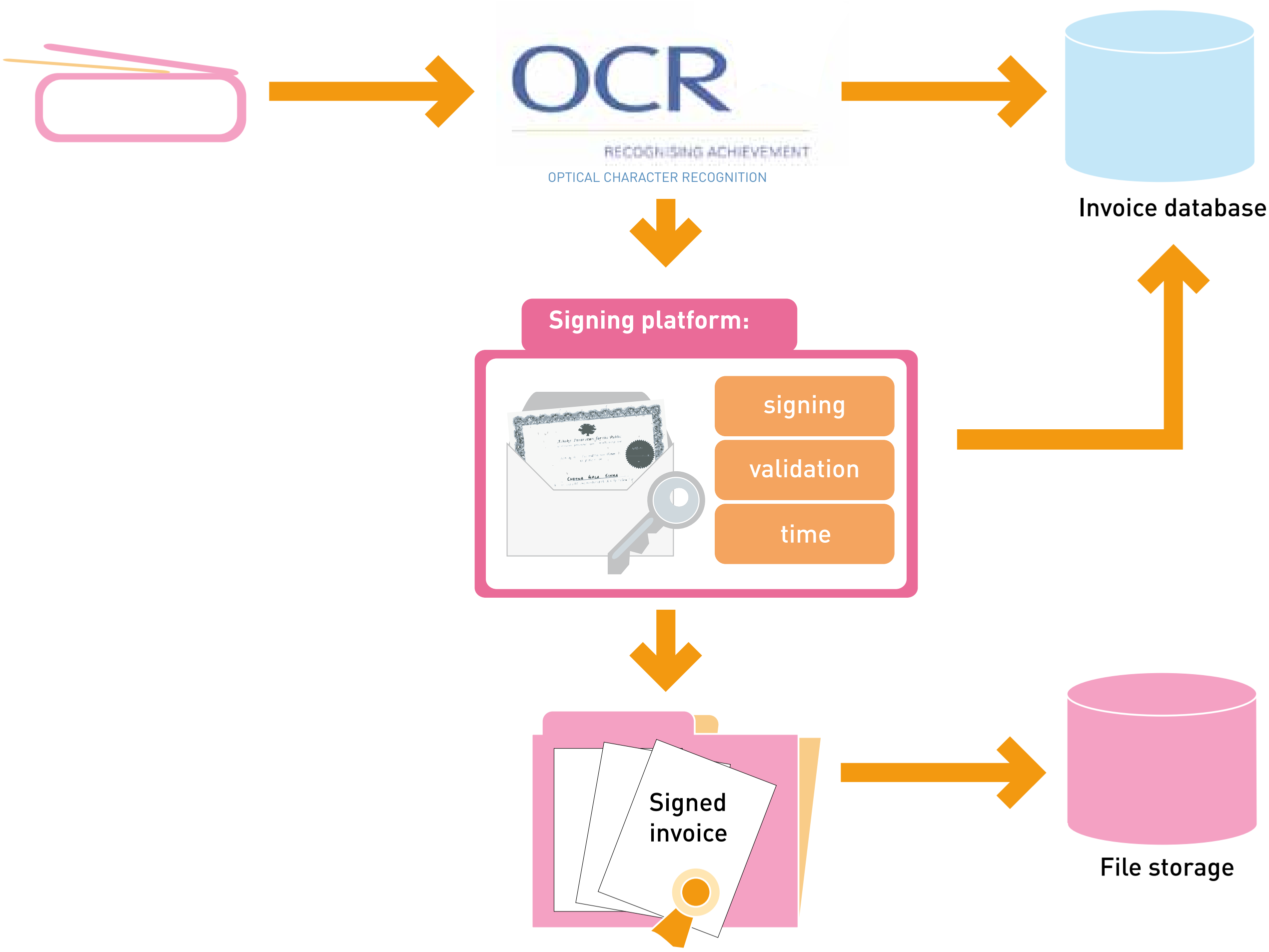


Fig. 9. Flowchart showing the certified digitalization process

The invoice is signed after it is digitalized. A supplementary process is the application of OCR (Optical Character Recognition) systems, which enable words to be extracted from the document, making the subsequent search easier. In this example, a signature type called "full signature" is used, which includes information from the time at which the validity of the certificate was verified and on the certification service provider's response when asked about this validity.

"The possibility to delegate material invoicing, whether to the recipients of transactions (self-invoicing), or to third parties, by hiring their services (third-party invoicing or "sub-invoicing"), is expressly provided for in the current legislation"

Samples of electronic invoice

Facturae invoice

Even though users do not need to know the internal coding of an electronic invoice, sometimes people would like to know what an invoice file looks like internally.

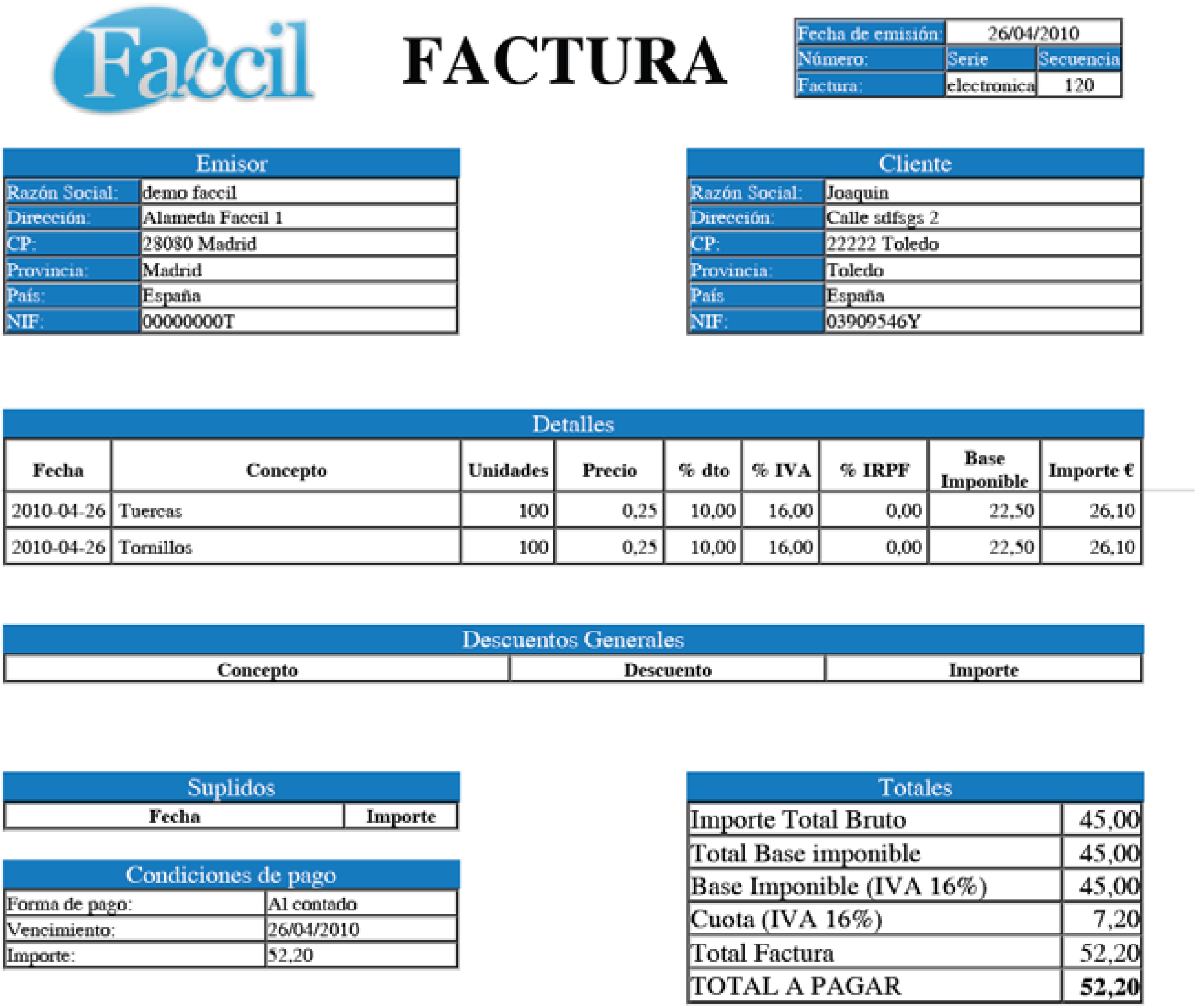
This is an example:

```
<?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>0000000000B18</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. Heading of an invoice in facturae format with an XAdES XL electronic signature

This can be viewed with an XSLT (Extensible Stylesheet Language Transformations) template and a CSS (Cascading Style Sheet), such as the one available on the facturae.es website. When this template is applied, the invoice is displayed in a specific form, but this display could be different if a different style sheet is used. Occasionally, this can be useful when someone has to review their invoices, since the invoices of all providers can be presented in the same format.



Faccil

FACTURA

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

Emisor	
Razón Social:	demo faccil
Dirección:	Alameda Faccil 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	Tornillos	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**

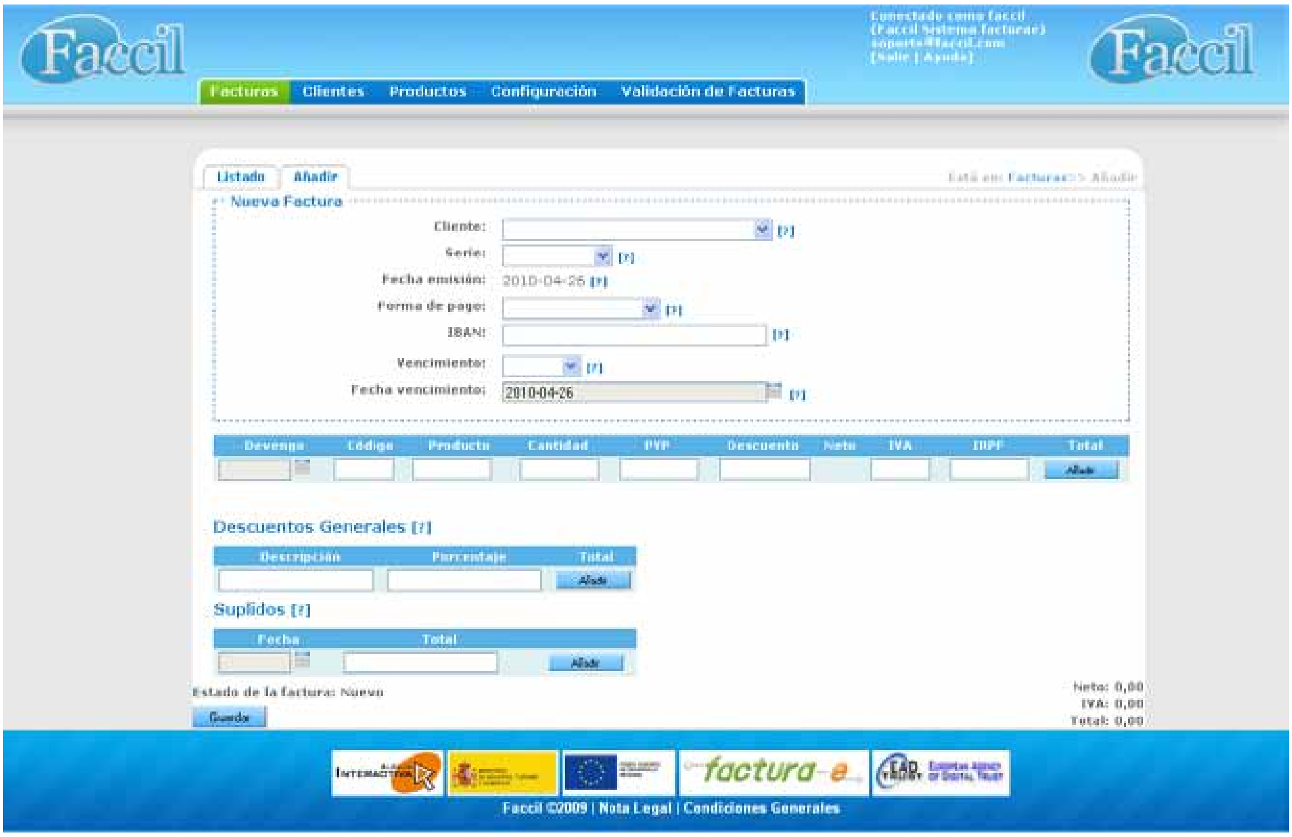
Fig. 11. Screenshot of an XML facturae invoice display upon application of conversion and style sheets. An XML invoice can be displayed in different ways, according to the template (style sheet) used. For example, recipients can apply their own templates in order to help them review many invoices, since the essential sections of the invoices will be positioned in the same area of the image.

Use of internet-based applications (Software as a Service or Cloud Computing)

Third-party platforms are probably the most convenient option for a small or medium-sized company. Generally, a monthly fee is paid for a service which can be accessed, cost-free and remotely, over the internet, with the third-party entity being in charge of ensuring the legality of the invoices through use of the electronic signature.

In this case, the company issuing the invoices does not have to concern itself with obtaining digital certificates, since the service provider is responsible for doing so. Some invoicing service providers, however, offer the option of using the company's certificates, if it has them.

The most commonly-used modality on these platforms is third-party invoicing, and, in the majority of cases, they include a simple ERP that can be used to manage invoicing for a small company.



Nueva Factura

Cliente: [?]
Serie: [?]
Fecha emisión: 2010-04-26 [?]
Forma de pago: [?]
IBAN: [?]
Vencimiento: [?]
Fecha vencimiento: 2010-04-26 [?]

Devenga	Código	Producto	Cantidad	PVP	Descuento	Neto	IVA	IRPF	Total

Descuentos Generales [?]

Descripción	Porcentaje	Total

Suplidos [?]

Fecha	Total

Estado de la factura: Nuevo

Neto: 0,00
IVA: 0,00
Total: 0,00

Fig. 12. Creating the invoice using a form.

In this case, the Faccil service, one of the many services offered on the Internet, has been used. When financial entities provide invoicing services, they also use the third-party invoicing modality, so the screen display is very similar to this one. Invoices are prepared using forms. Invoices remain in draft status until a decision has been taken that they are complete and ready to issue.

03.

Chapter 3. Advanced electronic invoicing projects

Identification of advanced projects

Advanced electronic invoicing projects entail a certain level of complexity in implementation and they often require several departments in the company (IT, administration, invoicing, purchasing, etc.) to take part in designing and implementing them.

Most common examples of advanced projects

In general terms, an electronic invoicing project can be considered to be advanced in the following cases:

- When a specific product is designed to be specifically oriented to the user's needs.
- When a generic platform or product is integrated in user information systems.
- When amendments are made to elements available in the company, such as integrating the electronic signature into ERPs.

The level of difficulty and length of time that this type of project will take varies depending on a series of key elements, such as the entity's technological and development capacity, the degree of involvement on the part of the participants, the availability of key elements in electronic invoicing systems (ERPs, digital certificates, etc.), the adaptability of the previous elements and the training of users involved.

On most occasions, it is advisable to seek assistance from third-party entities, software consultancies and developers, which will offer the company their experience in projects of this type and will cover areas that the entity cannot deal with alone. The expert's activity can include several aspects:

- Technological consultancy and advice
- Legal advice
- Tax advice
- Development and implementation
- Training
- Systems and communications

In an advanced electronic invoicing project, it is also important to clearly define the scope of the project at the outset, in other words to make a decision on the critical, advisable and unnecessary objectives. For example, a company may decide to carry out an invoice issuance and receipt project aimed at all the companies with which it operates, or, on the other hand, it may only aim to resolve the most complex invoicing issues with its strategic customers / suppliers. Similarly, it may decide whether to take on a full project (issuance / receipt), or to focus on only one of these two elements, according to which is the most important.

From a practical point of view, it would be advisable for a company to start by developing a project according to the invoicing importance (issuance /receipt) with regard to its most important customers, and then to subsequently complete the project according to the resources available. This solves the company's most urgent needs quickly, without ruling out future possibilities for growth.

Lastly, it is advisable to carry out a modular project, which makes it possible for the platform to grow further in future and to re-use the elements in other projects.

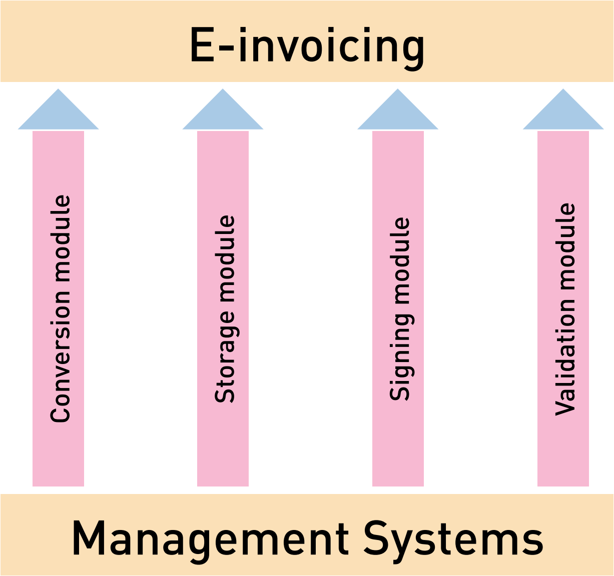


Fig. 13. Cornerstones of e-invoicing.

- **Conversion module:**
Performs modifications between input and output formats.

- **Storage module:**
Storage method for the original invoice (generated or received).

- **Signing module:**
For creating electronic signatures in the invoices in those cases where the issuer has signing capacity.

- **Validation module:**
This assesses the correctness of received invoices and the validity of the electronic signature.

The emphasis on storage or signature depends on the entity's role as the invoice issuer or recipient. Occasionally, however, all modules come into play, for example, in the self-invoicing and third-party invoicing modalities. In self-invoicing, it is the recipient who signs electronically. In third-party invoicing, a third party signs on behalf of the issuer and stores the electronic invoices on the recipient's behalf.

> *"In most cases, it is advisable to use third-party entities, which offer the company their experience in these kinds of projects and can cover areas that the entity cannot cope with alone".*

Invoice issuing-oriented projects

The main purpose of an invoice-issuing project is normally to achieve cost reductions in the manual handling of invoices: printing, envelopes, delivery, etc. However, other relevant objectives are also to optimize available resources, cut down payment times and improve the reliability of accounting reconciliation methods.

This is the most frequent type of project and the simplest to put into place, given that, in general terms, the issuing company controls the invoice formats and means of issuance, especially when the provider is in a position of strength in relation to its customers. Nevertheless, in most cases, it is necessary to convert formats in order to ensure interoperability with certain companies.

The most complex part of invoice issuance projects is usually the electronic signature process, given that it entails the integration of codes and certificates in the platform, as well as the development of the signing application, particularly when the company decides to use an electronic signature (not required by law) with all the validation elements allowing the recipient to subsequently verify it reliably over time, with the help of **Timestamp Authority support (TSA) and Validation Service Providers (VA).**

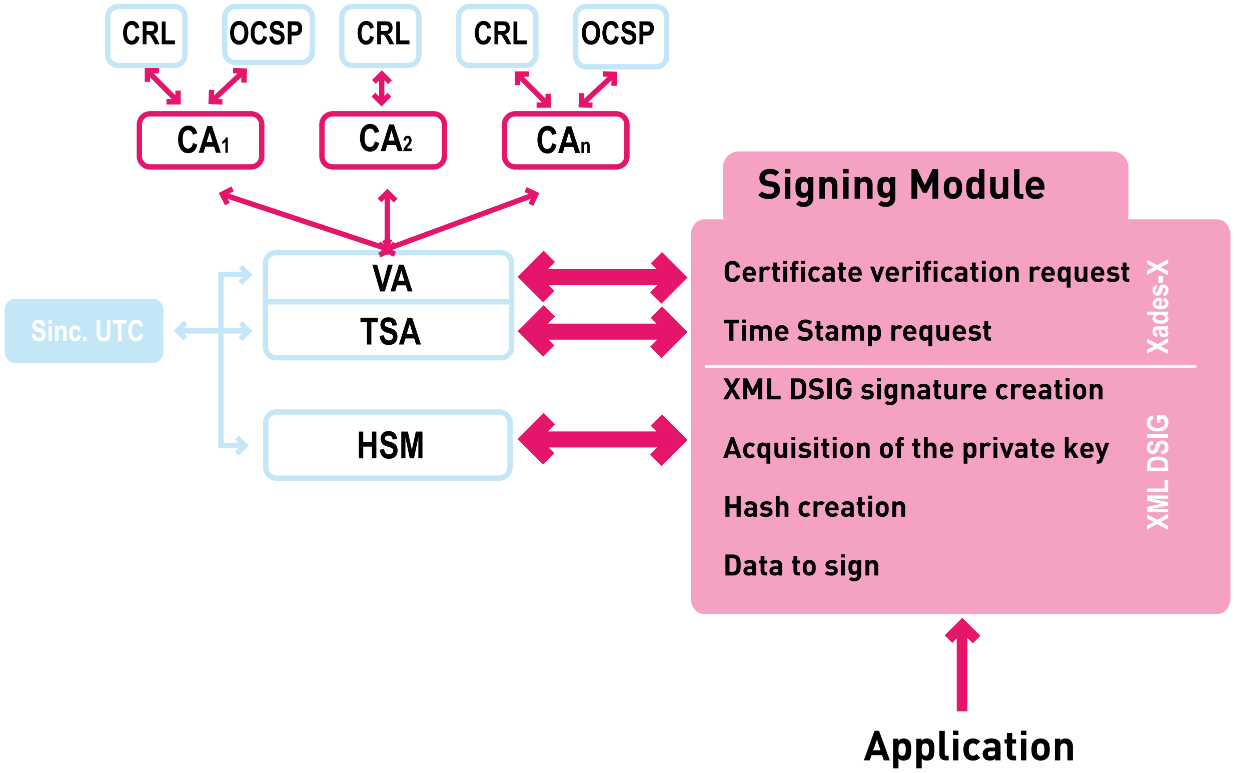


*Fig. 14. Potential chart of **XML**-based signature*

This modality covers the full ES-XL signature described in the standard TS 101 903. If the full signature is created by the signatory, the third party trusting the certificate does not have to concern itself with understanding the peculiarities of the CSP that issued the validation services certificate.

"The most complex part of issuance projects is usually the electronic signature process".

Even though this modality is not enforceable from a legal point of view, it frees the recipient from the problem of having to validate electronic signatures using certificates issued by certification service providers, whose processing of revoked certificates is not easily accessible to the recipient.

Invoice receipt projects

If the most complex part of the issuing process is the electronic signing of invoices, the most important aspect in invoice receipt is validation, both of the format of the invoice documents and of the certificates with which they have been signed.

For the verification of invoice formats, it is necessary to know the type of data received in order to subsequently convert these to the company's internal format and to process them in applications (generally ERP). Obviously, structured formats such as XML facilitate the conversion task considerably.

There are two main aspects relating to the validation of electronic signatures on invoices: the invoice format used (XML, CMS, etc.) and the certificate with which the invoice has been signed. As regards the first, it is essential to identify the signature format in order to be able to parse this signature and extract the necessary elements (signatory, certificate issuer, validity in time, location of the revocation information, etc.). Once the certificate information has been extracted, it is necessary to verify that the certificate was valid at the time of signing and that it has not been revoked, which requires the same information contained in the certificate and possibly from external sources. Today, elements exist to help validate electronic signatures, such as the Validation Authorities.

Fortunately, standards are being developed both in the format of the invoice document itself and in the associated electronic signature, most of these being XML-focused: facturae, UBL, CII, and, in terms of the signature, XAdES, etc. Once the validation and conversion processes have been carried out, the recipient should integrate the data obtained into its own system, bearing in mind that the invoice should be stored in the same format in which it was received, since this is considered the original for tax purposes.

Finally, as mentioned before, the National Tax Agency initiative to digitalize and secure invoices received in paper format is also important.

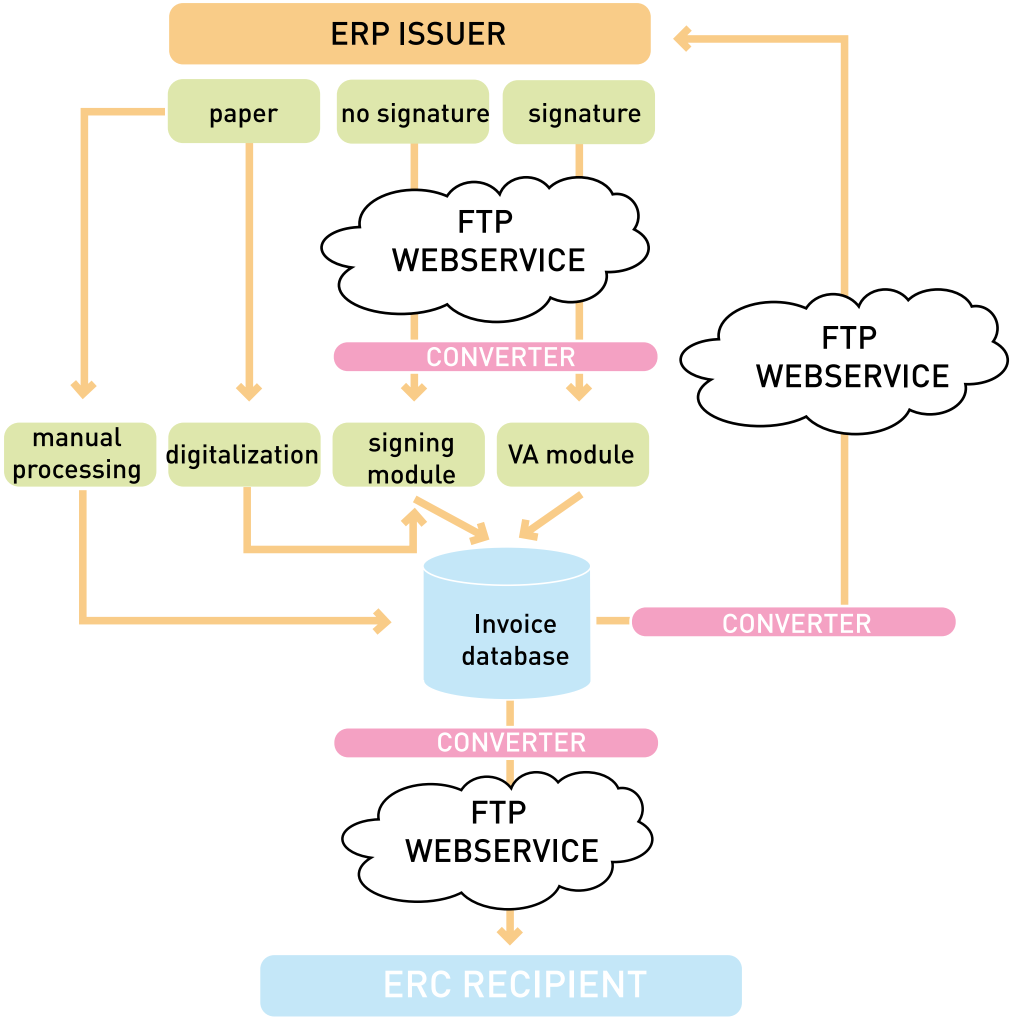


Fig. 15. Invoice processing and integration chart.

The project should encompass the use of several transfer systems, together with the invoice and signature formats.

"The differentiating element is validation, both of the format of the invoice documents and of the certificates with which they have been signed".

Preparation of the project

It is usually necessary to consider a short checklist, in order to ensure that we are fulfilling all the requirements.

Elements that should be taken into account before embarking on an e-invoicing project:

- Invoicing flow specification
- Document flow design
- Identification of roles involved
- Definition of legal requirements
- Management of integration with suppliers and customers
- Integration with the company's systems

- **Invoice flow specification:** analysis of the characteristics of providers/ customers in order to determine how to incorporate them into the project, and also of the formats used to issue/receive invoices.

- **Document flow design:** in order to identify inefficiencies in the process and facilitate implementation of automated workflow systems.

- **Identification of roles involved:** it is fundamentally important to identify human resources, both inside and outside the organization, that are involved in the project as well as those that are not.

- **Definition of legal requirements:** to define any aspects of current legislation that may affect the project.

- **Management of integration with suppliers and customers:** working with suppliers and customers to address all aspects that affect functionality, usability, format compatibility, etc.

- **Integration with the company's systems:** obviously, the electronic invoicing system must be integrated with the company's systems: ERP, invoicing systems, CRM and payment management systems.

Electronic invoicing to Public Administrations

Public administrations, by virtue of Law 11/2007 on Electronic access of citizens to public services, must be in a position to receive electronic invoices upon suppliers' request. However, electronic invoicing is not mandatory for companies.

The rule that does impose electronic invoicing obligations on companies that supply the state public sector is Law 30/2007, of 30 October, on Public Sector Contracts. This obligation is also established by Law 56/2007, of 28 December, on Measures to promote the information society, which also requires actions to be carried out to boost the use of electronic invoices throughout the rest of the country's productive sector, by encouraging collaboration between the Ministry of Industry, Tourism and Trade and the Ministry of Economy and Finance, and between these and the Autonomous Regions.

The above-mentioned ministries have collaborated in rolling out the facturae portal (http://www.facturae.es) and in developing Order PRE/2971/2007, of 5 October, on the electronic issuing of invoices when the recipient is the central government or public entities linked to or operated by it, and on the submission to central government and its associated and dependent entities, of invoices issued between individuals, which establishes the kind of electronic invoice format to be submitted to public administrations.

The Subdirectorate General of Information and Communication Technologies of the Ministry of Industry, Tourism and Trade has also carried out a series of actions to facilitate uptake of the e-Invoice in small and medium-sized companies, as well as tools that enable the signed documents to be verified, thereby ensuring the authenticity and integrity of the electronic invoicing process.

Apart from this work, European public administrations have been collaborating for some time now in order to firm up interoperability criteria, which are desireable, without prejudice to sovereignty issues, in public procurement and other development activities carried out by public authorities. One of the most relevant developments is the Peppol Project (Pan-European Public Procurement Online). The aim of this project is to establish a pilot solution at European level that, together with national solutions, will facilitate an interoperable electronic public procurement system across Europe.

From the standardisation point of view, it is worth mentioning two initiatives of the CEN (European Committee for Standardisation).

One of these is the CEN/ISSS Business Interoperability Interfaces for Public e-procurement in Europe Workshop (BII), which, based on UBL, defines the necessary messages based on the ontology defined by CODICE (Interoperable Components and Documents for e-procurement), among other references. CODICE is a development promoted by the General Directorate of State Assets, which is part of the Spanish Ministry of Economy and Finance).

The other initiative is the CEN Workshop on e-Invoicing, which has already initiated Phase III, following the publication in previous phases of relevant documents and surveys on the application of electronic invoicing regulations throughout Europe.

04.

Chapter 4. Interaction with paper-based invoicing

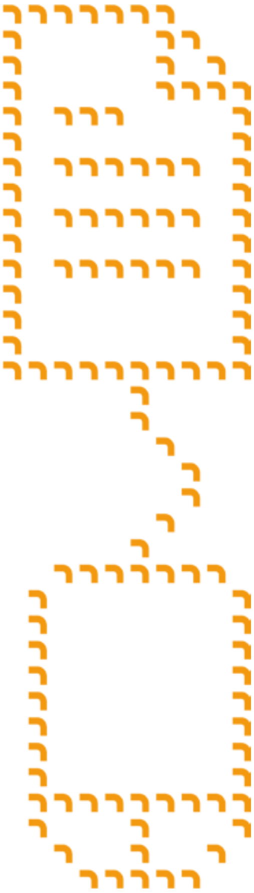
How to electronically store paper invoices

Although the legislation provides for electronic storage of invoices, the fact that invoices must be available for tax inspection in the format in which they were originally received means that electronic storage was until very recently understood to apply to electronically -issued invoices only.

Now, Order EHA/962/2007 has defined the way in which invoices received on paper should be processed, using the concept of **certified digitalization.** This is a process in which an electronically-signed digital image of the paper-based invoice is generated. This is considered to have the same value as an original invoice, having even greater certification value than an electronic certification, which means the paper invoice can be destroyed.

In order for the certification value described above to be approved, accredited devices, (which must pass an audit process in order to obtain this accreditation), should be used.

To ensure that the documents digitalized in this way fully comply with the authenticity conditions, it is advisable to use the **ES-X-L** electronic signature modality, also known as the complete signature, since the person responsible for verifying the signature does not have to worry about identifying the validity verification mechanism, which may be different for each provider. It should be noted that there are more than 20 certification systems in Spain alone, and that each of these has its own verification mechanisms.



If an OCR (Optical Character Recognition), system is used, the system can recognize letters and numbers, and superimpose these in a layer of the file, simplifying document indexation and searches. If the invoice has also been printed on the basis of an agreed template, the OCR will allow the invoice to be coded in the standard facturae format or another one, also helping the content of the invoice to be inserted into the computer system and processed in an automated manner, to a greater or lesser degree.

For this reason, it is advisable for issuers to adopt specific invoicing forms. This will help to facilitate the recipient's work, even when an invoice is issued in paper format.

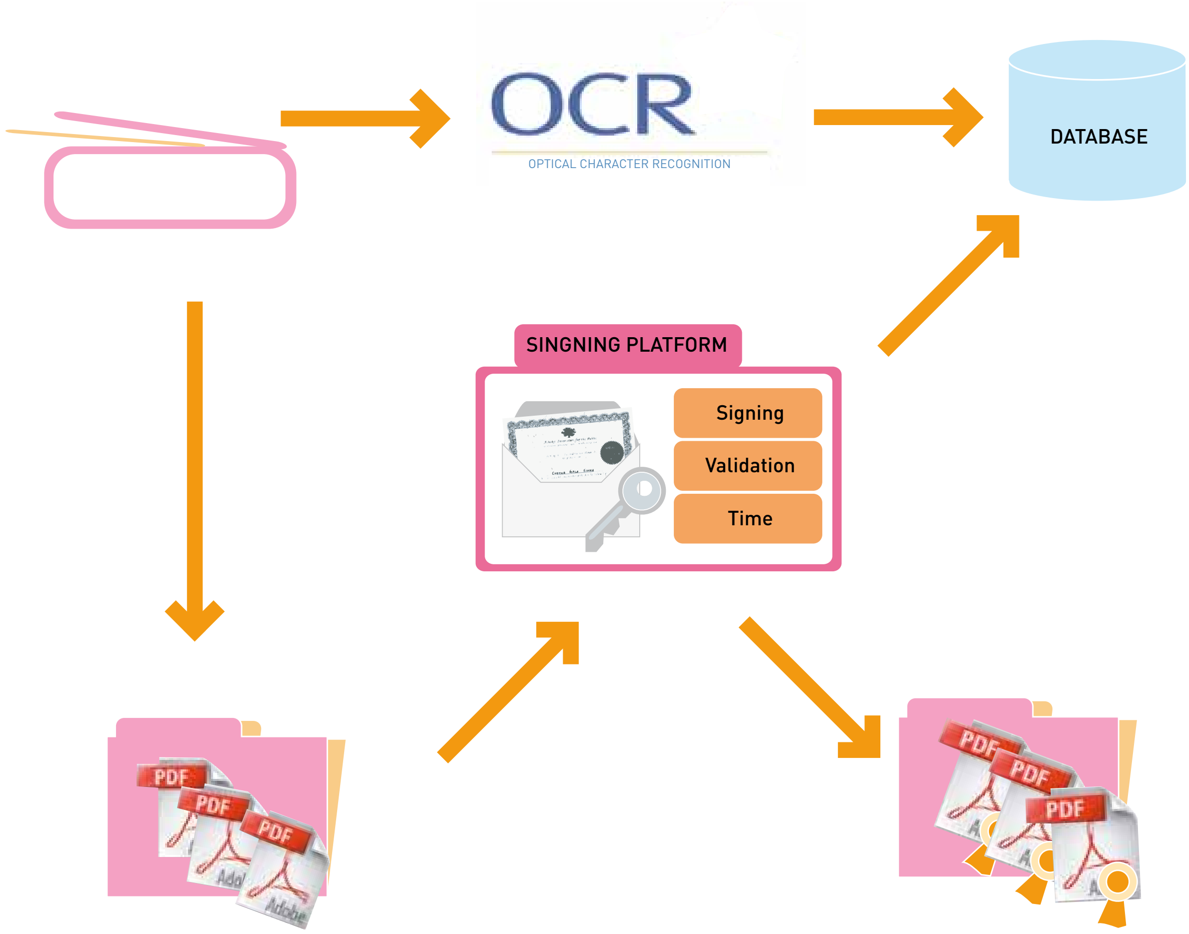


Fig. 16. Certified digitalization process.

The recipient of a paper invoice does not need authorization to digitalize invoices through "certified digitalization", as long as he or she uses software authorized by the Tax Agency and an electronic certificate that electronically signs digitalized documents. The PDF format is frequently used for digitalization purposes, because it is easy to read the digitalized invoices and to verify the metadata and electronic signatures using the free Adobe Reader software.

How to store invoices received electronically in paper format

Although it is possible to store electronic invoices in paper format using a bar code, another alternative mechanism can also be used.

When a third party is acting on behalf of the taxpayers, the issuer or recipient of electronic invoices may provide their clients with IT applications that handle a repository of invoices and substitutive documents issued or received, whichever is relevant, together with the electronic signature generated or verified (depending on the role of the issuer or the recipient of the invoice), providing a secure verification code for the document. This code makes it possible to access the associated document held in the repository, (for example via web access), guaranteeing user compliance with the legal requirements regarding electronic invoicing. In this event, a document printed on paper with this code is a valid system for preserving the electronic signature in paper format, provided that the repository in which the document and its electronic signature are stored is preserved, there is a signature verification mechanism in the repository, and the invoice is fully accessible using the electronic authentication code. This is specified in Article 6 of Order EHA/962/2007.

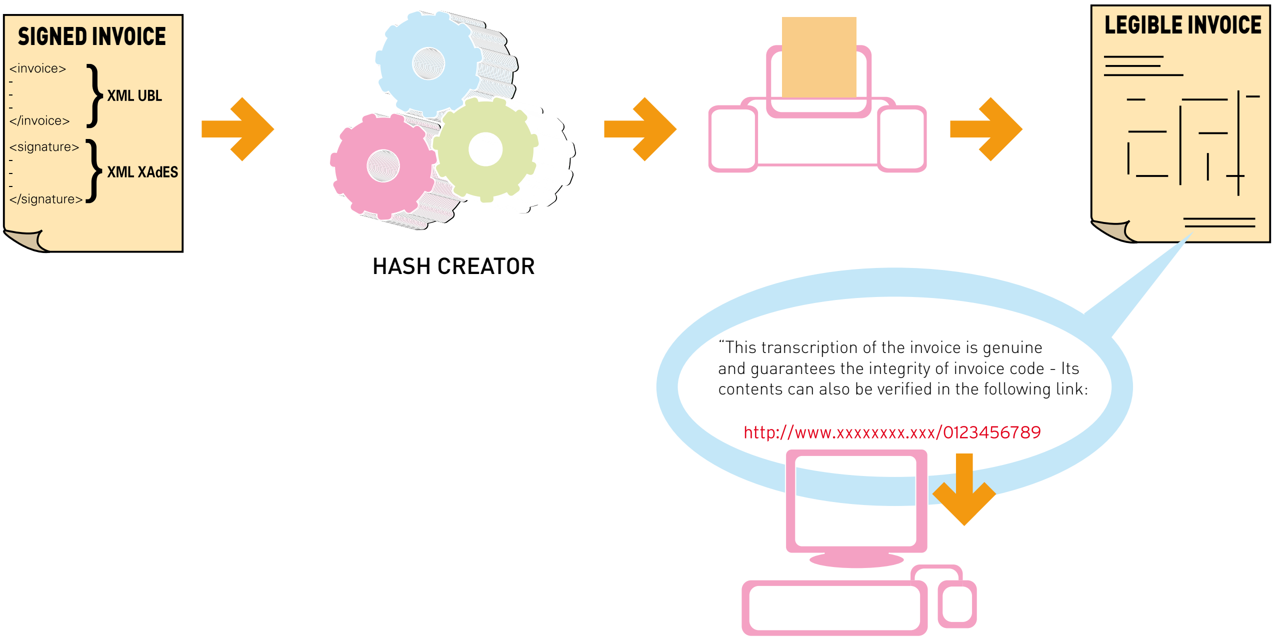

SIGNED INVOICE
<invoice>
</invoice>
XML UBL
<signature>
</signature>
XML XAdES
HASH CREATOR
LEGIBLE INVOICE
"This transcription of the invoice is genuine and guarantees the integrity of invoice code - Its contents can also be verified in the following link:
http://www.xxxxxxxx.xxx/0123456789

Fig. 17. Example of invoice retrieval code generation chart.

A unique identifying code is generated with the electronic invoice data. This code can be entered in the paper copy of the invoice so that it can subsequently be located and retrieved.

"Even though it is possible to store electronic invoices in paper format using a bar code, another alternative mechanism can also be used".

05.

Chapter 5. Electronic invoice and signature formats

Electronic invoice formats

The format containing the invoice, namely, the file where the invoice data are stored before being signed electronically, has no legal relevance unless the invoice is issued to a public entity. It could be a PDF file, an RTF file, an Excel document, plain text, HTML, XML, etc. Any format is valid, provided that it is subsequently signed electronically in order to make it legally valid.

In Spain, when the recipient is a central government authority, the invoice must be coded in XML facturae format. Under the second final provision of Order PRE/2971/2007, this format will be adjusted two years after the publication of the order, to UBL (Universal Business Language) format, or, if applicable, to the format established by the EU standardisation entities CEN (European Committee for Standardisation) or CENELEC (European Committee for Electrotechnical Standardisation), in order to permit the interoperability of invoices issued by any EU member states.

Currently, there is certain international consensus around adopting the future UN/CEFACT CII (Cross Industry Invoice) specification.

```
<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. XML invoice extract (UBL format) with electronic signature. For further information on this format, go to http://www.oasis-open.org/committees/ubl/.

Signature format

Special signature formats: dated and validated signature

Apart from **simple**, **advanced** and **qualified** signature types (qualified electronic signature), established both by the Directive and the Spanish Law on the Electronic Signature, other sub-types of advanced electronic signatures that are essential to facilitating the use of electronic signatures in several contexts have been defined by ETSI (the European Telecommunications Standards Institute).

The legally relevant types of signature are the following:

- **Simple:** Data which can be used in order to identify the signatory (authenticity)
- **Advanced:** Apart from identifying the signatory, this makes it possible to ensure the integrity of the document.
- **Qualified:** This is the advanced signature supported by a qualified certificate (certification granted following verification of the signatory's identity in person) and produced using a secure signature-creation device.

The advanced signature can include any amount of information relating to the moment at which it was created or the validity of the certificates. The most simple one is the basic signature, which includes the essential elements in electronic signing: the summary of the signed document (hash), the certificate of the signatory associated with the private key with which the signature is made, and the result of applying the private key to the summary, which is the actual electronic signature itself.

The **dated** signature (XAdES-T) adds time-related information to the basic signature about the time or verification of the signature, and the validated signature adds information to the dated signature on the validity of the certificate used at the time of the signature or its verification.

When the electronic signature is XML-encoded, these signature modalities are covered by the standard TS 101 903, in its XAdES-BES, XAdES-T and XAdES-XL aspects, although there are other variations.

The validated signature is also called the complete signature, because it includes all the elements that make it possible to verify that the certificate used by the signatory was valid at the time of signing, and allows long-term storage.

The advantage of the signatory encoding the signature in ESXL format is that this releases the recipient from the problem of having to validate the certificate used, given that the signature already includes all the elements guaranteeing its validity at the time of signing.

Electronic signatures used in electronic invoicing are usually the advanced and qualified signatures, and, for the facturae format, in the XAdES-BES and XAdES-XL modalities.

XML signatures

XML signatures are used when the invoices themselves are encoded in XML, although they can be used in any type of document, regardless of its format.

There are different format subtypes within XML-format electronic signatures, with XML Advanced Electronic Signatures (XAdES) being particularly important.

There are three signing modalities for all XML signatures:

- **Enveloped**, in which the signature is added at the end of the XML document as an additional element.
- **Enveloping**, in which the document is included in the signature, with the document signed being referenced as an object inserted within the signature.
- **Detached**, in which the signature and the document are separated into two files; the URL at which the document is located can be shown in the signature itself.

```
<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>
```

Figure. 19. XML signature (XAdES-XL) of the facturae signing policy 3.1

Even though the data relating to time stamping and certificate revocation can be very useful and lend great added value to the signing process, these are not obligatory for making the electronic signature valid.

Annex I.

Annex I. Introduction to electronic signature and certification

CSP and CA

Over the following pages, two terms are frequently used as synonyms even though they are not. Certification service provider (CSP) is a legal term defined in Directive 93/1999 and in Law 59/2003, while Certification Authority (CA) is a technical concept expressly contained in recommendation X.509 of the UIT-T. The term CSP is broader given that it includes the CAs that issue "electronic certificates", and also those CAs that "provide other services relating to electronic signatures", for example, VA (Validation Authority), RA (Registration Authority), TSA (Time Stamping Authority).

The handwritten signature

The handwritten signature makes it possible to certify the signatory's acknowledgement of, or agreement with, a document, and so it has great legal importance. Even though there are several ways to show or demonstrate conformity with different actions, and to seal agreements between individuals and companies, the handwritten signature has an especially high degree of acceptance.

The handwritten signature has the following features:

- It can only be affixed by one person
- It can be verified by anybody, by being compared with a sample

Any problem with recognition of the signature can be resolved, when it is handwritten, by matching it with a sample (the signature on an ID card or credit card).

Something that is so easy to do and to verify in the real world is not so simple in the virtual environment. It requires the use of cryptography and the mathematical properties of codified messages.

Cryptography

The main purpose of cryptography is to find systems that make it possible to transfer certain information that is considered confidential from an origin to a destination, in a way that is so safe that, if a message is intercepted, an attacker cannot recognize the message.

One of the purposes of modern cryptography is to find algorithms based on mathematical principles (such as the impossibility of computer processing certain complex problems) which, being public (in other words supposedly known by an attacking cryptanalyst), help to guarantee the integrity of messages protected by them, at least during the period of time that knowledge of protected information can be of use. Likewise, it should not be possible to obtain keys from encrypted and plain-text fragments of the message.

Symmetric encryption

The main characteristic of symmetric cryptography is that, by using the same algorithm and the same key, it makes it possible to obtain the encrypted text from the plain text and vice versa. Given that the algorithm is public, it is thus necessary to keep the key between the parties confidential.

Symmetric encryption is easier to understand, since it is similar to the way in which we keep things in real life. Here is an example:

Imagine we have a box with a lock. If we make a unique copy of the key and we give it to our partner, we have a mechanism for exchanging objects or messages with him or her in a confidential and secure manner.

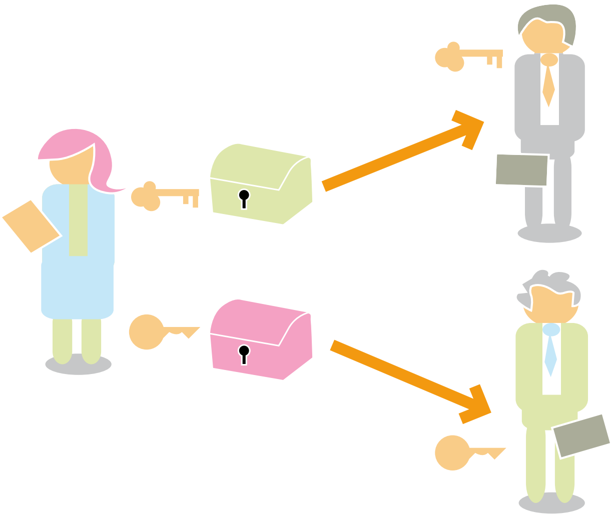


Fig. 20. Sharing symmetric keys.

The key which allows exchanging information between Alice and Bob should be different to the one shared by Alie and Charles.

It is thus possible to check that the sending was carried out by ourselves since we are the only ones who are able to introduce the document (the **use** of the box acts **as a signature**) and we also know that nobody else can know its contents while travelling (safe use).

The biggest problem arises when we wish that a numerous set of parties can keep communications among them. In this case, many boxes and a double number of keys are needed.

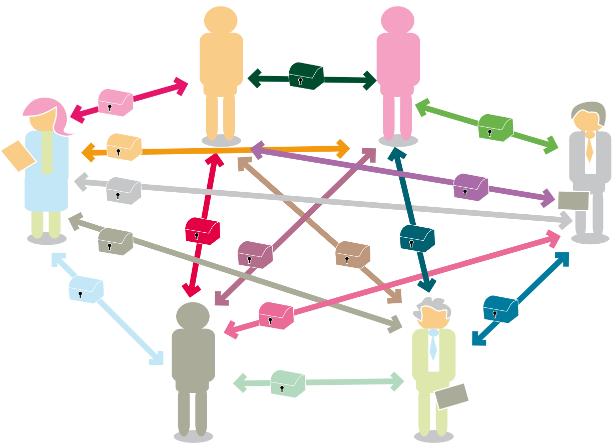


Fig. 21. The problem of multiplicity between partners and keys multiplicity problem.

A system in which keys have to be managed for every two individuals is not feasible.

The same boxes and keys cannot be used with different partners, given that this would result in a risk of impersonation or of the secrecy of the message being lost.

Asymmetric encryption

There is a possibility of finding a system that uses **different** keys for encrypting and decoding the message, in such a way that knowledge of the encryption key does not allow the message to be coded, and, inversely, knowledge of the encrypted text and the decoding key does not reveal any information on the encryption key.

One of the most widely used examples of this concept, proposed by Hellman and Diffie in 1976, is the Rivest, Shamir and Adleman (**RSA**) algorithm, based on the impossibility to computer process large compound numbers by factoring them into their constituent prime numbers.

In algorithms with pairs of keys, also called asymmetric or public-key algorithms, one of the keys is kept secret, while the other is made freely accessible: public.

Asymmetric encryption is hard to understand, and sometimes even hard to believe. In order to try to explain it, without using mathematics, we will again use a box-key analogy.

In this case, we will not use normal boxes, but "**magician's boxes**".

Imagine I have a false-bottomed box, formerly owned by a magician, with a cover that can be opened in two different ways with different keys. The way the box works means that, when it is opened with one key, something placed inside it passes into a compartment that can only be accessed with the other key. In this case, the keys are equivalent, in other words, an object placed inside the box using just one key can only be retrieved with the other key.

If I keep one of the keys as safely as possible and make copies of the other one, which I hand out far and wide or share publicly, anyone with one of these keys can give an object only to me without the others knowing. I alone will be able to collect the delivery. In this case, the box is used for additional safety.

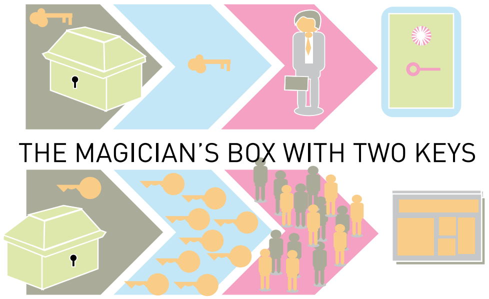


Fig. 22. Magician's box: a unique access key and many copies of the output key.

The access key is PRIVATE, and the output key, with multiple copies, is PUBLIC.

On the other hand, if I decide to show that I alone have had access to a certain piece of information or object, I can put it in the box using my key. Anyone who opens the box and finds the object knows that I am the only one who could have placed it there. In this case, the box is a tool that allows me to apply my electronic signature.

If everyone has a box like mine and shares the public keys with the others, we all have a system for sending messages to each other in a secure way and for signing transmissions. For 1,000 people, we would need 1,000 boxes, each of us having our own private key and the public keys of the other 999.

To draw a comparison, the symmetric encryption system, using normal boxes, would require 499,500 boxes and twice as many keys (combinations of 1,000 elements taken in pairs).

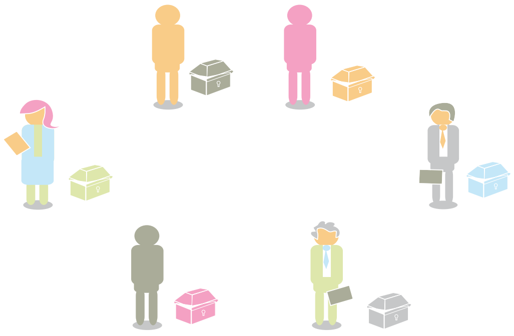


Fig. 23. Analogy of the multiple boxes and keys.
It is no longer necessary to share keys between every two users, as in the symmetric encryption system. Instead, each user has his or her pair of public-private keys.

Using equivalent principles, the electronic signature is based on public-key cryptographic systems. These systems use an algorithm that encrypts a plain text and encrypts it with a key. The encrypted text is restored to the original text by using a different key that is linked to the encryption key. If the encryption key is only held by one person and the decryption key is publicly known, the text that person encrypts can be used as their electronic signature, given that only they can create it but everyone can recognize it.

Taking this one step further, if we take an electronic document and we apply an algorithm to it in such a way that it allows us to obtain a short code depending on the contents of the document (rather like the essence of the document, or its fingerprint, meaning that, if any aspect of the document changes, the result does too) and we encrypt the short code with the private key, then we obtain an electronic signature that makes it possible to check whether any changes have been made to the document.

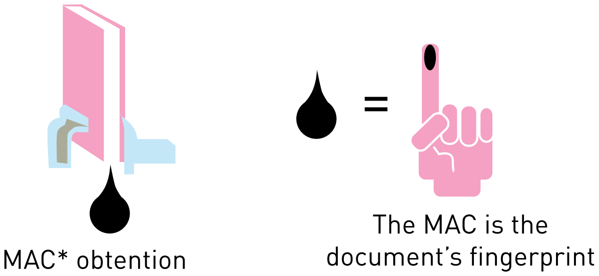


Fig. 24. Analogy of the message authentication code as a document's fingerprint.

"Hash" or "MAC" is a function that calculates a dependent value of the document on which it is being calculated, and which is different for different documents, however small this difference may be.

This code is often called the HASH or MAC (Message Authentication Code) function, and is calculated at the time the signature is made, and also when it is to be verified.

The result of the electronic signature algorithm and the decryption must match: the short code makes it possible to check that nobody has modified the document used as the basis for the electronic signature to be produced.

Apparently, the problem of making and verifying the electronic signature has been solved, but one essential element is still necessary: the **certification service provider.**

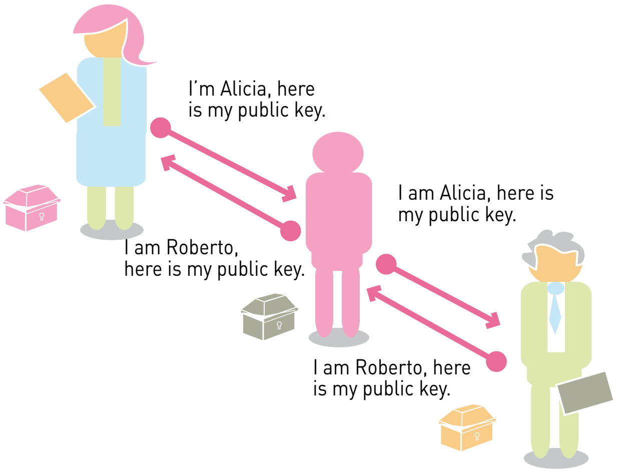


Fig. 25. "Man-in-the-middle" problem

This problem needs to be solved, even though its more theoretical than real.

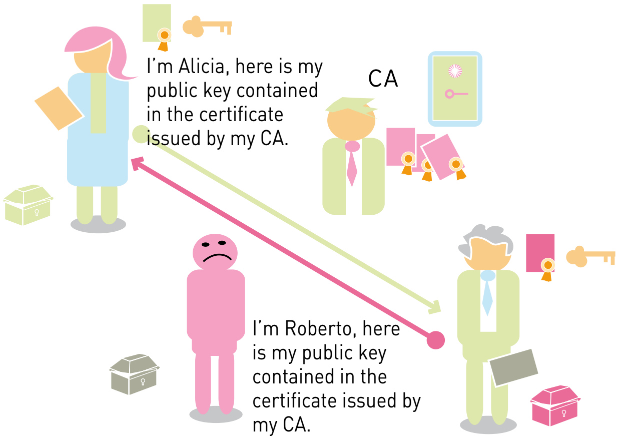


Fig. 26. Role of Certification Authorities.

An attack by the "man-in-the-middle" is no longer possible, because he or she cannot access the Certification Authority's private key, and so cannot forge the certificates.

In order to understand this need, we can consider the case in which two people, Alicia and Roberto, exchange their public keys via a communications system.

It is possible that the messages are intercepted, and that both Alicia and Roberto are confused about their identities and keys. Once the keys have been exchanged by this attacker, he or she could decode and recode the messages without Alicia or Roberto being aware that their messages have been revealed and substituted by the attacker.

Certification service provider

An entity recognized by the parties, known as a certification service provider, exists to prevent messages being unlawfully intercepted by people who manage to penetrate the key exchange circuit.

The certification service provider receives a request from one of the parties to issue a certificate guaranteeing that their public key is theirs and theirs alone, and it carries out the necessary enquiries in order to do this, enabling it to confirm the applicant's identity. When it is sure about this identity, it issues a certificate containing all the identification details, which are inseparably linked to the applicant's public key. In the certificate, all these data are encrypted with the private key provided by the certification service provider.

Given that the public key provided by the certification service provider is known by all the parties, anyone can extract the data from the certificate. However, nobody can supplant the certification service provider by using false certificates, since they to not have access to its private key.

Once Alicia and Roberto have their respective certificates, they will no longer exchange the keys via the transmission means, but will rather exchange their certificates. Again, using the boxes analogy, the certification service provider provides notification of its public key in the newspapers (continuing with the analogy) and provides evidence that it is a trustworthy entity, meaning its certificates can be considered valid. It uses its box, encrypted with its private key, in order to provide the identity information certified. Among the data provided is the public key associated with the certificate's identity.

This means it is possible to obtain the public key from our partner, and to use this to recognize his or her signature or be able to send confidential messages.

When a party communicates his or her certificate to another party, he or she states the certification service provider used. The certification service

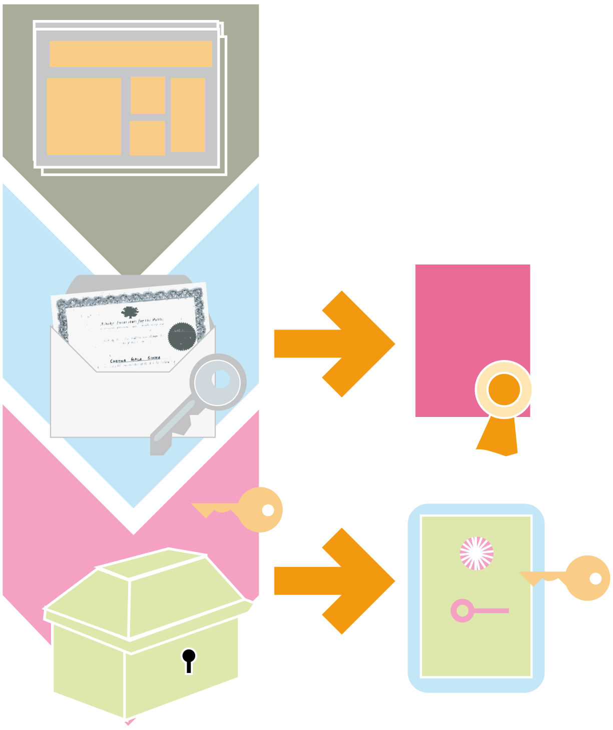


Fig. 27. Analogy of the keys managed by the Certification Service Providers (CSPs).

The CSP's public key is broadly available (as if published in a newspaper).Users' certificates are signed with its private key . The certificates are public documents (including their public key) linked to the user's private key (using the magician's box analogy), which it must safeguard diligently (illustrated by the analogy of the safe).

provider's public key should be known by everyone and it is the only key that needs to be previously known. Normally, it is incorporated in the electronic signature creation and verification software, or can be obtained from public dissemination systems, such as web servers.

Given the aforementioned, we see that the certification service provider must be a trustworthy entity (trusted third party), broadly known, with a certification policy that includes terms and conditions that are acceptable to all the parties, and which also permit, among other things, verification of identity, providing information on the use and validity of the certificates, and which handles revoked certificates (in order to prevent exposed private keys from being valid), and provides the list of certificates issued.

Given that there is more than one certification service provider in a network, selection of the most suitable certification service providers for each purpose will depend on the characteristics of their certification policy or on them being recognized by the entities accepting their certificates. Hierarchical systems are being developed in which all the certification authorities belonging to a particular hierarchy may carry out mutual certifications.

The parameters defining a certification service provider are its network address (an identified name) and its public key. It is also necessary to specify in its identification the certificate-issuing entity, the department or organization responsible for storing the private key and its location (city, country). Aspects such as the Tax Identification number or a registry reference are also desirable.

Registration entity

Given that special activities, must be carried out when the verification of the user identity is performed in the first certification, the certification service provider has an associated Registration Entity.

This registration entity keeps information on the relevant aspects of the registration and the identification procedures used, as well as the link between the registry and the identity guaranteed by the certification service provider.

There are also other kinds of registration entities, which prove that certain electronic actions have been carried out over time: certification before a notary of similar figure (as in the case of agreements executed before a notary public), accreditation certificates certifying sufficient legal capacity to operate or represent third-parties, registration of agreements or transfers of assets. Under current legislation on electronic administration, these are called electronic offices and one of their precedents was the account entry system used in the stock market.

Some of these entities carry out independent and additional activities apart from those rendered by certification service providers, which focus on the authentication of the parties and the related functions.

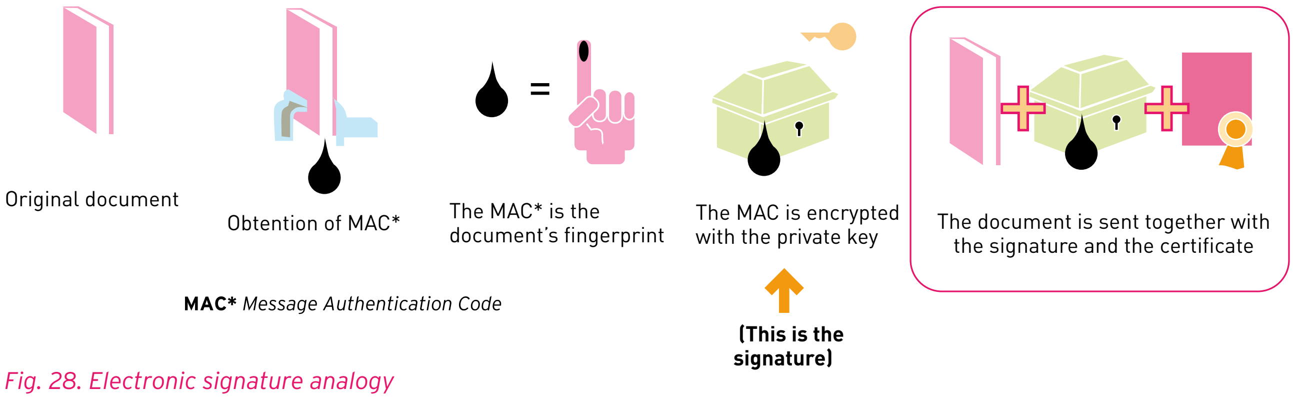

Original document
Obtention of MAC*
The MAC* is the document's fingerprint
The MAC is encrypted with the private key
The document is sent together with the signature and the certificate
MAC* Message Authentication Code
(This is the signature)

Fig. 28. Electronic signature analogy

The summary function is applied on the document (resulting in something similar to a fingerprint of the document) and is encrypted with the signatory's private key. The document, the certificate and the results of the previous operation are sent. This is the electronic signature. The electronic signature is different for each document, signed by the same user and the same document, if signed by different users.

The full picture

With all the elements described, it is already possible to have an idea on the way signing, verification process are carried out.

Signing process

The starting point is the original document for which the HASH (or MAC), is calculated, a unidirectional summary function, which identifies it unequivocally. The result of applying this function is encrypted with the certificate holder's private key (which, once again using the analogy, is placed in the "magician's box"). The result sent to the recipient comprises the **document**, the signed **hash** (or **MAC**) and the **certificate**.

Signature verification

The recipient receives the **document**, the signed hash and the certificate. The sender's public key. can be extracted from the certificate. Using this public key, the "magician's box" can be opened and, therefore, the hash originally calculated can be obtained. As we have the document, we can calculate its **hash** ourselves. When the two hashes are compared, the one calculated at origin may be the same as the one calculated at destination. If they do not match, this means that either the document or the signed hash has experienced some problem during transmission, which has affected its contents, therefore rendering the signature invalid.

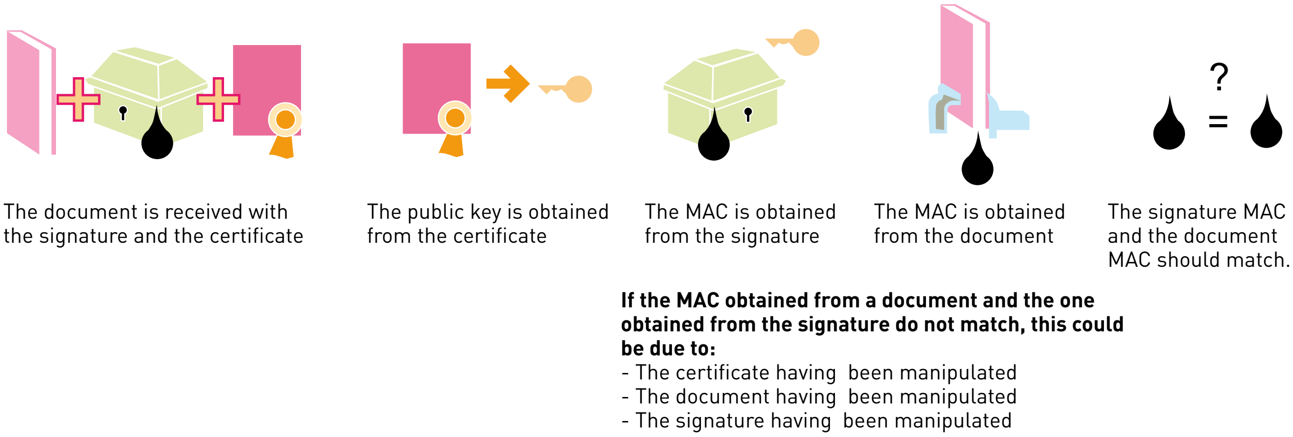

The document is received with the signature and the certificate
The public key is obtained from the certificate
The MAC is obtained from the signature
The MAC is obtained from the document
?
=
The signature MAC and the document MAC should match.
If the MAC obtained from a document and the one obtained from the signature do not match, this could be due to:
- The certificate having been manipulated
- The document having been manipulated
- The signature having been manipulated

Fig. 29. Verification of the electronic signature.

The signatory's public key can obtained from the certificate, which can be used to decrypt the signature to obtain the result of the summary function applied by the signatory. Also, by applying the same algorithm to the document, the summary function is calculated once again. Both values, the original and the one obtained at the destination, should be the same.

Security functions

An electronic signature system makes it possible to fulfil the following safety functions:

- Integrity,
- Signatory identification (attributability),
- Proof of agreement with the contents signed (consent provision),
- Time of signing

There are also other security principles to be satisfied, according to the characteristics of the certificate and the protocol used, such as availability, auditability, reliability, confidentiality, detection of messages missing in a sequence, sufficient capacity to perform the function and legal evidence

Integrity

The contents of the messages cannot undergo any accidental or intentional changes after being signed.

Signatory identification

It is possible to know who issued the message and their main attributes.

Proof of agreement with the contents signed

The signatory agrees with the contents of the document, or is in some way linked to it (as its author, reviewer, or by confirming knowledge of it, etc).

Time of signing

If the signature is carried out correctly, incorporating reliable information on the time, this proves that the document already existed before the particular moment given as the time of signing.

Storage of keys and secure signature creation devices

An important aspect in the electronic invoicing environment involving the use of digital certificates relates to the storage of the private key associated with the public key and the certificate used for signing invoices.

What is commonly known as the digital certificate actually comprises three important elements:

1. The private key: this is a key generated randomly from mathematical algorithms of a certain length. Currently, the algorithm RSA and 1024-bit keys are usually used for personal keys. This key must be known and managed by its user only.

2. The public key: this key is generated based on the previous one, even though it is extremely difficult to work out the private key once this public key is known. The purpose of this key is to be exchanged, therefore it is public in nature.

3. The public key generated is incorporated, together with the certificate user's details (name, DNI, company, etc.), with a document created under standard X509 v.3. This document is signed by the certification service provider, thereby certifying the authenticity of all the data contained in it. This document signed by the certification service provider is the digital certificate.

The security of the signing system is thus based on protection of the private key. This key can be stored in different ways:

1. Plain-text storage: The private key is stored on the disc without any protection, except, where relevant, the normal protection used for sensitive files.

2. Storage in special repositories: Microsoft has its own key and certificate manager, which allows the private key to be protected with a password. The main problem with this is the dependence on a platform and the lack of security in the process.

3. PKCS#12 / PEM Storage: files containing the private key, the public key and the certificate. The private key can be password-protected.

4. Storage on memory cards: some chip memory cards allow keys and certificates to be stored and retrieved. Their main advantage is that they are portable, while their disadvantage is that the cryptographic operations are not performed on the card.

5. Storage on cryptographic tokens: cryptographic cards are portable just like the

memory card, but cryptographic operations are performed on the card itself, meaning the private key never leaves it.

6. HSM (Hardware Security Module) storage: the cryptographic hardware has the same functionality as the tokens, but this is optimized to make it possible to carry out batch processes. It is advisable to use these when many cryptographic operations are being performed and the system is to be given a high level of security. It can also include cryptographic accelerators, which optimize its functionality.

In order to use signature keys, it is absolutely advisable to use some kind of HSM Cryptographic Hardware, given its greater efficiency (in terms of speed and security) as opposed to the software storage alternative.

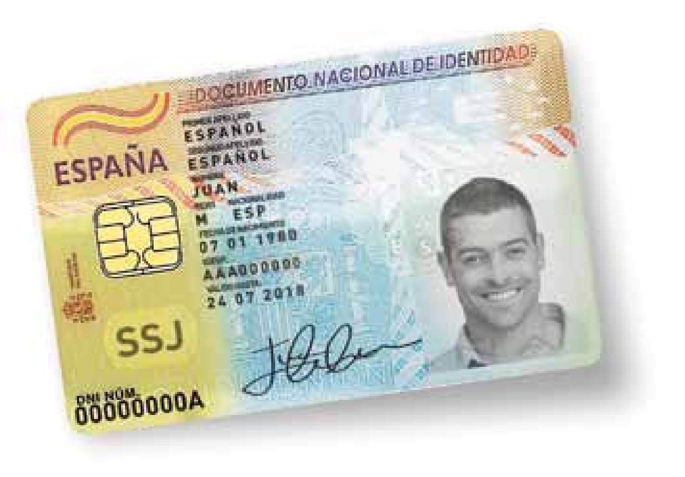


Fig. 30. The electronic DNI is considered a secure signature creation device

The means to be used will depend on the scope of the project, although we should bear in mind that the legislation on electronic signatures requires the use of secure signature creation devices to generate qualified signatures.

Annex II.

Annex II. Legal framework for electronic signatures and invoicing

Legal validity of electronic invoicing

Electronic invoicing is fully legal in all European countries. The applicable rules, fundamentally, are the following:

- Directive 1999/93/EC of the European Parliament and Council, of December 13, 1999, on a Community framework for electronic signatures.
- Directive 2006/112/EC of the European Council, of November 28, 2006, on the common system of value-added tax. The text for the future regulation that will amend this directive and that is to be transposed to national legal systems by 1 January 2013, has been approved.
- Law 37/1992, of December 28, on ValueAdded Tax.
- General Tax Law 58/2003, of December 17.
- Law 59/2003, of December 19, on the Electronic Signature.
- Organic Law 15/1999, of December 13, on the Protection of Personal Data.
- Law 1/2000, of January 7, on Civil Procedure.
- Law 53/2002, of December 30, on Tax, Administrative and Social Measures (Article 164).
- Law 1/2000, of January 7, on Civil Procedure.
- Law 11/2007[1], of June 22, on the electronic access of citizens to public services
- Law 30/2007, of October 30, on Public Sector Contracts.
- Law 56/2007, of December 28, on Measures to Promote the Information Society.
- Royal Decree 1624/1992, of December 29, approving the Value-Added Tax Regulations, and amending Royal Decree 1041/1990, of July 27, on census declarations, Royal Decree 338/1990, of March 9, on the Tax Identification Number; Royal Decree 2402/1985, of December 18, on the obligations related to issuing and delivering invoices (for businesses and self-employed professionals), and Royal Decree 1326/1987, of September 11, on the application of EU Directives.
- Royal Decree 1496/2003, of November 28, approving the Regulation governing invoicing obligations, and amending the Regulation on Value-Added Tax.
- Royal Decree 87/2005, of January 31, amending the Regulation on Value-Added Tax, approved by Royal Decree 1624/1992, of December 29, the Regulation on Special Taxes, approved by Royal Decree 1165/1995, of July 7, and the Regulation governing invoicing obligations, approved by Royal Decree 1496/2003, of November 28.
- Royal Decree 1553/2005, of December 23, regulating the issuing of national identity and electronic signature certificates.
- Royal Decree 1065/2007, of July 27, approving the General Regulation of tax management and inspection actions and proceedings, and implementation of common rules on tax application procedures.
- Royal Decree 1720/2007, of December 21, approving the Regulation implementing Organic Law 15/199, of December 13, on the protection of personal data.
- Royal Decree 2126/2008, of December 26, amending the Regulation on Value-Added Tax, approved by Royal Decree 1624/1992, of
- December 29, as well as the General Regulation of tax management and inspection actions and

[1] Spanish legislation can be found and downloaded from the website of the Official Spanish Gazette (BOE) (http://www.boe.es/aeboe/ consultas/bases_datos/iberlex.php), EU legislation can be found and downloaded from the Eur-Lex portal (http://eur-lex.europa.eu/es/index.htm), and specific regulations issued by ministry departments can be downloaded from the legislation section of the 060 website (http://legislacion.060.es/). A legislative index can also be accessed, among other information relating to electronic invoicing, on the Spanish Government's electronic invoicing website: http://www. facturae.es/es-ES/Documentacion/Normativa/Paginas/FacturaElectronica.aspx.

proceedings, and implementation of common rules on tax application procedures, approved by Royal Decree 1065/2007, of July27.

- Royal Decree 1671/2009, of November 6, partially implementing Law 11/2007, of June 22, on the electronic access of citizens to public services, Royal Decree 1/2010, of January 8, amending certain tax obligations and tax application procedures and other tax related rules.
- Order HAC/1181/2003, of May 12, establishing specific rules on the use of the electronic signature in fiscal relationships with the Spanish National Tax Agency, by electronic, computer, and telematic means.
- Resolution, of 24 July 2003, of the Directorate General of the National Tax Agency, establishing the procedure to be followed in accepting certificates issued by electronic certification service providers.
- Order EHA/962/2007, of April 10, developing certain provisions on electronic invoicing and the retention of invoices, contained in Royal Decree 1496/2003, of November 28, approving the regulation governing invoicing obligations.
- Order PRE/2971/2007, of October 5, on the issuance of invoices by electronic means when the recipient of said invoices is the Public Administration or other public entities linked to or dependent on the Public Administration, and on the submission of invoices exchanged between individuals before the Public Administration and its related or dependent public entities.
- Resolution of 24 October 2007, issued by the National Tax Agency, on the procedure for approving digitalization software provided for in Order EHA/962/2007, of April 10, 2007.

Provincial governments with their own legislative capacity have published equivalent regulations, applicable in their regional area, that are practically identical to the regulations applicable in the rest of the country.

Spanish companies are legally obliged to issue and deliver invoices or substitutive documents, in the cases required by law, in relation to all the commercial transactions they carry out as part of their business.

This legal duty is accompanied, where relevant, by the obligation to comply with current legislation on electronic invoicing, in particular Articles 6 and 7 of the Regulation governing the invoicing obligations approved by RD 1496/2003, which indicate, as minimum obligatory requirements, the information that should be contained both in the invoices issued and copies of them:

- **The invoice number**, and, if applicable, **serial number.** The use of different series numbers gives the various invoicing modalities, including self-invoicing and third-party invoicing, a high degree of flexibility.
- **Issue date.** In some cases, this date will match the date of delivery of the goods or service provided, but if it does not, the delivery date may not exceed the deadline established by law.
- **Name** and surnames, or **registered company name**, both of the invoice issuer and recipient.
- The invoice should indicate the corporate name under which the company is registered. In other words, for validity verification purposes, the invoice should contain the full name as registered in the deed of incorporation held by the Commercial Registry, with no trade names or any abbreviations being valid except those abbreviations that, for technical reasons, are too long to allow the full name to be registered and are commonly accepted, such as S.A., S.L., SC, etc. (Spanish equivalents of Plc., Ltd., etc.).
- **Tax Identification Number (NIF).** By virtue of Directive 2001/115/EC, companies must add the letters ES before the Tax Identification Number conferred by the Tax Agency (according to international standard ISO-3166 alfa2, which is used to identify the member state that has assigned the tax identification number).
- **Physical address** of taxable persons, both the issuer and the recipient. This does not have to be the same as the place of delivery of the goods or services. This information can be included in the invoice, but it is not an essential requirement for it to be valid.
- **Description of transactions**, highlighting the manner and date of delivery of the goods or provision of the service.
- If the information contained in delivery notes is used in order to fulfill this requirement, this should be mentioned in the relevant invoice, clearly indicating the corresponding delivery note, which should be kept duly attached to the invoice. This is due to the delivery note being considered a supporting document for the transactions carried out, in other words the fact it is considered as an integral part of

the invoice to which it is attached, and it will be subject to the same retention requirements obligations as this invoice.

- If the invoice recipient is a business owner or professional, all the transactions carried out on different dates within a calendar month can be grouped together in a single invoice.
- Similarly, this kind of grouping of items in a single invoice can also be carried out on the various transactions carried out with the same provider if the issuer is a tax payer (VAT).
- The **tax rate or rates** applicable to transactions. Or an express indication of the reason for VAT exemption or non-application of VAT, if applicable.
- **Tax amount** deducted.

It is worth noting that the new European legislation will be more flexible, in permitting several mechanisms that guarantee the authenticity and integrity of electronic invoices.

Legal aspects of the electronic signature

A rule concerning the implementation of electronic invoicing is Law 59/2003 on the Electronic Signature, which establishes that the qualified electronic signature is equivalent to a handwritten signature, and states that the legal recognition of any electronic signature, whether the simple or advanced kind, cannot be refused because it is submitted in electronic format. This law is the transposition of Directive 1999/93

There are great technical variations in carrying out the electronic signature. Directive 2006/112, which regulates electronic invoicing at a European level, establishes that any electronic signature should be advanced, with member states able to demand that they be qualified, as is the case in Spain. The new text that will amend the Directive will encompass the advanced electronic signature in the sense of point 2 of Article 2 of Directive 1999/93/EC of the European Parliament and the Council, of December 13, 1999, establishing the Community framework for electronic signatures, based on a qualified certificate, and created by a secure signature creation device, in line with points 6 and 10 of Directive 1999/93/EC.

When electronic invoicing is performed, the simplest way of giving the electronic document that contains it legal validity is to incorporate an electronic signature into it. Article 18 of Royal Decree 1496/2003 expressly establishes that an **advanced** electronic signature will be valid, in line with the provisions of Article 2.2 of **Directive 1999/93/EC** of the European Parliament and of the Council, of 13 December 1999, establishing a Community framework for the electronic signature based on a qualified **certificate** and created with a **secure signature creation device**, in compliance with the provisions of sections 6 and 10 of Article 2 of this Directive.

In other words, any qualified certificate is valid. The nature of the certificate is established in technical rules deriving from the Directive. This type of certificate is specifically designed to be issued to natural **persons**.

The qualified certificate confers the signature with the highest level of security in the hierarchy established by Law 59/2003, on the Electronic Signature:

The electronic signature (simple) is the set of data in electronic format, combined with other data or associated with them, which can be used as a way of identifying the signatory (of the associated data).

The advanced **electronic signature** makes it possible to identify the signatory and detect any further change in the information signed, which is exclusively linked to the signatory and the associated data, and which has been created in a way that the signatory can keep under their exclusive control. In other words, it has been produced using public-key cryptography and with a supporting electronic certificate.

The qualified electronic signature is an advanced electronic signature based on a qualified certificate and generated by using a secure signature creation device. The recognized electronic signature has the same value as regards electronically-contained data as a handwritten signature does for information written on paper.

The recognised electronic signature is often also called qualified, based on the term qualified certificate used in the Directive, and which was in the end translated in Spanish as "reconocido" ('recognised').

For example, we can say that a computerised handwritten signature, incorporated to a document, can be considered a **simple** electronic signature. The identification of a user by means of a username and key (password), or by means of a

PIN, as for credit cards, is also considered a form of simple electronic signature.

A variation of the **advanced** electronic signature uses public-key cryptography and a verification code for the document contents, such as, for example, the one used in e-mails. In this case, even if the certificate used has not been following a strict identity verification process, the basic presumptions required by the regulation are still complied with. The use of cryptographic systems, such as PGP, also fulfils these requirements.

Strict identity checks fufil one of the formal requirements for the **qualified certificate**, although this is not the only one. This means that sub-levels of advanced electronic signature can sometimes be established, according to the strictness of the certification service provider (or its registration entities–registration authorities) when issuing the certificate (i.-claimed identity, ii.-verified e-mail address, iii.-details indirectly verified through association with other information, iv.-details indirectly verified through pre-existing relationship, v.-remote submission of documents and evidence).

When the signatory's details are verified in person, and other formal requirements are fulfilled, the certification service provider is ready to issue recognized certificates, which – together with the secure signature-creation devices – generate the qualified electronic signature.

The general rule is to use **personal certificates as far as possible** (so they will be accepted anywhere in Europe).

Among these personal certificates, those including a reference to the company in which the individual renders his or her services in their coding is to be preferred. It is even better to use **representation certificates** which have been obtained with a power of attorney limiting their use to the signing of invoices.

Article 7 of Law 59/2003, of December 19, on the Electronic Signature, expressly regulates the electronic certificates for legal entities.

Although by means of a legal fiction, legal persons' legal personality and capacity to operate is recognized in legal proceedings. These powers can only be effectively exercised through the intervention of a natural person acting on the entity's behalf, as set out in Article 35 and subsequent articles of the Spanish Civil Code.

However, the Law on the Electronic Signature introduces a new development, the possibility for legal entities to sign for themselves, thereby linking them to the transactions they have carried out by telematic means.

To make this possible and valid, the signature creation information must be stored by the applicant natural person, whose details are included in the electronic certificate and who takes on the responsibilities established by law.

The intervention of the legal persons' representatives is a clear example of so-called necessary representation. This representation results from a public document being granted that recognizes a particular natural person as the legal representative of a specific legal person.

Law 59/2003, of December 19, on the Electronic Signature, governs representation certificates (Articles 11.4, 13.3 and 23.2), the contents of which should expressly mention the public document certifying the signatory's powers.

The legal regime applicable to this type of certificate is similar to that established by general legislation in relation to other kinds of representation.

Representation certificates are ideal for using and developing electronic invoicing systems.

Order EHA/962/2007 clarifies that any other advanced electronic signature, based on a qualified certificate (from any EU certification service provider, in accordance with national legislation deriving from Directive 1999/93) and generated using a secure signing device (which Article 3.3 of Law 59/2003, on the electronic signature, calls the qualified electronic signature) is fully valid.

By virtue of Order **HAC/1181/2003**, the certificates on the AEAT website (www.agenciatributaria.es), where the electronic certificate-issuing entities can be found, are valid (http:// www.agenciatributaria.es/wps/portal/DetalleContenido?&content=c60501ae9dc89010VgnVCM1000004ef01e0aRCRD&channel=6c1ce5e17736e110VgnVCM1000004ef01e0a____&ver=L&site=56d8237c0bc1ff00VgnVCM100000d7005a80____&idioma=es_ES).

Since 20 March 2004, when Law 59/2003 on the Electronic Signature came into force, the Ministry of Industry, Tourism and Trade has been responsible for carrying out censuses of certification service providers. The list of these can be obtained by searching the Ministry of Industry, Tourism and Trade website (www.mityc.es), with the electronic signature certification service providers to be found at (http://www.mityc.es/dgdsi/es-ES/Servicios/FirmaElectronica/Paginas/Prestadores.aspx).

Also, any certificate which is codified to indicate that it is qualified according to the standards **TS 101 862 and RFC 3739** (recognized certificate profile) is valid, which presupposes that the CSP complies with the following standards:

- **TS 101 456.** Policy requirements for CSPs issuing qualified certificates.
- TS 102 **042.** Policy requirements for CSPs issuing public key certificates.

In other words, as expressly established in Royal Decree 1496/2003, and Article 4 of Order EHA 962/2007, certificates issued by any provider that are in line with the legal framework deriving from Directive 1999/93/EC, are suitable.

According to Article 11 of this Directive, CSPs operating in Europe can be identified by searching the European Commission website on the page "Notification procedure Article 11 of Directive 1999/93/EC"
(http://ec.europa. eu/information_society/policy/esignature/eu_ legislation/notification/index_en.htm).

Annex III.

Annex III. Related links

- Spanish Government Electronic Invoicing website (Ministry of Economy and Finance, and Ministry of Industry, Tourism and Trade):
http://facturae.es/

- Electronic signing website of the Ministry of Industry, Tourism and Trade:
http://www.mityc.es/dgdsi/es-ES/Servicios/FirmaElectronica/

- Electronic DNI website of the Ministry of Home Affairs:
http://www.dnielectronico.es

- Information on the UBL format on OASIS:
http://www.oasis-open.org/committees/ubl/

- Information on UN/CEFACT:
http://www.unece.org/cefact/

- Information on the CEN BII (Business Interoperability Interfaces for Public procurement in Europe) specifications:
http://spec.cenbii.eu/
http://www.cen.eu/CEN/sectors/sectors/isss/activity/Pages/ws_bii.aspx

- Information on CEN Workshop on e-Invoicing:
http://www.cen.eu/CEN/sectors/sectors/isss/activity/Pages/einvoicing_2.aspx

- Website containing information on invoicing systems in Europe developed by CEN/CENELEC:
http://www.e-invoice-gateway.net/

- Information on electronic invoicing on the European Commission website:
http://ec.europa.eu/internal_market/payments/einvoicing/index_en.htm