

Facturació electrònica

Josep Lluís Ferrer Gomila

Llorenç Huguet Rotger

M. Magdalena Payeras Capellà

PID_00199770

Els textos i imatges publicats en aquesta obra estan subjectes –llevat que s'indiqui el contrari– a una llicència de Reconeixement-NoComercial-SenseObraDerivada (BY-NC-ND) v.3.0 Espanya de Creative Commons. Podeu copiar-los, distribuir-los i transmetre'ls públicament sempre que en citeu l'autor i la font (FUOC, Fundació per a la Universitat Oberta de Catalunya), no en feu un ús comercial i no en feu obra derivada. La llicència completa es pot consultar a <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca>.

Índex

Introducció	5
1. Requisits legals	9
2. Factura electrònica: signatura i certificats reconeguts	13
2.1. Infraestructures de clau pública: PKI	13
2.2. Els certificats electrònics	16
2.3. La signatura electrònica	17
2.4. Esquema de la signatura electrònica	18
2.5. Format XML de signatura en facturació electrònica	22
3. Els sistemes de facturació electrònica	27
3.1. Requisits de totes les factures	28
3.2. Obligacions legals per a l'emissor	28
3.3. Obligacions legals per al receptor	29
3.4. Conservació electrònica de les factures	30
3.5. Procediments d'emissió i recepció de factures electròniques ..	32
4. Descripció d'un cas real	36
4.1. Reflexions sobre la implantació d'una solució de facturació electrònica	37
4.2. Implantació d'una solució de facturació electrònica: cas real .	39
Exercicis d'autoavaluació	45
Bibliografia	46

Introducció

La facturació electrònica es preveu, des de 2007, com un dels objectius de la Llei d'impuls de la societat de la informació (LISI, 56/2007), i trasllada a les empreses el repte de la seva implantació. Aquesta llei, defineix la factura electrònica com: “un document electrònic que compleix els requisits exigibles legalment i reglamentàriament a les factures i que, a més, garanteix l'autenticitat de l'origen i la integritat del contingut de la factura, la qual cosa impedeix que l'emissor la rebutgi”.

L'empresa del segle XXI s'ha d'adaptar al desenvolupament de les tecnologies de la informació per a ubicar-se al bell mig de la societat de la informació, on, en particular, Internet els ofereix molts serveis que permeten treballar telemàticament i, gràcies a l'impuls normatiu que dóna cobertura jurídica, d'una manera més professional, flexible i dinàmica; oferint-los, alhora, un estalvi de temps i de costos de gestió documental prou significatius.

Des de sempre, una factura és el justificant fiscal del lliurament d'un producte o de la provisió d'un servei, que afecta l'obligat tributari emissor (el venedor) i l'obligat tributari receptor (el comprador). Tradicionalment és un document en paper, l'original del qual ha de ser arxivat pel receptor de la factura. Habitualment, l'emissor de la factura conserva una còpia o la matriu, en la qual es registra la seva emissió.

Aquest és un procés basat en la manipulació d'una gran quantitat de papers que juntament amb el seu processament comptable manual suposen un llast per a la competitivitat de l'empresa.

La factura electrònica és l'equivalent digital de la factura en paper. La facturació electrònica, (també ens hi referirem com a **e-facturació**) consisteix en la transmissió de les factures, o documents anàlegs, entre emissor i receptor per mitjans electrònics (fitxers informàtics) i telemàtics (d'un ordinador a un altre), **signats electrònicament amb certificats reconeguts**, la qual cosa garanteix l'**autenticitat** del seu origen i la **integritat** del seu contingut.

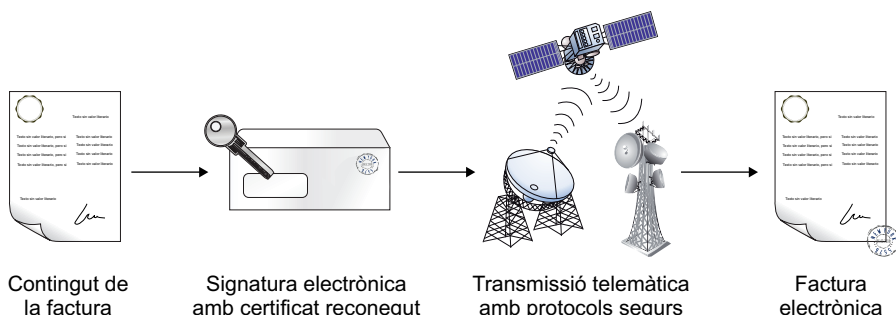
Els certificats reconeguts han de seguir els estàndards del sector de normalització de la Unió Internacional de Telecomunicacions, UIT-T (abans, el Comitè Consultiu Telefònic i Telegràfic CCITT)), en particular el protocol X.509v3, o d'una versió superior, que han de ser admesos per una autoritat de certificació que participa en les relacions tributàries per mitjans electrònics i telemàtics amb l'Agència Estatal d'Administració Tributària (AEAT).

El gràfic següent mostra el procés de facturació electrònica:

Observació

La factura electrònica té la mateixa validesa legal que la factura emesa en paper.

Factura tradicional	Factura electrònica
Paper	Fitxer electrònic
Signatura normal	Signatura electrònica + Certificat electrònic reconegut
Enviament postal	Transmissió telemàtica



Es pot considerar la factura electrònica com un document tributari generat per mitjans informàtics en format electrònic, que reemplaça el document físic en paper, però que conserva el mateix valor legal amb unes condicions de seguretat (autenticitat i integritat) que no es donen en la factura en paper. Aquest valor legal permet atribuir a la factura electrònica l'obligació tributària de l'emissor.

Entre els molts avantatges de la facturació electrònica trobem:

- **Estalvi de costos i millora de l'eficiència. Control d'accions errònies.** Encara que és difícil avaluar el cost global associat a la facturació en paper, és evident que en la facturació electrònica es redueixen els costos del paper, els d'impressió, els de manipulació (tasques d'ensobriment, emmagatzematge en fitxers i carpetes físiques) i d'enviament per correu postal, entre d'altres. D'altra banda es pot considerar que la interacció electrònica i telemàtica durant tot el procés, ajudarà a la millora de l'eficiència i al control d'errors. Com que el procés administratiu es pot automatitzar, es redueixen les tasques més reiteratives i així també es redueixen els errors humans.
- **Major seguretat en el resguard dels documents i menor probabilitat de falsificació.** L'ús de certificats electrònics reconeguts ofereix a les factures les garanties d'autenticitat de l'emissor i d'integritat de la factura, que disminueixen enormement les probabilitats de falsificació.

L'automatització del procés d'emmagatzemament de les factures fa que augmenti la seguretat dels documents guardats, alhora que en facilitarà la recuperació.

- **Integració amb les aplicacions de gestió internes de l'empresa. Facilitat en els processos d'auditoria.** L'intercanvi electrònic de factures permet reduir el temps de gestió de les factures d'una manera considerable, sobretot

Millora mediambiental

La factura electrònica, en substituir la factura emesa en paper, aporta uns beneficis mediambientals innegables:
1 tona de paper = 15 arbres + 250m³ d'aigua.

si es poden integrar en els ERP (*Enterprise Resource Planning*) de l'emissor per a la generació de factures i integrar les factures a l'ERP del receptor, per a la seva gestió, mitjançant formats estàndard estructurats.

La facturació electrònica permet una administració i comptabilitat automatitzades, la qual cosa comporta una reducció de temps de gestió i aporta moltes facilitats en els processos d'auditoria, ja que permet, de manera ràpida, verificar en quin estat es troba una factura i tota la informació que hi està associada (albarans, cobraments, pagaments, etc.).

ERP *Enterprise Resource Planning*

Els sistemes de planificació de recursos empresarials són sistemes de gestió d'informació que automatitzen moltes de les pràctiques de negoci associades als aspectes operatius o productius d'una empresa.

- **Optimització de la tresoreria. Ús eficaç dels recursos financers.** La facturació electrònica permet accedir als serveis avançats de finançament i pagament que ofereixen les entitats financeres com ara el facturatge electrònic (*e-factoring*) o confirmació electrònica (*e-confirming*).

Facturatge electrònic

És una modalitat de facturatge (fórmula de finançament basada en la cessió de factures a un tercer, a canvi d'uns costos derivats de l'avançament del pagament de les factures abans del seu venciment) en què el document cedit correspon a una factura electrònica i les transaccions que es fan entre el client, el deutor i el tercer (generalment una entitat financera) són totalment en línia.

Confirmació electrònica

És un servei que ofereix una entitat financera per tal de facilitar als seus clients la gestió del pagament de les compres que fan, amb la finalitat que el proveïdor pugui cobrar les factures abans de la data de venciment. Realment és un servei de gestió de pagaments i no de deute.

- **Eliminació d'espais per a emmagatzemar documents històrics. Agilitat en la localització d'informació.** Si abans ens hem referit a l'estalvi de costos de paper, és bo recordar que amb la facturació electrònica es redueix substancialment la necessitat d'espai físic que es necessita per a guardar les factures en paper al mateix temps que es millora la localització de la factura i de tota la informació que en fa referència.

Per a la realització de la factura electrònica és imprescindible considerar els requeriments següents:

- 1) Utilitzar un format electrònic de factura, que sol ser: EDIFACT, XML, PDF, HTML, DOC, XLS, TXT, etc.
- 2) Disposar d'un sistema de transmissió telemàtica: la factura electrònica ha de partir d'un ordinador i ser recollida, per al seu procés, per un altre ordinador. El mitjà telemàtic per a l'enviament del fitxer signat, que és un únic fitxer que conté la factura i la signatura reconeguda, és lliure; és a dir, es pot utilitzar el correu electrònic, un FTP (*File Transfer Protocol*), una pàgina web des de la qual es pugui descarregar la factura o enviar-la mitjançant un servei web (*Web service*).
- 3) Disposar de programari per a dur a terme la signatura electrònica reconeguda, o avançada, per tal de garantir la integritat i l'autenticitat, tant del document electrònic com de la transmissió telemàtica.

FTP

Es tracta d'un protocol de xarxa per a la transferència d'arxius que es basa en l'arquitectura client-servidor permetent que des d'un equip d'un usuari es pugui connectar a un servidor d'un altre (per exemple el d'un proveïdor) per a baixar-se'n arxius o per a pujar-n'hi, independentment del sistema operatiu utilitzat en cada equip.

1. Requisits legals

Per tal que l'ús d'Internet sigui segur, especialment en les transaccions que tenen o poden tenir contingut econòmic, s'han de poder garantir els requeriments següents:

- **Identitat:** Tenir la seguretat que s'està realitzant la transacció amb la persona / entitat desitjada.
- **Legitimació:** Conèixer si l'interlocutor està capacitat professionalment o legalment per a portar a terme la gestió o la transacció que està intentant realitzar.
- **Confidencialitat:** Tenir la seguretat que només l'empresa / administració i la persona / entitat amb la qual s'està realitzant la transacció poden accedir a la informació.
- **Integritat:** Tenir la seguretat que els documents que són motiu de la transacció siguin els originals; és a dir, els documents no han estat manipulats.
- **Autenticitat:** Tenir l'evidència de la realització d'un conveni, contracte, transacció, etc., amb els requisits suficients per a la seva validesa.
- **Autenticació:** Tenir la seguretat que l'interlocutor és realment el qui diu ser.
- **Disponibilitat:** Tenir garanties de poder accedir al document electrònic durant tot el temps i que aquest continuï tenint validesa jurídica.

Avui dia existeixen les eines necessàries i les garanties jurídiques per a poder garantir la confiança en les relacions per mitjà de la xarxa. Per tal de justificar el quadre legislatiu que dona empara a la facturació electrònica, des del punt de vista jurídic, podeu considerar les publicacions següents, tant d'àmbit espanyol com comunitari.

Normativa espanyola

A Espanya, s'aplica de manera general la Directiva de la Unió Europea 2001/115/CE (20/12/2001), on es defineixen els aspectes tècnics precisos perquè siguin vàlides, legalment i fiscalment, l'ús de les factures en suports electrònics.

També marca el deure de garantir l'autenticitat en origen (de l'emissor) i la integritat del contingut de la factura (dades). Aquesta Directiva està adaptada a l'ordenament nacional, principalment en aquestes normes:

- Ordre HAC/3134/2002 del Ministeri d'Hisenda i Administració (publicada al BOE, 13-12-2002), que desenvolupa el règim de facturació telemàtica, en la qual s'autoritza directament als sistemes que fan ús de la signatura electrònica basada en certificats reconeguts (derogada per l'Ordre EHA 962/2007).
- Resolució de l'AEAT 2/2003 (BOE 28-02-2003), de la Direcció general de l'Agència Estatal d'Administració Tributària (AEAT), sobre determinats aspectes relacionats amb la facturació telemàtica. En particular, admet, entre d'altres, els certificats reconeguts per l'FNMT (Fàbrica Nacional de Moneda i Timbre).
- Ordre HAC 1181/2003 del Ministeri d'Hisenda i Administració (publicada al BOE, 15-05-2003), per la qual s'estableixen normes específiques sobre l'ús de la signatura electrònica en les relacions tributàries per mitjans electrònics, informàtics i telemàtics amb l'Agència Estatal d'Administració Tributària.
- Reial decret 1496/2003 (BOE, 29-11-2003), pel qual s'aprova el Reglament que regula les obligacions de facturació, i es modifica el Reglament de l'Impost sobre el valor afegit. En particular, es regula la prestació dels serveis d'emissió i de conservació de les factures, per part de tercers.
- Llei general tributària 58/2003 (BOE, 18-12-2003) que constitueix l'eix central de l'ordenament tributari en el qual es recullen els seus principis essencials i es regulen les relacions entre l'administració tributària i els contribuents.
- Llei 59/2003 (BOE, 20-12-2003) de **signatura electrònica**, en la qual es regulen els diferents sistemes de signatura electrònica i altres serveis, i el seu nivell de valor legal. És un text millor adaptat a les necessitats dels prestadors i dels usuaris, que transposa la directiva europea. A més dóna un tractament especial al DNI electrònic i als certificats de persones jurídiques.
- Reial decret 87/2005 (BOE, 01-02-2005), pel qual es modifiquen el Reglament de l'impost sobre el valor afegit, aprovat pel reial decret 1624/1992, el Reglament dels impostos especials, aprovat pel reial decret 1165/1995 i el Reglament pel qual es regulen les obligacions de facturació, aprovat pel reial decret 1496/2003, en particular pel que fa les factures o documents substitutius rectificatius.
- Ordre EHA 962/2007 del Ministri d'Economia i Hisenda (BOE, 14-04-2007), per la qual es desenvolupen determinades disposicions sobre facturació telemàtica i conservació electrònica de factures, contingudes en el Reial decret 1496/2003, pel qual s'aprova el reglament que regula les obligacions de facturació (deroga l'Ordre HAC/3134/2002).

Facturació telemàtica

Aquest és el terme que es fa servir en aquestes normatives per tal d'indicar la facturació electrònica. Per tant, en aquest apartat hem respectat aquesta sintaxi.

- Resolució AEAT (BOE, 24-10-2007) de l'Agència Estatal d'Administració Tributària, sobre procediment per a l'homologació de programari de digitalització previst en l'Ordre EHA 962/2007.
- Llei 11/2007 (BOE, 23-06-2007) d'accés electrònic dels ciutadans als serveis públics. En la Llei s'explicita que és necessari que les administracions públiques garanteixin: la disponibilitat, l'accés, la integritat, l'autenticitat, la confidencialitat, la conservació de les dades, informacions i serveis; sota els principis de seguretat en la implantació i utilització de mitjans electrònics i del de proporcionalitat en relació amb les mesures de seguretat exigides i en relació amb les dades que es requereixin als ciutadans.

D'aquesta llei destaquen els 46 articles que fan referència a identitat digital, signatura electrònica, seguretat jurídica, indicant la importància que dona el legislador a aquests aspectes.

A aquesta llei s'hi fa referència amb l'acrònim LAECSP.

- Ordre PRE 2971/2007 (BOE, 15-10-2007) sobre l'expedició de factures per mitjans electrònics quan el destinatari d'aquestes sigui l'Administració General de l'Estat, o organismes públics vinculats que en són dependents i sobre la presentació davant l'Administració General de l'Estat, o els seus organismes públics vinculats o dependents, de factures expedides entre particulars.
- Llei 30/2007 (BOE, 31-10-2007) de contractes del sector públic. Aquesta llei té com a objecte regular la contractació del sector públic. Fa contínues referències a la utilització dels mitjans electrònics, informàtics i telemàtics en l'àmbit de la contractació pública, i sempre fent referència a aconseguir com a finalitat fer més fluides i transparents les relacions entre els òrgans de contractació i les empreses licitadores. En aquesta llei es posa en relleu la importància de la signatura electrònica, del segellament de temps i del document electrònic. A més es veu ben clar el motiu i la voluntat del legislador en què les administracions públiques impulsin la utilització d'aquests mitjans.

A aquesta llei s'hi fa referència amb l'acrònim LCSP.

- Llei 56/2007 (BOE, 29-12-2007) de mesures d'impuls de la societat de la informació, que defineix la factura electrònica com un document electrònic que compleix els requisits legal i reglamentàriament exigibles a les factures. Aquesta llei és d'alguna manera la LAESCP del sector privat, en la qual s'estableix l'obligació per a un conjunt d'empreses d'admetre els mitjans telemàtics, amb garanties jurídiques en les relacions amb els seus clients.

A aquesta llei s'hi fa referència amb l'acrònim LISI.

- Ordre PRE 2794/2011 (BOE, 18-10-2011), per la qual es determina el marc d'exercici de les competències estatals en matèria de factura electrònica, es crea el Fòrum Nacional Multilateral sobre facturació electrònica i s'impulsa el Servei Central de Gestió de la Facturació Electrònica en l'àmbit de l'Administració General de l'Estat.
- Reial decret 3/2011 (BOE, 16-11-2011) de text refós de la llei 30/2007 de contractes del sector públic.

Normativa Comunitària

- Directiva 1997/6/CE del Consell, de 17 de maig de 1977, en matèria d'harmonització de les legislacions dels estats membres relatives als impostos sobre el volum de negocis. Sistema comú de l'IVA: Base imposable uniforme. (Vigent a 15-05-2004).
- Directiva 1999/93/CE del Consell, de 13 de desembre de 1999, que té per finalitat facilitar l'ús de la signatura electrònica i contribuir al seu reconeixement jurídic, creant un marc jurídic, tant per a la signatura electrònica com per a determinats serveis de certificació electrònica per tal de donar seguretat jurídica a la comunicació i el comerç electrònics.
- Directiva 2001/115/CE del Consell, de 20 de desembre de 2001, per la qual es modifica la Directiva 77/388/CEE a fi de simplificar, modernitzar i harmonitzar les condicions imposades a la facturació en relació amb l'impost sobre el valor afegit.
- Directiva 2006/112/CE del Consell, de 28 de novembre de 2006, relativa al sistema comú de l'impost sobre el valor afegit.
- Directiva 2010/45/UE del Consell, de 13 de juliol de 2010, per la qual es modifica la Directiva 2006/112/CE, pel que fa a les normes de facturació.

Hi ha algunes normatives internacionals aplicables de manera general a la factura electrònica, encara que les Nacions Unides, per mitjà de la UN/CEFACT han publicat recomanacions com ara UNeDocs que defineixen plantilles per a les factures impreses i formats EDI i XML per a les modalitats electròniques. A Europa, la facturació electrònica es regula a la Directiva 2001/115, que havia de ser adoptada en cada país abans del 31 de desembre de 2003, tal com va succeir a Espanya.

Avui dia l'organització GS1 (abans EAN/UCC) ha organitzat comitès internacionals d'usuaris de 108 països membres, per a conformar les guies de facturació electrònica estàndard a escala mundial.

2. Factura electrònica: signatura i certificats reconeguts

En aquest apartat donarem unes nocions sobre la signatura electrònica per a la seva utilització en la factura electrònica, així com en les infraestructures que hi estan implicades.

2.1. Infraestructures de clau pública: PKI

En l'àmbit de la facturació electrònica és imprescindible garantir la identitat dels usuaris, a més dels serveis de seguretat: confidencialitat, integritat, autenticació i no repudi.

Perquè aquestes operacions es puguin realitzar de manera fiable s'han de complir dues condicions:

- Que la clau privada es custodii de manera segura i no es reveli a ningú. Per a aconseguir això, la clau privada s'emmagatzema en un suport físic impossible de duplicar, com una targeta intel·ligent. A més per a accedir al contingut de la targeta es necessita un número personal que només el seu posseïdor legítim coneix.
- Que es pugui determinar a quina persona pertany una clau pública. D'aquesta manera es pot saber, per exemple, qui ha dut a terme la signatura electrònica d'un document.

Per a donar compliment a aquesta darrera condició, s'utilitza el *certificat electrònic*, el suport tecnològic del qual és la criptografia de clau pública. Així es pot veure un certificat electrònic com un document electrònic que associa una clau pública amb el seu propietari.

Així el certificat electrònic contindrà la clau pública juntament amb dades de caràcter personal del posseïdor de la clau (nom, DNI...). Normalment conté més informació (dates de validesa i altres), així com també es refereix a l'àmbit d'utilització del certificat, el que es coneix com política de certificació. Per exemple, si és un certificat d'ús personal o ens acredita per a actuar en nom d'una empresa.

En realitzar una signatura electrònica se sol adjuntar el certificat electrònic del signant de manera que es pot extreure la seva clau pública per a verificar la signatura i alhora comprovar la identitat del signant.

Una infraestructura de clau pública (PKI, *Public Key Infrastructure*) és una estructura de sistemes informàtics, procediments d'operació, protocols, polítiques de certificació, repositoris d'informació, estàndards, declaracions de pràctiques i recursos humans la finalitat dels quals és oferir als usuaris una plataforma per a la gestió de la identitat digital.

Una PKI disposa dels elements i de l'arquitectura necessaris per a integrar tots els procediments de sol·licitud de certificats, verificació d'identitats, generació de claus, emmagatzematge i publicació de certificats electrònics, renovació, revocació, etc.

Les infraestructures de clau pública es fonamenten en la interacció de diferents subsistemes, dels quals destaquen els següents:

- **Autoritat de certificació, CA:** una autoritat de certificació (*CA: Certificate Authority*) és una entitat de confiança la finalitat de la qual és emetre, renovar i revocar certificats electrònics. Les autoritats de certificació constitueixen el nucli de les infraestructures de clau pública, que permet utilitzar els **certificats electrònics** amb total seguretat.
- **Autoritat de registre, RA:** una autoritat de registre (*RA, Registration Authority*) és una entitat encarregada de portar a terme els processos de verificació d'identitat, sol·licitud i distribució de certificats electrònics. Normalment, en una PKI els usuaris finals no interactuen directament sobre la CA, sinó que canalitzen les seves operacions per mitjà d'una o diverses RA. No obstant això, aquests subsistemes no poden expedir certificats electrònics per ells mateixos.
- **Certificats electrònics:** un certificat electrònic és un arxiu o document electrònic expedit i signat per una CA en el qual es vincula una identitat a una clau pública, vinculada, al seu torn, a la corresponent clau privada. Per a obtenir un certificat electrònic, l'usuari es dirigeix a una RA (autoritat de registre), la qual verifica la identitat de l'usuari i demana a la CA que expedeixi el certificat.
- **Sistemes gestors de certificats electrònics: la recomanació X.509:** l'auge de la certificació electrònica neix de la consolidació internacional del protocol estàndard X.509 de la ITU-T. Els sistemes gestors de certificats electrònics són el conjunt d'aplicacions que aprofiten els serveis de la identitat digital juntament amb els paquets de programari que implementen les funcions bàsiques d'una PKI. La seva implementació respon a tres categories: les integrades en el sistema operatiu, les lliures (de codi obert) i les comercials.
- **Directorí LDAP (*Lightweight Directory Access Protocol*):** la seva finalitat és la de mantenir un registre d'usuaris i actuar com magatzem per als certificats electrònics i la llista de certificats revocats (CRL). El protocol LDAP

Exemples de CA: Verisign, FNMT, CATCert...

En l'actualitat, un usuari pot escollir entre múltiples CA per a aconseguir un certificat electrònic, però les més utilitzades són a escala internacional *Verisign* (www.verisign.com), a escala estatal *FNMT* (www.fnmt.es) i en l'àmbit català *CATCert* (www.catcert.cat).

La recomanació X.509 de la ITU-T

Aquesta recomanació forma part de la sèrie de recomanacions X.500 del sector d'estandarització de telecomunicacions de la ITU (*International Telecommunications Union*), la finalitat de les quals és definir un servei de directori. Per directori s'entén un servidor o conjunt distribuït de servidors que gestionen una base de dades d'informació sobre usuaris. En l'actualitat, parlar d'X.509 i certificats electrònics és parlar del mateix concepte.

és una versió simplificada del protocol X.500 que especifica tant el model d'informació com els mecanismes d'accés a aquesta.

- **Llistes de certificats revocats (CRL) i el protocol OCSP:** una llista de Certificats revocats (CRL, *Certificate Revocation List*), és un document electrònic expedit i signat per una CA en el qual s'inclouen els números de sèrie de tots aquells certificats que, sense haver expirat, han estat revocats per algun motiu. La recomanació X.509 defineix un format estàndard per a les llistes CRL.

En rebre un certificat electrònic, l'usuari ha de consultar la CRL de la CA que signa el certificat per a verificar-ne la validesa. El protocol OCSP (*Online Certificate Status Protocol*) permet realitzar consultes en temps real sobre la base de dades de certificats revocats d'una CA. Alguns navegadors web ja inclouen suport per a OCSP.

- **Prestador de serveis de certificació, PSC:** el prestador de serveis de certificació és una entitat, reconeguda pels participants, que fa la gestió dels subsistemes de la PKI per a evitar la interceptació dels missatges per part d'un interlocutor il·legítim que s'insereix en el circuit d'intercanvi de claus. Evidentment, el PSC ha de ser una entitat de confiança (o també anomenada TTP, *Trusted Third Party*), la qual en la seva política de certificació ha d'incloure clàusules acceptables per als diferents interlocutors, que permeti, entre altres coses, la verificació d'identitat, que doni informació sobre ús i validesa dels certificats i que faci la gestió de certificats revocats i ofereixi la llista de certificats expedits.

El PSC rep la petició d'un participant perquè emeti un certificat que garanteixi que la seva clau pública és, precisament, la seva. Quan el PSC té certesa d'aquesta identitat, emet un certificat en el qual es recullen les dades d'identificació i, inseparablement, la clau pública del peticionari. En el certificat, totes aquestes dades van encriptades amb la clau privada del PSC. Atès que la seva clau pública és coneguda per tots els interlocutors, qualsevol és capaç d'extreure les dades del certificat. No obstant això, ningú és capaç de suplantar el PSC emetent certificats falsos, ja que per això hauria de disposar de la seva clau privada.

Els paràmetres que defineixen un PSC són la seva adreça de xarxa (nom distingit) i la seva clau pública. A més és necessari especificar en la seva identificació: entitat emissora del certificat, departament o organització responsable de la custòdia de la clau privada, i ubicació (ciutat, país...). També són importants aspectes com l'identificatiu fiscal i la o referència registral.

Validació de certificats

La validació de certificats en temps real és imprescindible per al desenvolupament de la factura electrònica.

2.2. Els certificats electrònics

Quant als certificats, per a qualsevol tipus d'empresa, podem distingir els quatre tipus següents:

- **Certificats de pertinença de persona física.** Aquest certificat permet que el titular s'identifiqui com a treballador d'una empresa, al mateix temps que garanteix la identitat de l'empresa de la persona física titular del certificat i la seva vinculació, en virtut del càrrec que hi ocupa. L'ús d'aquest certificat es restringeix únicament al titular, i la cessió del certificat és exclusivament responsabilitat seva.
- **Certificats de persona jurídica.** Aquest certificat identifica una empresa amb personalitat jurídica que es pot utilitzar sempre que s'admeti en les relacions que mantingui la persona jurídica amb les administracions públiques o en la contractació de béns o serveis que siguin propis de la seva activitat ordinària. La seva custòdia és responsabilitat de la persona física que el sol·licita; tot això, sens perjudici del fet que el puguin utilitzar altres persones físiques vinculades a l'empresa.
- **Certificats de persona física de representant.** Aquest certificat s'emet a favor d'una persona física representant d'una empresa que li permet actuar en nom de l'empresa a què pertany. El titular s'identifica com a persona física pertanyent a una empresa, alhora que hi afegeix la qualificació de representant legal de l'empresa. L'ús d'aquest certificat es restringeix únicament al titular, i la cessió del certificat és exclusivament responsabilitat seva.
- **Certificat de factura electrònica.** Aquest és exclusiu per a l'activitat de facturació. No permet fer cap altre tràmit, en nom de l'empresa, que no sigui la facturació electrònica, ni amb l'Administració ni entre empreses. Aquest certificat ofereix una seguretat extra en la signatura de factures, especialment per a les grans empreses que confien en el certificat a l'hora d'emetre factures electròniques. L'Agència Estatal d'Administració Tributària (AEAT) els certifica com a vàlids a l'efecte de la facturació electrònica i, segons el que disposa la directiva de la UE, estan vinculats a una persona i són vàlids per a emetre factures a l'estranger.

Pel que fa als certificats reconeguts, l'article 11.1, estableix que són els certificats electrònics emesos per un proveïdor de serveis de certificació que compleixi els requisits que estableix aquesta llei 59/2003, quant a la comprovació de la identitat i la resta de circumstàncies dels sol·licitants i quant a la fiabilitat i les garanties dels serveis de certificació que presta.

2.3. La signatura electrònica

Des del punt de vista tècnic, en el marc d'ETSI (*European Telecommunications Standards Institute*) es destaquen els tipus de signatura electrònica de rellevància legal:

- **Simple.** Constituïdes per dades que puguin ser usades per a identificar i autenticar el signant.
- **Avançada.** Quan, a més d'identificar al signant, permet garantir la integritat del document.
- **Reconeguda.** Quan és una signatura avançada, emparada per un certificat reconegut i realitzada amb un dispositiu segur de creació de signatura. Aquesta signatura també es denomina **qualificada**.

En el procés de signatura, s'usa un certificat d'usuari que garanteix l'autenticitat de l'emissor i una petjada, o empremta digital (normalment una funció *hash*), que garanteix la integritat. És a dir, en cas de modificació de la factura durant el procés telemàtic, la signatura és invàlidada pel programari del receptor.

La signatura avançada pot incloure més o menys informació, relativa al moment de creació o a la validesa dels certificats. La més senzilla recull els elements essencials de la signatura electrònica: el resum del document signat (*hash*), el certificat del signant associat a la clau pública del signant, i el resultat d'aplicar la clau privada del signant al resum, que és la signatura electrònica pròpiament dita.

D'altra banda, parlarem de **signatura datada** si s'afegeix a la signatura bàsica informació temporal sobre el moment de la signatura o de la seva verificació (segellament de temps o *time stamping*), i de **signatura validada** si s'afegix a la signatura datada informació sobre la vigència del certificat emprat en el moment de la signatura o de la seva verificació. La signatura validada es denomina també **signatura completa**, perquè inclou tots els elements que permeten comprovar que el certificat utilitzat pel signant estava vigent en el moment de la signatura, i permet així el seu emmagatzematge a llarg termini.

Tot i que les dades relatives, tant en el segellament de temps com en la revocació del certificat són de gran utilitat, i aporten un gran valor afeïgit al procediment de signatura, no són d'obligat compliment per a la validesa d'una factura electrònica.

L'article 3.2 de la Llei 59/2003 indica que la signatura electrònica avançada és la que permet identificar el signant i detectar qualsevol canvi posterior de les dades signades. Està vinculada al signant i a les dades a les quals fa referència de manera única i ha estat creada per mitjans que el signant pot mantenir exclusivament sota el seu control.

Lectura recomanada

Considerarem que es coneixen els algorismes de signatura electrònica, com ara RSA, DSA, etc. Però, per a aprofundir-ne es pot consultar el llibre: L. Huguet, J. Rifà, J. Tena. *Criptografia Avançada*.

Material docent de la UOC, PID_00185087.

hash o MAC

El *hash* o MAC (*Message Authentication Code*) és una funció resum que calcula un valor, sempre de la mateixa mida en número de bits, depenent del document sobre el qual es calcula i que és diferent per a diferents documents, tot i que la seva diferència sigui petita. Aquesta és una funció unidireccional, en el sentit que conèixer el resum no ens aporta informació del document, encara que identifica unívocament el document sobre el qual s'ha aplicat.

Segellament de temps

El segell temporal o *time stamping* garanteix el moment exacte en el temps en què s'ha produït la signatura d'un document. El servei de segellament temporal, que normalment fa una autoritat de certificació, permet a l'usuari acreditar el dia i l'hora en què ha rebut o enviat un arxiu informàtic, i això és fonamental en el cas de la factura electrònica o en el cas d'emmagatzematge temporal de documents digitals.

I en l'article 3.3 defineix la signatura electrònica reconeguda com la signatura electrònica avançada basada en un certificat reconegut (que compleixi els requisits establerts en aquesta llei quant a la comprovació de la identitat i altres circumstàncies dels sol·licitants) i generada mitjançant un dispositiu segur de creació de signatura.

La llei defineix aquests dispositius com els que ofereixen, almenys, les garanties següents:

- Que les dades utilitzades per a la generació de la signatura es poden produir només una vegada i assegurar raonablement el seu secret.
- Que hi ha una seguretat raonable que les dades utilitzades per a la generació de signatura no poden ser derivades de les de verificació de signatura o de la pròpia signatura. A més la signatura està protegida contra la falsificació amb la tecnologia existent en cada moment.
- Que les dades de creació de signatura poden ser protegides de manera fiable pel signant contra la seva utilització per tercers.
- Que el dispositiu utilitzat no altera les dades o el document que s'hagi de signar ni impedeix que aquest es mostri al signant abans del procés de signatura.
- Que el consentiment d'ambdues parts: de l'emissor i del receptor, es necessita perquè la facturació electrònica tingui la mateixa validesa legal que la factura en paper.

En els països en què la legislació ho admet, la validesa d'una factura electrònica és exactament la mateixa que la de la factura en paper i gràcies a la signatura electrònica que inclou es garanteix la seva integritat i un alt nivell de traçabilitat, per la qual cosa judicialment és un document considerat com vinculant i que no necessita de major prova o consignació que la seva pròpia existència.

2.4. Esquema de la signatura electrònica

Vegem un esquema del procediment de signatura electrònica i de la seva verificació, suposant que emissor i receptor disposen d'un sistema criptogràfic asimètric (per exemple, el criptosistema RSA) i que el receptor disposarà del certificat de la clau pública del signant.

Validesa de la signatura electrònica

La signatura electrònica, per a ser usada en facturació electrònica, ha de ser reconeguda, per tal d'aconseguir el major grau de seguretat d'acord amb la Llei 59/2003. Només la signatura reconeguda té validesa legal igual a la manuscrita. El termini de resolució és de sis mesos, a comptar des de la data de presentació de la sol·licitud en el registre. Si la verificació no hagués finalitzat en aquest termini, o no s'hagués dictat resolució expressa, la sol·licitud es podrà entendre desestimada per silenci administratiu.

Criptosistema RSA

El criptosistema RSA consisteix a xifrar valors numèrics associats a blocs, d'una determinada llargada, de caràcters en què estan escrits els missatges originals (per exemple, xifrar els valors numèrics de blocs de caràcters ASCII). Suposem $m \in [2, n - 1]$ corresponent a un cert bloc a xifrar.

L'algorisme d'enciptació es redueix al càlcul d'una exponencial on la clau pública és el parell de nombres (e,n) :

$$c = E_{(e,n)}(m) = m^e \bmod n$$

L'algorisme de desenciptació, per a poder obtenir m a partir de c , consisteix també en una exponenciació, on la clau privada és ara un altre parell de nombres (d,n) :

$$m = D_{(d,n)}(c) = c^d \bmod n$$

Els paràmetres n , e i d s'obtenen de la manera següent:

- 1) Trobar el valor $n = p \cdot q$, on p i q són dos nombres primers grans (a l'inici ja se suggerien un centenar de dígit cadascun).
- 2) Coneixent p i q , calcular: $\phi(n) = (p-1) \cdot (q-1)$.
- 3) Agafar e relativament primer amb $\phi(n)$.
- 4) Calcular $d = e^{-1} \bmod \phi(n)$.

Signatura electrònica, basada en l'RSA

Els algorismes d'enciptació i desenciptació de l'algorisme RSA són commutatius; és a dir: $D_k(E_k(m)) = E_k(D_k(m))$, i, per tant, l'esquema RSA pot ser utilitzat per a ambdós objectius de privacitat i autenticitat.

En funció d'aquesta commutativitat es pot utilitzar l'RSA per a construir signatures electròniques. En aquest cas, si suposem que un usuari A vol enviar un missatge m a un altre usuari B i la clau pública de A és (e_A, n_A) i la clau privada (d_A, n_A) , podem arbitrar un sistema de signatura electrònica, perquè B pugui autenticar a A , de la manera següent:

Per part de l'usuari A : Signarà m amb la seva clau privada: $s = D_{(d_A, n_A)}(m) = m^{d_A} \bmod n_A$ i aleshores enviarà a l'usuari B : (m, s)

Per part de B , un cop rebut el criptograma (m, s) , farà:

- 1) Xifrar s amb la clau pública de A : $E_{(e_A, n_A)}(s) = s^{e_A} \bmod n_A$
- 2) Verificar si el valor trobat anteriorment és igual a m .

En aquest cas es dona la signatura per vàlida. En cas contrari, vol dir que hi ha hagut algun problema en la transmissió de m , o en la mateixa signatura.

Com a alternativa a la signatura electrònica RSA, el 1991 el NITS (*National Institute of Standards and Technology*) va fer la proposta de l'algorisme DSA (*Digital Signature Algorithm*) com un estàndard de signatura electrònica, basat en el sistema criptogràfic asimètric d'ElGamal que es basa en la funció unidireccional exponencial discreta en un cos finit \mathbb{Z}_p i un element primitiu α .

Fortalesa de la funció unidireccional logaritme discret

En un cos finit \mathbb{Z}_p és fàcilment calculable $y = \alpha^x \bmod p$; però per a valors grans de p , donat y és computacionalment ineficient calcular el logaritme discret $x = \log_{\alpha} y \bmod p$. En la dificultat d'aquest càlcul es basa la fortalesa del criptosistema ElGamal i, per tant, també de l'algorisme DSA.

Aquest algorisme DSA fou desenvolupat per l'NSA (*National Security Agency*), amb el propòsit de reduir la longitud del missatge m a xifrar. Per aquesta raó, en el procés de signatura es fa servir una funció *hash*, per exemple l'SHA.

Els paràmetres d'aquesta signatura DSA són:

- p , un nombre primer el valor del qual és comprès entre 512 i 1024 bits.
- q , un factor primer de $p - 1$ d'uns 160 bits. Sigui $n = (p - 1)/q$
- α , tal que $\alpha = g^n \bmod p$, on g és un nombre menor que $p - 1$ i de manera que $\alpha \bmod p > 1$.
- x , un nombre qualsevol menor que q . Aleshores es calcula y , tal que $y = \alpha^x \bmod p$.

Els nombres p , q i α són públics per a tots els usuaris de la xarxa, així com també serà públic el *hash*, $H()$ que s'usarà (per exemple, el *hash* SHA-1 que, sigui quina sigui la mida del missatge a signar, ens donarà un resum de 160 bits).

D'altra banda, x és la clau privada d'un usuari, i y és la corresponent clau pública.

Sigui m el missatge que A vol transmetre a B , el qual vol signar perquè B pugui fer-ne l'autenticació. L'usuari A , del qual se suposen coneguts els paràmetres anteriors, excepte x , haurà de realitzar les operacions següents:

- 1) Triar un nombre aleatori k , menor que q .
- 2) Generar dos valors r i s , tals que:

$$r = (\alpha^k \bmod p) \bmod q$$
, i

$$s = ((H(m) + x \cdot r) \cdot k^{-1}) \bmod q$$
- 3) Enviar el missatge m i la seva signatura electrònica (r,s)

L'usuari B , en rebre el missatge m , i la seva signatura electrònica corresponent (r,s) , podrà fer el següent procés d'autenticació:

- 1) Seleccionar del directori públic els paràmetres de A : p,q,α i $H()$
- 2) Calcular: $w = s^{-1} \bmod q$,

$$u_1 = (H(m) \cdot w) \bmod q$$
 i

$$u_2 = (r \cdot w) \bmod q$$
- 3) Calcular: $v = ((\alpha^{u_1} \cdot y^{u_2}) \bmod p) \bmod q$
- 4) Autenticar:
 Si $v = r$ aleshores la signatura electrònica de A , (r,s) , és acceptada per B .
 En cas contrari, el missatge m o la signatura (r,s) han sofert algun canvi durant la transmissió.

Procediment de la signatura electrònica

De manera general, el procediment de la signatura electrònica segueix el que hem indicat per al cas de la signatura RSA i DSA. Oblidant-nos de fórmules, partim d'un document original (en aquest cas, la factura electrònica) el qual és sotmès, per l'emissor, als passos següents:

- 1) L'emissor aplica al document original (e-factura) la funció unidireccional *hash*, obtenint el corresponent resum.
- 2) L'emissor encripta, amb la seva clau privada, el resum resultant de l'aplicació anterior. El resultat serà la seva signatura electrònica.
- 3) L'emissor envia al destinatari el conjunt format pel document original (l'e-factura), la seva signatura electrònica i el certificat de la seva clau pública.

Comprovació / verificació de la signatura electrònica

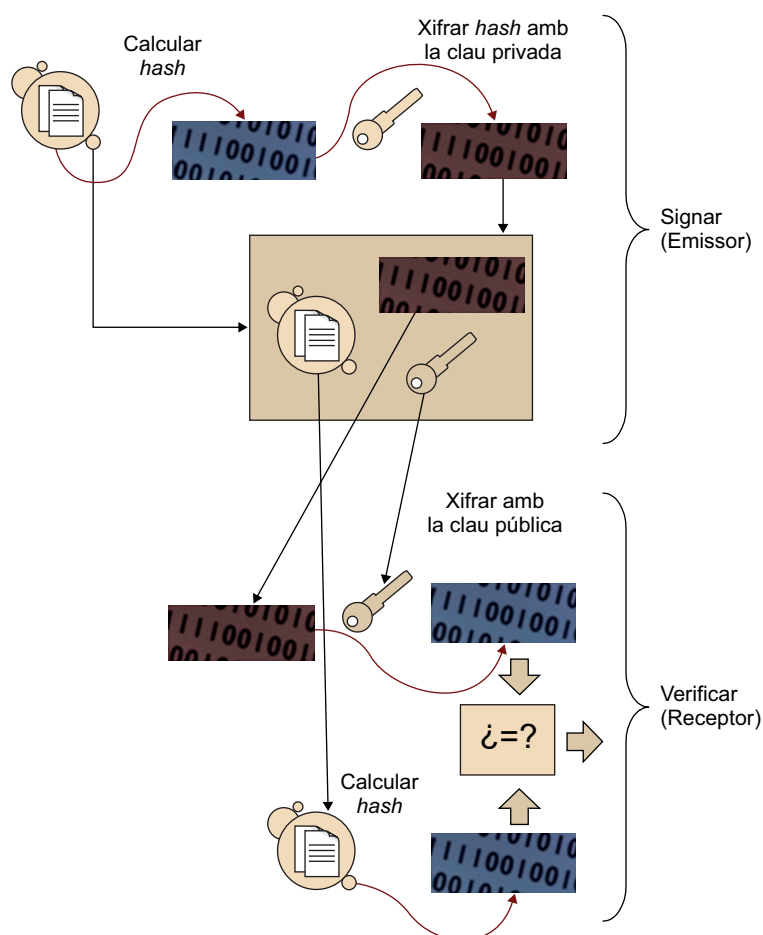
El receptor rep el conjunt format pel document original (l'e-factura), la signatura electrònica i el certificat de la clau pública de l'emissor. A partir del certificat, el receptor podrà extreure la clau pública de l'emissor i seguir els passos següents:

- 1) Atès que el receptor disposa del document original, pot calcular el *hash*, obtenint així el mateix resum que havia obtingut l'emissor.
- 2) El receptor, amb la clau pública de l'emissor, podrà xifrar la signatura electrònica i, per tant, obtenir el *hash* que es va calcular en origen.

En comparar el *hash* obtingut al pas 1, amb el *hash* obtingut en el pas 2, ambdós han de coincidir.

En cas que no coincideixin, o bé el document o bé el *hash* signat han tingut alguna incidència en la transmissió i, per tant, la signatura no és vàlida.

En la figura següent podeu veure el diagrama de funcionament:



Procediment de signatura electrònica i la seva verificació

2.5. Format XML de signatura en facturació electrònica

No hi ha requisits formals respecte a la forma en què s'ha de procedir a la codificació de la factura, però, per a cada format, hi ha una forma peculiar de codificar la signatura electrònica. Les modalitats més habituals són les següents:

1) PDF. Quan al destinatari només li interessa guardar electrònicament la factura, però no evitarà tornar a teclejar les dades, ja que amb aquest format no es facilita l'ingrés de les dades de la factura en l'ordinador del receptor.

El format de signatura queda inclòs dintre del format PDF i permet associar una imatge, per la qual cosa és un dels més adequats per a la seva visualització. S'empra *AcrobatReader v7* o *Foxit PDF Reader*. L'aparença de la signatura és molt visual, ja que és possible associar-hi un gràfic com a signatura electrònica o un segell d'empresa.

2) EDIFACT. Quan l'enviament es fa d'ordinador a ordinador, la qual cosa vol dir que el destinatari és una empresa que té capacitat tecnològica per a tractar de manera automatitzada la informació rebuda, i així les dades s'ingressen en l'ordinador de destinació automàticament. Aquest estàndard és desenvolupat

per l'organització GS1 (*Global System 1*; des de 2005, unió de les antigues EAN (*European Article Number*) i UCC (*Uniform Code Council*) que és l'organització més reconeguda mundialment en l'elaboració de normes relatives a la distribució i subministrament.

A Espanya, és AECOC (Associació de Fabricants i Distribuïdors d'Espanya), com a representant de GS1, l'encarregada de desenvolupar i vetllar pel compliment dels estàndards EDI.

Encara que hi ha un missatge EDI específic per a la signatura, aquesta es duu a terme mitjançant un missatge CMS (*Cryptographic Message Syntax*) (derivat de l'estàndard PKCS 7, usat per a xifrar i signar missatges en una PKI). Però, si la factura és EDIFACT, l'RD 1496/2003 i la Directiva europea 2001/115 possibiliten l'exhoneració de la signatura.

3) XML. Aquesta és una altra sintaxi, quan l'enviament és d'ordinador a ordinador. XML és un llenguatge estès principalment a l'Amèrica del Nord que a poc a poc va guanyant terreny a Europa. Hi ha diverses variants, essent les més importants: UBL (*Universal Business Language*), protegit per OASIS, i el llenguatge GS1 protegit per l'organització del mateix nom. A Espanya, la variant de factura CCI-AEAT, anomenada *Facturae*, protegida pel Centre de Cooperació Interbancària i l'Agència Tributària és la més difosa, i disposa de sistemes de traducció a i des d'UBL.

El format de signatura electrònica en XML es denomina XAdES. De les diferents modalitats de signatura XAdES, la més recomanable és XAdES-X-L/ que inclou informació sobre el temps en el qual es va portar a terme la signatura electrònica i informació sobre la validesa del certificat electrònic qualificat que l'acompanya.

Aquí ens centrarem en el format XML, que és recollit en la norma europea TS 101 903.

El llenguatge XML (*eXtensible Markup Language*) és un llenguatge desenvolupat per W3C (*World Wide Web Consortium*), a partir de l'estàndard XMLDSig, que permet definir la gramàtica de llenguatges específics per a estructurar documents grans, especialment útil a l'hora de comunicar entre elles diverses aplicacions. Quan s'usa el format XML es fa servir el llenguatge UBL universal que simplifica l'intercanvi d'informació financera de manera automàtica, fent possible la interoperabilitat de les factures emeses per qualsevol estat membre de la Unió Europea.

Actualment el format XML s'ha convertit, de fet, en un estàndard per a l'intercanvi d'informació estructurada entre diferents plataformes, ja que permet, de manera fàcil, la compatibilitat entre sistemes per a compartir la informació d'una manera segura i fiable (com en el cas de la facturació electrònica) entre particulars.

D'aquesta manera, quan les factures electròniques es codifiquen en XML utilitzarem les signatures XML, encara que es poden aplicar a qualsevol tipus de document, amb independència del seu format, destacant el format XML *Advanced Electronic Signature*, conegut com **signatura XAdES**.

En tota signatura XML, segons l'estàndard XMLDSig, hi ha tres modalitats:

- *Enveloped*, en el qual la signatura s'afegeix al final del document XML com un element més. Aquest és el format usat per *facturae*.
- *Enveloping*, en el qual el document s'inclou dintre de la signatura en la qual es referencia el signant com a objecte inserit en la signatura.
- *Detached*, en el qual la signatura i el document se separen en dos arxius (l'URL (*Uniform Resource Locator*) on el document pot aparèixer en la pròpia signatura).

La norma europea TS 101 903 estableix també dues modalitats de signatura electrònica que inclouen el segellament de temps. La variant T afegeix el segellament a una signatura bàsica (BES) i la variant C que, a més del segellament de temps, afegeix informació sobre la ruta de verificació de la validesa del certificat obtingut d'una consulta OCSP o de CRL. D'altra banda, aquesta mateixa norma preveu la modalitat X-L que inclou informació sobre l'estat de revocació del certificat, obtenint d'aquesta manera una signatura que allibera al receptor del problema de validació del certificat enfront el proveïdor de serveis.

XAdES (*XML Advanced Electronic Signatures*) és un conjunt d'extensions a les recomanacions XML-DSig per a adequar-les a la signatura electrònica avançada.

Mentre XML-DSig és un marc general per a la signatura electrònica de documents XML, XAdES especifica perfils precisos d'XML-DSig per a ser utilitzats amb signatura electrònica reconeguda tal com es defineix a la Directiva 1999/93/CE.

Un benefici important de la XAdES és que els documents signats electrònicament poden continuar essent vàlids durant llargs períodes de temps, fins i tot si els algorismes criptogràfics subjacents han estat trencats.

La figura següent mostra la cadena de formats XAdES de signatures electròniques, segons el nivell de protecció que ofereix:

Facturae

Quan el client és l'administració pública (govern central, governs autonòmics, ajuntaments i diputacions), a partir del 30/10/2010 les empreses estan obligades a remetre totes les factures en format electrònic que es pot aconseguir utilitzant la plataforma www.facturae.es.

Les signatures electròniques i *facturae*

Les signatures electròniques utilitzades en el cas de *facturae*, són en les modalitats XAdES-BES i XAdES-X-L.

Cadena de formats XAdES	
Format	Descripció
XAdES-BES	Forma bàsica per signatura electrònica avançada.
XAdES-EPES	Forma bàsica, més informació sobre la política de signatura.
XAdES-T (<i>timestamp</i>)	Afegeix segellat de temps per a protegir contra el repudi.
XAdES-C (<i>complete</i>)	Afegeix referències a dades de verificació (certificats i llistes de revocació) per a permetre la verificació i la validació <i>off-line</i>
XAdES-X (<i>extended</i>)	Afegeix segellat de temps a XAdES-C per tal d'evitar que la cadena de certificats es pugui veure compromesa en un futur.
XAdES-X-L (<i>extended long-term</i>)	Afegeix els certificats i les llistes de revocació en els documents signats per a permetre la verificació en el futur, inclús si els originals ja no són disponibles.
XAdES-A (<i>archival</i>)	Afegeix la possibilitat de segellat de temps periòdic de documents arxivats per a prevenir que puguin ser compromesos a causa de l'afebliment de la signatura si romanen arxivats durant un llarg període de temps.

Quant a la perdurabilitat de les signatures al llarg del temps, s'ha de tenir en compte el tema de la validació de les signatures a llarg termini. Actualment, pel que fa la majoria de signatures, només es fa una comprovació de la CRL/OCSP (llista de certificats revocats, amb el protocol de certificació en línia del certificat) en el moment de fer la signatura, però no se'n conserva cap evidència. Així, quan en el futur es vulgui comprovar la validesa de la signatura i el certificat ja hagi caducat o s'hagi revocat, no es podrà determinar si en el moment de signar el certificat la signatura era vàlida.

Per a evitar aquest efecte, es recomana usar procediments de signatura que permetin crear una signatura completa i autoverificable i que incorporin a la signatura electrònica els elements temporals (segellament de temps de l'autoritat de certificació) i de validació que permeten verificar la signatura sense ajuda externa. D'aquesta manera, es podran fer les validacions sense necessitat de connectar-se en línia amb cap servei de l'autoritat de certificació.

Amb el segellament de temps, l'usuari, sense connexió a Internet, podrà tenir una factura electrònica amb tota la informació necessària per tal que sigui vàlida independentment del temps transcorregut.

CADES (*CMS Advanced Electronic Signatures*) és un conjunt d'extensions de sintaxi de missatges criptogràfics (*CMS Cryptographic Message Syntax*) de dades signades mitjançant signatura electrònica avançada. Mentre CMS és un marc general per a la signatura electrònica de documents, com ara correu electrònic (per mitjà d'S/MIME) o PDF, CADES especifica perfils precisos de CMS per a ser usats amb signatura electrònica avançada tal com es defineix a la Directiva 1999/93/CE. Un benefici important de la CADES és que els documents

signats electrònicament poden continuar essent vàlids durant llargs períodes de temps, fins i tot si els algorismes criptogràfics subjacents han estat trencats.

La figura següent mostra la cadena de formats CADES de signatures electròniques, segons el nivell de protecció que ofereix:

Cadena de formats CADES	
Format	Descripció
CADES	Forma bàsica per signatura electrònica avançada.
CADES-T (<i>timestamp</i>),	Afegeix segellat de temps per a protegir contra el repudi.
CADES-C (<i>complete</i>)	Afegeix referències a dades de verificació (certificats i llistes de revocació) per a permetre la verificació i la validació <i>off-line</i> .
CADES-X (<i>extended</i>)	Afegeix segellat de temps a CADES-C per tal d'evitar que la cadena de certificats es pugui veure compromesa en un futur.
CADES-X-L (<i>extended long-term</i>)	Afegeix els certificats i les llistes de revocació en els documents signats per a permetre la verificació en el futur, inclús si els originals ja no són disponibles.
CADES-A (<i>archival</i>)	Afegeix la possibilitat de segellat de temps periòdic de documents arxivats per a prevenir que puguin ser compromesos a causa de l'afebliment de la signatura si romanen arxivats durant un llarg període de temps.

3. Els sistemes de facturació electrònica

Tal com hem dit, la factura electrònica és un tipus de factura que es diferencia de la factura en paper per la forma de gestió informàtica i l'enviament mitjançant un sistema de comunicacions que, conjuntament, permeten garantir l'autenticitat i la integritat del document electrònic.

Una factura electrònica es construeix en dues fases: en la primera es crea la factura tal com s'ha fet sempre i s'emmagatzema en un fitxer de dades i, en la segona, es procedeix a la seva signatura amb un certificat electrònic, propietat de l'emissor, que encripta el contingut de factura i, de manera opcional, hi afegeix el segellament de temps (*time stamping*). Aquesta signatura electrònica, generada per l'emissor, permetrà al receptor verificar la integritat de la signatura i l'autenticació del signant. Els algorismes criptogràfics utilitzats tant pel *hash* del document com per la signatura han d'estar plenament acceptats per la comunitat internacional: per exemple, RSA i DSA, per a la signatura, i SHA com a funció *hash*.

El segellament de temps en els documents electrònics contenen el resum (el *hash* del document), la data i l'hora en què fou generat, obtinguda d'una font fiable i la signatura electrònica. Aquests segells permeten garantir que la informació continguda en el document no s'ha modificat des del moment en què es va generar el segell i es pot adjuntar a la informació per a garantir el seu no repudi (penseu en la importància del segellament de temps en els contractes amb les companyies d'assegurança).

L'emissor envia la factura al receptor per mitjans electrònics, com poden ser CD, memòries flaix i, fins i tot, Internet. Si bé es dediquen molts esforços per a unificar els formats de factura electrònica, actualment està sotmesa a distintes normatives i té diferents requisits legals exigits per les autoritats tributàries de cada país, de manera que no sempre és possible l'ús de la factura electrònica, especialment en les relacions amb empreses estrangeres que tenen normatives diferents a la del propi país.

Els requisits legals respecte al contingut mercantil de les factures electròniques són exactament els mateixos que regulen les factures en paper. Els requisits legals en relació amb la forma imposen un determinat tractament per tal de garantir la integritat i l'autenticació i certs formats que facilitin la interoperabilitat.

La factura electrònica permet que institucions, empreses i professionals deixin enrere les factures en paper i les reemplacin per la versió electrònica del

Integració de l'e-factura

La factura electrònica guanya potència quan s'integra en els processos de gestió de l'empresa, tant pel que fa a la seva emissió com quant a la seva recepció. Així es multipliquen els beneficis en tractar els documents de manera electrònica dins de l'empresa.

document tributari. Té exactament la mateixa validesa i funcionalitat tributària que la factura tradicional en paper. Tot el cicle de la facturació pot ser administrat en format electrònic.

3.1. Requisits de totes les factures

Com a requisit de totes les factures independentment de com es transmetin, en paper o en format electrònic, l'article 6 de l'RD 1496/2003 que regula el contingut d'una factura estableix que els camps obligatoris són:

- Número de factura, i si escau, sèrie.
- Data d'expedició.
- Nom i cognoms, o raó social, de l'emissor i del receptor.
- NIF de l'emissor i del receptor.
- Domicili fiscal dels dos tributors: de l'emissor i del receptor.
- Descripció de les operacions (base imposable).
- Data del lliurament del bé o de la prestació del servei (si és distinta a la d'expedició).
- Referència, de manera inequívoca, a l'albarà, si n'hi ha.
- Tipus impositiu aplicable a l'operació.
- Quota tributària o repercutida.

Per a complir la norma i que una factura electrònica tingui la mateixa validesa legal que una emesa en paper, el document electrònic que la representa ha de contenir els camps obligatoris exigibles a tota factura, estar signat mitjançant una signatura electrònica avançada, basada en certificat reconegut, i ser transmès d'un ordinador a un altre, recollint el consentiment d'ambdues parts.

Hi poden haver altres requisits, marcats per part de l'emissor o del receptor, encaminats a facilitar la conciliació automàtica de les factures en els sistemes d'informació propis.

3.2. Obligacions legals per a l'emissor

1. Consentiment del receptor. Aquest consentiment es podrà formular de manera expressa per qualsevol mitjà, verbal o escrit (segons l'article 2 de l'Ordre 962/2007). També s'haurà d'acordar amb el receptor el format de la factura electrònica i quin ha de ser el mitjà telemàtic d'enviament.

2. Creació de la factura. Mitjançant una aplicació informàtica, amb els continguts obligatoris mínims requerits.

3. Signatura electrònica reconeguda. Per a garantir l'autenticitat de l'origen i la integritat de les factures.

Renúncia a la facturació electrònica

En qualsevol moment, tant l'emissor com el receptor de facturació electrònica pot renunciar a continuar amb el procediment.

4. Remissió telemàtica. El fitxer de la factura electrònica, en el format acordat, és tramès per qualsevol mitjà de comunicació electrònic i/o digital, des de l'ordinador de l'emissor a l'ordinador del receptor per al seu procés administratiu, inclosos el de comptabilització i anotació als registres de l'IVA, segons directrius de l'autoritat tributària.

5. Conservació de còpia o matriu de la factura. Aquesta obligació es regula en l'article 1 de l'RD 1496/2003, on s'especifica l'obligació d'expedir, lliurar i conservar factures. Si es conserva la matriu de la factura, ja no és necessari conservar les còpies de les factures electròniques signades, ja que a partir de la matriu es poden tornar a generar.

6. Conservació durant el període de prescripció. La llei exigeix conservar les factures dels darrers cinc anys. Per tal de conservar les factures electròniques correctament, cal tenir en compte l'Ordre EHA 962/2007, en la qual es recull la validesa de la digitalització de les factures i l'homologació del programari necessari, així com també admet la impressió de les factures electròniques per mitjà del codi PDF-417.

En el supòsit de l'article 6 de l'Ordre EHA-962/2007, un document imprès en paper amb aquest codi és vàlid, sempre que es mantingui l'esmentat repositori en el qual hi ha el document i la seva signatura electrònica, quan hi ha un mecanisme de verificació de la signatura i es pot accedir de manera completa al document mitjançant aquest codi electrònic d'autenticació. Aquesta és la solució més senzilla: indicar a la factura impresa l'URL o el localitzador del document electrònic d'on procedeix la factura en paper. D'aquesta manera es disposa de la mateixa validesa que pot aportar la impressió amb PDF-417. A més, la conversió a document electrònic és immediata, només accedint a la font, de manera que qualsevol pot comparar el contingut del paper amb el document electrònic.

7. Garantia d'accessibilitat completa. S'han de gestionar les factures de manera que permetin: la visualització, la recerca selectiva, la còpia o la descàrrega en línia i la impressió. Aquesta és una obligació inherent a la conservació de les factures per mitjans electrònics tractant de facilitar l'auditoria i inspecció de les factures electròniques.

8. Subcontractació a un tercer. Totes les fases anteriors poden ser subcontractades a un tercer, sense que l'emissor perdi la seva responsabilitat respecte de les obligacions tributàries.

3.3. Obligacions legals per al receptor

1. Recepció de la factura per mitjà electrònic. El receptor s'ha d'assegurar de la llegibilitat en el format original en el qual s'hagi rebut, així com, si escau, de les dades associades i mecanisme de verificació de signatura. Per

Matriu de la factura

S'entén per matriu d'una factura electrònica el conjunt de dades, taules, bases de dades i/o fitxers que contenen totes les dades reflectides a la factura, juntament amb els programes que van permetre generar-la.

L'article 6 de l'Ordre EHA-962/2007, preveu una solució alternativa

Quan l'emissor i/o receptor de factures i documents substitutius electrònics sigui un tercer que actua en nom i per compte dels obligats tributaris, haurà de complir els requisits expressats anteriorment. No obstant això, un cop complerts, podran posar a disposició del seus clients aplicacions informàtiques que gestionen un repositori de factures i documents substitutius emesos o rebuts, segons correspongui, juntament amb la signatura electrònica generada o verificada en els termes d'aquesta Ordre, proporcionant un codi d'autenticació de missatges associat a cada document. Aquest codi permetrà l'accés al document associat existent en el repositori i garantirà, a qui hi accedeix, que compleix els requisits previstos en aquesta Ordre.

això el receptor ha de conservar els originals signats, la qual cosa permetrà la verificació dels continguts mínims exigibles de la factura i la verificació segura de la signatura electrònica.

2. Eines de verificació de signatures i vigència de certificats. Haurà de disposar d'eines que permetin la verificació de la signatura i de la identitat de l'emissor, al mateix temps que haurà de poder verificar la vigència del certificat de l'emissor; és a dir, que el certificat utilitzat per a la generació de la signatura electrònica no ha perdut la seva eficàcia per revocació, caducitat o qualsevol causa establerta en l'ordenament jurídic.

3. Comptabilització i anotació en registres d'IVA. Seguint les directrius de l'autoritat tributària.

4. Conservació durant el període de prescripció. Eventualment, podrà conservar la factura impresa amb marques gràfiques (núvols de punts) en format PDF-417. O, alternativament, tal com s'ha mencionat en el cas de l'emissió, fent ús del que disposa l'article 6 de l'Ordre EHA-962/2007.

5. Garantia d'accessibilitat completa. S'han de gestionar les factures de manera que permetin la visualització, la recerca selectiva, la còpia o la descàrrega en línia i la impressió.

6. Subcontractació a un tercer. Totes les fases anteriors poden ser subcontractades a un tercer, sense que el receptor en perdi la responsabilitat.

3.4. Conservació electrònica de les factures

La llei exigeix conservar les factures dels darrers cinc anys, la qual cosa implica arxivar, gestionar i conservar els documents corresponents.

La factura electrònica és un fitxer informàtic i, com a tal, es pot guardar en diferents suports: disquet, CD-ROM, memòria USB, disc dur o paper.

Pel que fa a les factures electròniques, s'estableix que el receptor pot conservar les factures en el mateix format i suport original en què van ser emeses, tret que s'opti per alguna de les formes de conversió autoritzades en l'Ordre EHA/962/2007. Segons aquesta Ordre, podem considerar dos procediments per a la conservació de les factures; el de conservar electrònicament una factura en paper, mitjançant una digitalització certificada, i el de conservar en paper una factura electrònica, mitjançant el format PDF-417.

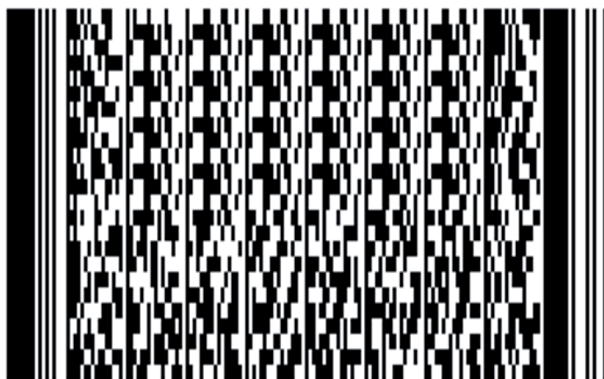
La figura següent mostra el núvol de punts del codi PDF-417:

Regulació segons l'Ordre EHA 962/2007

Aquesta Ordre regula l'obligació que té el receptor de verificar la signatura i comprovar la validesa dels certificats de les factures trameses per mitjans electrònics. És a dir, el receptor haurà de disposar del programari escaient que li permeti saber si la signatura de la factura és vàlida, o no.

Obligacions dels tercers

En la facturació, electrònica o no, sempre hi ha dos obligats tributaris: el que té l'obligació de remetre la factura, i guardar-ne almenys la matriu, i el client que té l'obligació de rebre-les i conservar les factures tal qual. Aquestes obligacions es poden cedir a tercers perquè actuïn en nom de l'obligat tributari. En qualsevol cas, els responsables últims davant les autoritats tributàries són els obligats tributaris, és a dir, el professional que ha d'expedir-la i el seu client destinatari.



En el primer cas, si així es vol, la digitalització certificada consisteix en el procés pel qual es transformen les factures rebudes en paper en una imatge digitalitzada (escàner) que després se signarà electrònicament. Una vegada feta la digitalització certificada d'una factura, es pot destruir el document en paper ja que el document transformat té el caràcter d'original.

Per a realitzar la digitalització certificada només cal utilitzar programari homologat per l'Agència Tributària.

En el segon cas, el de voler conservar en paper una factura electrònica, s'utilitza el format PDF-417, encara que, actualment, ja ha caigut en desús ja que no és un requisit de la facturació electrònica i, a més, cal programari especial per a poder imprimir les factures en format electrònic. No obstant això, quan s'emetin factures en paper, s'haurà d'adjuntar un conjunt de codis PDF-417 que recullin en un fitxer UBL totes les dades de la factura, per a facilitar-ne la digitalització.

L'Ordre ministerial EHA/962/2007 defineix els elements necessaris per a convertir les factures rebudes en paper al seu equivalent electrònic, sempre que en l'operativa de digitalització s'emprí un procés que garanteixi que el resultat de la digitalització és imatge fidel del document original en paper, i que el dispositiu de digitalització (escàner) produeix la imatge acompanyada d'una signatura electrònica qualificada, tal com es defineix a la Directiva comunitària 1999/93. El procés que ho assoleix és denominat *digitalització certificada*.

Per a poder realitzar aquest tipus d'impressió, la factura electrònica que s'ha rebut haurà hagut de ser emesa amb un programari específic que generi i inclogui en la factura electrònica aquest núvol de punts del codi PDF-417. A més en aquesta normativa s'indica que les factures electròniques es poden transcriure a paper incloent-hi marques gràfiques d'autenticació, produïdes segons l'especificació PDF 417, tal com es disposa en la Resolució de l'AEAT 2/2003.

La impressió d'una factura electrònica en format PDF-417, té validesa legal, ja que aquest format inclou en el document imprès un codi, en núvol de punts, per a la seva identificació i validació. Aquest núvol de punts és una marca

e-factura en paper

Sempre és més senzill enviar la factura electrònica en qualsevol format, signada electrònicament, de manera que el receptor la pugui obrir i imprimir, si ho vol. L'e-factura signada electrònicament és l'únic que s'ha de conservar per a la inspecció tributària.

gràfica que inclou el contingut íntegre de les dades de la factura i la signatura electrònica del fitxer.

3.5. Procediments d'emissió i recepció de factures electròniques

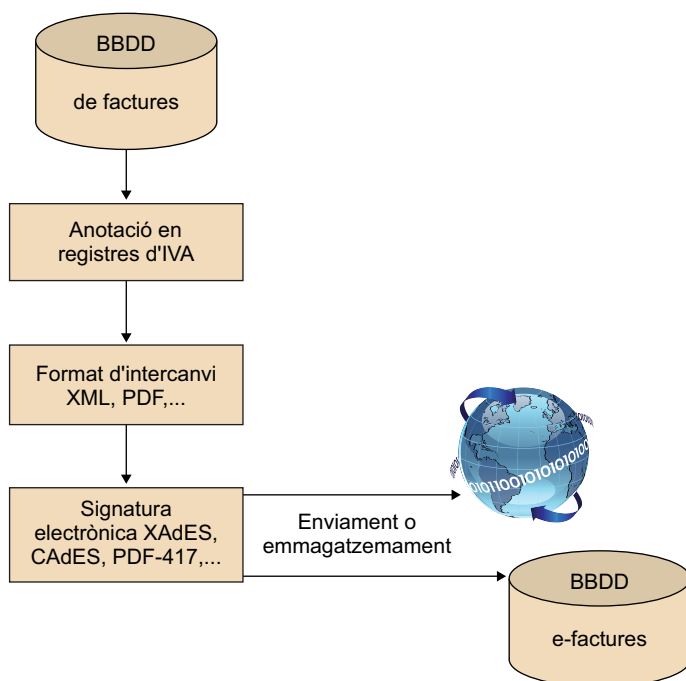
Ja hem dit que l'obligació bàsica de l'emissor és signar la factura electrònicament, i la del receptor, verificar la factura i conservar-la en el format original.

Suposant que disposem d'una plataforma de facturació electrònica i del corresponent certificat electrònic reconegut per una autoritat de certificació, anem a descriure els procediments d'emissió i recepció de factures electròniques.

Pel que fa a l'emissió de factures electròniques, se segueixen els passos següents:

- 1) Amb la plataforma de facturació electrònica es genera la factura, o la recuperem d'una base de dades, del mateix sistema d'informació de l'empresa, on hi ha emmagatzemats els fitxers o matrius de les factures.
- 2) Un cop recuperada la factura, es fa la corresponent anotació en els registres d'IVA de l'empresa, si no ho ha fet automàticament la plataforma de facturació.
- 3) La factura és codificada en el format d'intercanvi escollit, segons el mitjà de transmissió posterior.
- 4) La factura és signada electrònicament, segons el format escollit, amb la clau privada de l'emissor. És interessant que l'aplicació escollida pugui verificar la signatura, és a dir, determinar si és vàlida o no, si està caducada o si s'ha revocat. D'aquesta manera s'assegura que s'ha enviat al receptor una factura electrònica amb una signatura correcta.
- 5) La factura signada és enviada, o desada en una base de dades a la qual hi podrà accedir el receptor. La podem enviar per correu electrònic, a través d'una plataforma web (*Web service*) o en paper, per correu ordinari, per a la qual cosa s'haurà d'imprimir el codi PDF-417 o, alternativament, el codi d'autenticació. Quant a l'emmagatzemament, se suposa que la plataforma de facturació electrònica les dipositarà en llocs segurs i d'una manera estructurada, per tal de facilitar-ne la recuperació per data, nom, CIF, etc.

La figura següent mostra el diagrama del fluxe d'emissió de factures electròniques:



Pel que fa a la **recepció de factures electròniques**, en primer lloc s'ha de saber com es rebrà la factura i per quin mitjà telemàtic es rebran: si per correu electrònic, si l'hem de baixar d'una pàgina web (en aquest cas s'haurà d'introduir nom d'usuari i clau de pas), si en paper, rebuda a través del correu ordinari, on s'ha inclòs el codi PDF-417 o el codi d'autenticació, etc.

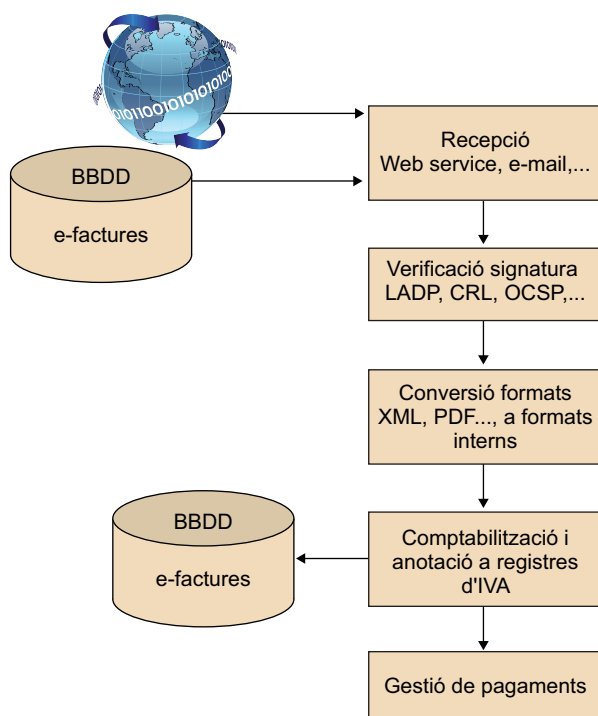
Un cop rebuda o recuperada la factura electrònica, se segueixen els passos següents per a la seva gestió:

- 1) S'ha de verificar la validesa de la signatura electrònica, comprovant primer si el certificat electrònic amb el qual s'ha signat és vàlid o no ho és. A través de les llistes CRL de les autoritats de certificació: si el certificat no és vàlid, aleshores tampoc ho serà la factura que el conté.
- 2) Convertir el format de la signatura rebuda en el format intern per a la seva gestió, especialment per a poder-les integrar en els ERP de l'empresa.
- 3) Comptabilitzar la factura en la comptabilitat de l'empresa i fer les anotacions pertinents en els registres d'IVA.

Verificació a CRL

A Internet hi ha visors gratuïts que permeten veure l'estat de la signatura i aplicacions estàndard que, si troben un fitxer PDF signat, automàticament verifiquen la validesa de la signatura. Amb un visor de signatures podem veure les propietats del certificat: saber qui l'ha emès, si el document s'ha modificat després d'haver-lo signat, i, si s'escau, consultar el segell temporal.

La figura següent mostra el diagrama del fluxe de recepció de factures electròniques:



Així mateix, hi ha altres models de facturació electrònica, com ara les plataformes de tercers i l'autofacturació.

Plataformes de tercers i autofacturació

Recordem que en la facturació, aplicant la legislació a la modalitat electrònica, hi ha dos obligats tributaris:

- Un professional o empresari que té l'obligació d'enviar telemàticament les factures en format electrònic, si així ho ha sol·licitat expressament el client, signades electrònicament i conservar almenys la seva matriu.
- Un client que té l'obligació de rebre-les i conservar les factures en el mateix format que les ha rebudes.

Es pot optar per donar compliment a aquestes obligacions mitjançant sistemes informàtics propis amb els quals executar tots els serveis de la facturació electrònica d'emissió, de signatura, d'enviament i de conservació.

Però també es pot optar per cedir i delegar aquestes obligacions. Hi ha dos models de delegació: acudir a plataformes de tercers o a l'autofacturació.

Plataformes de tercers: En aquest cas, l'emissor pot cedir l'expedició, la signatura i l'enviament de les factures a un tercer, així com la conservació de les factures o les seves matrius. D'altra banda, el receptor pot cedir la recepció i conservació de les factures.

Observació

És molt important tenir en compte que sempre, independentment del model triat, els responsables últims davant les autoritats tributàries són els obligats tributaris; és a dir, el professional o l'empresari (emissor) que ha d'expedir la factura i el client destinatari (receptor).

Aquesta opció és la més pràctica per a les petites i mitjanes empreses, ja que se simplifiquen les tasques i l'esforç, i normalment el cost és proporcional al nombre de factures electròniques emeses i/o rebudes.

Autofacturació: En aquest cas és el receptor de la factura qui emet la factura electrònica, de tal manera que és el mateix client qui controla el format i garanteix la conciliació comptable.

4. Descripció d'un cas real

Per a abordar la implantació de la factura electrònica en una empresa, els requeriments dependran en gran mesura de l'abast del projecte, depenent essencialment del volum de factures que l'empresa maneja, tant des del punt de vista de recepció com del d'emissió.

En aquest sentit, es pot començar només emetent factures electròniques, o només rebent-les, i fer-ho en qualsevol moment. A més, no és necessari facturar electrònicament a tots els clients de l'empresa, ni tampoc que totes les factures emeses en un mateix exercici per al mateix client siguin electròniques.

Hi ha moltes maneres d'implantar la factura electrònica en una empresa, des de l'enviament per correu electrònic de factures en format PDF signades, fins a la implantació de solucions avançades integrades en els sistemes propis de l'empresa, passant per solucions intermèdies, com les plataformes de facturació independents de la resta de sistemes de l'empresa.

Abans de posar en marxa un projecte de facturació electrònica, hem de considerar una sèrie de paràmetres per tal de triar la plataforma (aplicació informàtica i certificat electrònic) que s'adapti millor a les necessitats de l'empresa i al pressupost disponible.

Pel que fa al cost de la implantació de la facturació electrònica dependrà, bàsicament, de diversos factors:

- 1) **Situació inicial:** el cost variarà depenent de si l'empresa disposa o no del programari o maquinari que es requereix per a emetre i/o rebre factures electròniques.
- 2) **Necessitats:** no és el mateix haver d'emetre factures electròniques a tots els clients de l'empresa o només a una part.
- 3) **Modalitat:** el cost de facturar electrònicament amb plataformes de tercers és diferent del cost que cal invertir quan la facturació electrònica es realitza totalment amb sistemes propis.

La inversió serà proporcional a l'estalvi de costos, de temps i a l'augment de l'eficiència que es vulgui obtenir. Es poden posar en marxa projectes de facturació electrònica amb un pressupost baix, però si es vol la integració en els sistemes de gestió de l'empresa augmenta el preu de la implantació al mateix

Coautors

En la redacció d'aquesta secció hem comptat amb la inestimable col·laboració dels consultors de facturació electrònica: **Margarita Martínez Aguiló** i **Joan Miquel Ramon Tur**, que han aportat la seva experiència en la implantació de solucions de factura electrònica, tant a nivell de grans empreses com en el disseny i implementació de plataformes de facturació electrònica.

temps que els estalvis globals del procediment de facturació són també més elevats.

4.1. Reflexions sobre la implantació d'una solució de facturació electrònica

Abans d'abordar la implantació d'una solució real de facturació electrònica, farem unes reflexions, des de l'experiència, que poden ser d'utilitat.

L'argumentari més comú per a la implementació de la factura electrònica a una empresa es basa en aquestes consideracions:

- **Disminució de costos:**
 - 1) *Variables*. Depenen de la quantitat de factures emeses. Paper, tòner, franqueig, personal, etc.
 - 2) *Fixes*. Recursos i infraestructures per a emetre les factures. Per exemple, impressores, aplegadores, personal, arxiu, etc.
- **Simplificació dels processos administratius:** la manipulació física passa a ser informàtica / telemàtica. Això inclou arxivament i comunicació de rebuig del client.
- **Millora del circulant** per optimització de la gestió de cobrament:
 - 1) La factura entra abans en el circuit de pagament del client.
 - 2) Disminueixen les factures en via morta.
- **Millora en les relacions comercials:**
 - 1) Evitant discrepàncies per assumptes administratius.
 - 2) Creant un ambient àgil d'intercanvi d'informació.

Però la realitat és que hi ha una implantació progressiva i molt lenta d'emissió de factures, fins que s'aconsegueix la substitució total de les factures en paper, amb la qual cosa no s'aconsegueix la majoria de les millores esmentades anteriorment, ni la disminució de costos, ni la simplificació de processos (durant un cert temps es dupliquen). Per tant, per a assolir l'objectiu de la implementació de la facturació electrònica, s'ha de tenir en compte que:

- És necessari realitzar esforços i invertir recursos perquè els clients acceptin la factura electrònica.
- És un objectiu difícil d'assolir a curt termini.

Per aquesta raó, hi ha durant un període més o menys llarg, una convivència d'emissió de factures electròniques i factures en paper. Aquesta situació es dona en una gran majoria d'empreses i és el cas més comú i la principal barrera d'entrada que interessa analitzar amb profunditat.

Altres barreres d'entrada, que fan que les empreses no vulguin abordar la facturació electrònica, rau en el fet que hi ha moltes plataformes de facturació electrònica de tercers al mateix temps que provoquen un aïllament d'aquestes diferents plataformes. La competència entre elles fa que sigui molt difícil la interoperació; a més ofereixen valors afegits diferents atenent a criteris del seu negoci: les associades a bancs, oferint *factoring* o *confirming*; les associades a centrals de compres, oferint comanda / albarà; les que venen del món de la gestió documental, oferint altres serveis, enre d'altres. En general la casuística de la gestió de les factures és molt àmplia, però podem destacar:

- Hi ha moltes empreses que volen emetre o rebre la factura amb paper. En particular aquelles que entreguen les factures juntament amb la mercaderia i la donen al client en mà (per exemple, clients directes als hotels) i les que requereixen adjuntar a la factura altres documents (traçabilitat, bons, albarans, etc.).
- Quan hi ha un volum de factures molt elevat, no es justifica el fet de pagar una variable per factura a la plataforma d'un tercer; a l'empresa li surt més a compte un desenvolupament propi.
- Quan l'empresa té una venda directa per mitjà del seu portal web, hi ha receptors molt deslocalitzats, diferents països i diverses legislacions.
- Els emissors amb un nombre molt baix de factures accepten fer ús d'una plataforma però el troben car i, encara més, si no poden establir relacions en tots els seus receptors les envien per un altre canal.

El plantejament per a abordar els requeriments de la implantació de la factura electrònica en una empresa, dependrà, en gran mesura, de l'abast del projecte, però en el nostre cas ens fixarem en l'acompliment de cinc objectius que creiem que són clau per a la correcta adopció, per part de l'empresa, de la factura electrònica.

- 1) Involucrar els tercers (clients i proveïdors) en l'ús de la factura electrònica, facilitant la gestió del consentiment i de l'establiment de la relació.
- 2) La integració de les dades estructurades de la factura electrònica entre el sistema de gestió i els tercers (sistemes dels receptors / emissors).
- 3) Garantir l'autenticitat de la factura electrònica i el compliment legal.

4) Permetre gestionar els distints events relacionats amb la factura electrònica (pagada, rebutjada, incidències).

5) Custodiar la factura electrònica legalment facilitant la conciliació i donant suport per al cobrament.

La necessitat de plantejar-lo com un projecte es justifica perquè amb el foment de l'ús de la factura electrònica s'ha fet necessari gestionar legalment situacions no previstes abans:

- Gestionar els distints mitjans, canals i formats per a enviar o rebre factures electròniques (en lloc d'un únic canal, el paper).
- Concentrar en un repositori els diferents magatzems de factures electròniques (per exemple, les rebudes de l'operadora de telèfons i la de la llum de cada una dels seus webs).
- La necessitat de gestionar el consentiment i la informació de com es reben o s'envien les factures electròniques (per exemple, quin format PDF/XML, si és necessari un avís per correu electrònic, etc.).
- La necessitat de generar signatures electròniques i disposar de mecanismes de validació de les factures electròniques rebudes.

4.2. Implantació d'una solució de facturació electrònica: cas real

L'empresa

Ens centrarem en el cas que l'empresa interessada a implantar la solució de facturació electrònica és una cadena hotelera que disposa de diversos centenars d'hotels dispersos en diferents països i continents. Alguns dels hotels són propis i uns altres solament els gestiona cobrant per aquest servei de gestió.

L'organització es basa en una sola central administrativa des d'on s'intenta supervisar i realitzar la majoria dels cobraments i pagaments. Idealment, en la central administrativa, s'haurien de rebre i emetre totes les factures. Actualment això no és possible per dos factors:

- Molts proveïdors locals de productes peribles (pa, verdures i altres queviures) remetent les factures als hotels directament.
- Els hotels tenen la necessitat d'emetre les factures i cobrar als denominats clients directes, que són els que arriben a l'hotel sense un bo emès per l'agència de viatges o un altre intermediari.

La central administrativa té, actualment, un altre problema més important per a realitzar la seva labor i es deriva del fet que depèn completament de les dades que rep de cadascun dels hotels, siguin propis o gestionats. No tots els hotels utilitzen els mateixos aplicatius de gestió, la qual cosa té com a conseqüència que les dades que es reben no són homogènies en el format ni en la informació que se'n pot extreure.

Les expectatives

L'empresa fa una ferma aposta per la facturació electrònica i s'inicia el projecte amb els objectius següents:

- Disminuir els costos i ser més eficients.
- Contribuir a la política mediambiental estimant que amb el projecte podria arribar a estalviar el consum de prop de sis tones de paper anuals.
- Millorar substancialment el seu servei i les relacions amb els seus clients i proveïdors per a evitar errors, pèrdues de documentació i en gestionar més ràpidament les incidències que es produeixin.
- Disminuir el temps transcorregut entre l'emissió i el cobrament de les factures.
- Obtenir un benefici (o descompte en la seva emissió) per cada proveïdor que ells aportessin a la plataforma de facturació electrònica.

Solució de facturació electrònica adoptada i acord comercial

Després de considerar que internament no es tenen prou coneixements, ni tècnics ni legals, sobre facturació electrònica s'opta per una solució de factura electrònica completament externa a l'organització. S'estudien les alternatives que compleixen els requeriments legals i tècnics. Finalment se signa un acord comercial amb una plataforma de facturació, que ofereix la factura electrònica com un servei.

La plataforma de facturació seleccionada garanteix, a emissors i a receptors, l'estricta compliment de la legislació vigent en matèria de signatura i facturació electrònica, amb serveis de delegació de signatura i custòdia legal (actuant com a tercera part de confiança), preparada per a acceptar ells prestadors de serveis de certificació reconeguts per l'AEAT. A més, ofereix comprovació de la validesa dels certificats electrònics que acompanyen la factura.

A nivell tècnic, també proporciona seguretat a les transaccions electròniques, suporta múltiples formats d'entrada i sortida, una administració simple i flexible. També serveis web necessaris per a poder integrar-se amb els sistemes

d'informació de l'empresa, la qual cosa és molt necessària per a l'automatització dels fluxos de treball i de dades de l'empresa.

Fases del projecte

Analitzant una mica més amb detall el projecte s'observen que els sistemes i procediments afectats per l'emissió de factures són molt diferents als afectats per a la recepció de factures. Amb aquestes premisses, el projecte es divideix en dues fases: recepció de factura electrònica i emissió de factura electrònica.

Es decideix que la primera fase sigui la que més estalvis de costos proporcionï, per la qual cosa es valoren com a més significatius:

Emissió	Recepció
Impressió: consumibles i paper	Manipulació, classificació
Enviament: ensobrat i correu	Extracció i comptabilització de la informació

El cost més elevat correspon, en ambdós casos, als recursos humans dedicats a la tasca, i sens dubte les majors dedicacions són les de traspasar les dades del paper als sistemes d'informació de l'empresa, així com els de comptabilitzar les factures rebudes.

D'aquesta manera, la **primera fase** és la que fa referència a la recepció de factures electròniques. Aquesta fase s'aborda en tres subfases:

- 1) Prova pilot amb dos proveïdors de confiança: es realitzen proves d'enviaments, fins que es donen per vàlids i es posa el sistema en producció. Durant aquesta prova pilot no s'aborda la integració en els sistemes comptables de la cadena, amb la qual cosa es continua comptabilitzant manualment. Això implica que en aquesta fase no s'obtenen els estalvis esperats.
- 2) Extensió a trenta proveïdors més. Se seleccionen aquells dels quals es rep major volum de factures.
- 3) Resta de proveïdors: mateixos passos que la fase anterior.

La **segona fase** és la que fa referència a l'emissió de factures electròniques. També es planteja en tres subfases:

- 1) Fer un pilot amb una agència de viatges (minorista) i amb un operador turístic (majorista).
- 2) Extensió a cinc operadors turístics i cinc agències de viatges.
- 3) Incorporació gradual de la resta de clients, tenint en compte la casuística del client directe, que es vol dur la factura en mà.

En ambdues fases del projecte s'han hagut d'abordar aspectes i tasques tècniques i funcionals i altres de matís més logístic i comercial.

Les primeres òbviament s'han assumit per part de la direcció dels sistemes d'informació de la cadena hotelera i les segones per part dels recursos comercials, tant de la pròpia cadena hotelera, com de l'empresa que gestiona la plataforma de facturació.

Pel que fa a la part **tècnica i funcional** del projecte d'implantació es pot destacar, fonamentalment, la necessitat de connectar els sistemes d'informació de tots els agents involucrats amb la cadena hotelera, és a dir, la pròpia cadena, els seus clients i els seus proveïdors (la integració ha de contemplar rebre factures de la plataforma, així com també enviar-les), d'una part, i de l'altra part, integrar la informació en els sistemes d'informació de cadascun dels intervenents en la relació comercial amb la cadena.

Una vegada que tots els agents involucrats es comuniquen emprant la plataforma, sorgeixen problemes a resoldre i que no tenen a veure amb la factura electrònica i la seva presentació o format. Estan més aviat relacionats amb la informació continguda i la semàntica exacta de cada dada. Això exigeix una solució mitjançant consultoria, que s'ha de fer amb molta cura, i en la qual cal que un consultor especialitzat en la plataforma faci d'intermediari entre la cadena de clients i proveïdors per a aconseguir l'acord entre les parts.

Pel que fa a la part logística i comercial del projecte d'implantació i per tal que el projecte tingui èxit es detecta com un element crític el fet que assumeixen al projecte com més proveïdors i clients siguin possibles. Per a assolir tanta involucració com sigui possible es fa una campanya promocionant la solució de factura electrònica entre els clients i proveïdors. La campanya inclou diferents tipus d'accions i un seguiment de l'acompliment dels objectius marcats.

Conclusions

Encara que el projecte ha anat complint les seves fases, el seu èxit no ha estat complet en no cobrir-se totes les expectatives plantejades inicialment per certes raons fonamentals:

- La massa de clients i proveïdors se sumen molt lentament al projecte. Això fa que la substitució total de les factures en paper per les electròniques planteji cada vegada un horitzó més llunyà.
- El cost d'adhesió de clients i proveïdors és més alt de l'estimat, per les diferents casuístiques i incidències a resoldre.
- Per a aconseguir enviar i rebre la major quantitat de factures de manera electrònica no queda més remei que plantejar-se adherir-se a altres plataformes de factura electrònica:

CADENA HOTELERA S.A.
 CTRA. LA MANGA S/N
 7182 - MAGALLUF
 Tel.: 971
 antonio.rovira@cadhotelera.com

FACTURA Nº: 722/136667
 FECHA: 12/08/2007
 MONEDA: EUR
 RESERVA: 156469
 LOCALIZADOR:

Cliente/Guest:
 OPERADORES TURISTICOS SL
 AVDA. DE LA LUZ, 6

Ref. Cliente/Guest Ref.:
 Bono/Voucher: 196467F9Z
 Bono/Voucher: 196467FVB

38400 - PUERTO DE LA CRUZ
 C.I.F.:

Observaciones/Comments:

iberjet

De/From	Ato	Servicio/Service	Precio/Price	Total
05/08/2007	12/08/2007	Prestacion de servicios al 7.00%	2.074,80	2.074,80
Suma Total:			2.074,80	EUR

Tipo/Type	Base Imponible/Net	I.V.A./V.A.T	Total
	7,00 %	1936,07 EUR	136,73 EUR
			2.074,80 EUR

Fecha/Date	Tipo Pago/Payment Type	Nr. Tarjeta/Card Number	Total
12/08/2007	Cta. Credito		-2074,80 EUR

Total Pagos: 0,00 EUR

RESTO A PAGAR:	2074,80 EUR
-----------------------	-------------

```

<?xml version="1.0"?>
<inv:Invoice xmlns:inv="http://www.docentime.es/Bizlayer/UBL/Invoice-1.0" xmlns:ubl="http://www.docentime.es/Bizlayer/UBL/MultipleInvoice-1.0"
xmlns:cac="urn:oasis:names:specification:ubl:schema:xsd:CommonAggregateComponents-1.0"
xmlns:cbc="urn:oasis:names:specification:ubl:schema:xsd:CommonBasicComponents-1.0"
xmlns:cc="urn:oasis:names:specification:ubl:schema:xsd:CurrencyCode-1.0" xmlns="urn:oasis:names:specification:ubl:schema:xsd:Invoice-1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <ID>722/136667</ID>
  <cbc:IssueDate>2007-08-12</cbc:IssueDate>
  <cbc:Note/>
  <TaxPointDate>2007-08-12</TaxPointDate>
  <InvoiceCurrencyCode>EUR</InvoiceCurrencyCode>
  <AdditionalDocumentReference>
    <cac:ID>196467F9Z</cac:ID>
  </AdditionalDocumentReference>
  <AdditionalDocumentReference>
    <cac:ID>196467FVB</cac:ID>
  </AdditionalDocumentReference>
  <cac:BuyerParty>
    <cac:SellerAssignedAccountID>65746</cac:SellerAssignedAccountID>
    <cac:Party>
      <cac:PartyIdentification>
        <cac:ID>B38044921</cac:ID>
      </cac:PartyIdentification>
      <cac:PartyName>
        <cbc:Name>OPERADORES TURISTICOS S.L.</cbc:Name>
      </cac:PartyName>
      <cac:Address>
        <cbc:StreetName>AVDA.DE LA LUZ, 6 ED</cbc:StreetName>
        <cbc:CityName>PUERTO DE LA CRUZ</cbc:CityName>
        <cbc:PostalZone>38400</cbc:PostalZone>
        <cbc:Region>TENERIFE</cbc:Region>
        <cac:Country>
          <cac:IdentificationCode>ES</cac:IdentificationCode>
        </cac:Country>
      </cac:Address>
    </cac:Party>
  </cac:BuyerParty>
  <cac:SellerParty>
    <cac:Party>
      <cac:PartyIdentification>
        <cac:ID>A75504976</cac:ID>
      </cac:PartyIdentification>
      <cac:PartyName>
        <cbc:Name>CADENA HOTELERA, S.A.</cbc:Name>
      </cac:PartyName>
      <cac:Address>
        <cbc:StreetName>Gremio PAR, Poligono 2</cbc:StreetName>
        <cbc:CityName>Palma de Mallorca</cbc:CityName>
        <cbc:PostalZone>07004</cbc:PostalZone>
        <cac:Country>
          <cac:IdentificationCode>ES</cac:IdentificationCode>
        </cac:Country>
      </cac:Address>
    </cac:Party>
  </cac:SellerParty>
  <cac:PaymentMeans>
    <cac:PaymentMeansCode>ZZZ</cac:PaymentMeansCode>
    <cbc:DuePaymentDate>2007-08-12</cbc:DuePaymentDate>
  </cac:PaymentMeans>
  <cac:Payment>
    <cac:ID>Cta. Credito</cac:ID>
    <cbc:PaidAmount amountCurrencyID="EUR">2074.80</cbc:PaidAmount>
    <cbc:ReceivedDate>2007-08-12</cbc:ReceivedDate>
  </cac:Payment>
  <cac:TaxTotal>
    <cbc:TotalTaxAmount amountCurrencyID="EUR">135.73</cbc:TotalTaxAmount>
    <cac:TaxSubTotal>
      <cbc:TaxableAmount amountCurrencyID="EUR">1939.07</cbc:TaxableAmount>
      <cbc:TaxAmount amountCurrencyID="EUR">135.73</cbc:TaxAmount>
      <cac:TaxCategory>
        <cac:ID>VAT</cac:ID>
        <cbc:Percent>7.00</cbc:Percent>
        <cac:TaxScheme>
          <cac:TaxTypeCode>VAT</cac:TaxTypeCode>
        </cac:TaxScheme>
      </cac:TaxCategory>
    </cac:TaxSubTotal>
  </cac:TaxTotal>
  <cac:LegalTotal>
    <cbc:LineExtensionTotalAmount amountCurrencyID="EUR">2074.80</cbc:LineExtensionTotalAmount>
    <cbc:TaxExclusiveTotalAmount amountCurrencyID="EUR">1939.07</cbc:TaxExclusiveTotalAmount>
    <cbc:TaxInclusiveTotalAmount amountCurrencyID="EUR">2074.80</cbc:TaxInclusiveTotalAmount>
  </cac:LegalTotal>
  <cac:InvoiceLine>
    <cac:ID>1</cac:ID>
    <cbc:InvoicedQuantity quantityUnitCode="PCE">1.00</cbc:InvoicedQuantity>
    <cbc:LineExtensionAmount amountCurrencyID="EUR">2074.80</cbc:LineExtensionAmount>
    <cac:Delivery>
      <cac:ID>156469</cac:ID>
      <cbc:RequestedDeliveryDateTime>2007-08-05T00:00:00</cbc:RequestedDeliveryDateTime>
      <cbc:PromisedDateTime>2007-08-12T00:00:00</cbc:PromisedDateTime>
    </cac:Delivery>
    <cac:Item>
      <cbc:Description>Prestacion de servicios al 7.00%</cbc:Description>
      <cac:TaxCategory>
        <cac:ID>VAT</cac:ID>
        <cbc:Percent>7.00</cbc:Percent>
        <cac:TaxScheme>
          <cac:TaxTypeCode>VAT</cac:TaxTypeCode>
        </cac:TaxScheme>
      </cac:TaxCategory>
    </cac:Item>
    <cac:BasePrice>
      <cbc:PriceAmount amountCurrencyID="EUR">2074.80</cbc:PriceAmount>
    </cac:BasePrice>
  </cac:InvoiceLine>
  <inv:SellerDepartment>
    <cac:PartyIdentification>
      <cac:ID>722</cac:ID>
    </cac:PartyIdentification>
    <cac:PartyName>
      <cbc:Name>CADENA HOTELERA S.A.</cbc:Name>
    </cac:PartyName>
    <cac:Address>
      <cbc:StreetName>CTRA. LA MANGA, S/N</cbc:StreetName>
      <cbc:CityName>MAGALLUF</cbc:CityName>
      <cbc:PostalZone>7182</cbc:PostalZone>
      <cac:Country>
        </cac:Country>
      </cac:Address>
    <cac:Contact>
      <cbc:Telephone>971131958</cbc:Telephone>
      <cbc:Telefax>antonio.rovira@cadhotelera.com</cbc:Telefax>
    </cac:Contact>
  </inv:SellerDepartment>
</inv:Invoice>

```

Exercicis d'autoavaluació

1. Què és un certificat electrònic i en què consisteix la CRL i l'OSCP d'una PKI?
2. En quina normativa europea es recullen les modalitats de la signatura XML? Quines són, segons l'estàndard XMLDesig?
3. Quines són les principals diferències de les modalitats de signatura electrònica XAdES i CAdES?

Bibliografia

J. Rifà, L. Huguet. *Comunicación digital: Teoría matemática de la información. Codificación algebraica. Criptología*, Ed. Masson 1991.

www.facturae.es/