

L' ÚS DE LA SIGNATURA ELECTRÒNICA EN EL PROCEDIMENT ADMINISTRATIU: PRESENT I FUTUR

M. Lourdes Simó Goberna

**Tècnica Superior del Departament de Benestar Social
Generalitat de Catalunya**

1.Introducció

Des de fa relativament poques dècades estem assistint a una implantació generalitzada a la societat actual de les anomenades TIC (Tecnologies de la Informació i de la Comunicació). Si bé aquestes noves tecnologies de comunicació i de transmissió electrònica de dades han estat usades sobre tot per al transferiment abundant d'informació entre elles, actualment el creixement cada cop més ràpid de les anomenades "autopistes de la informació" ha fet que els sistemes de intercanvi electrònic de dades s'hagin d'incloure en unes infraestructures creades expressament per aprofitar totes les possibilitats que Internet genera per al desenvolupament econòmic.

La signatura electrònica, en totes les seves formes, constitueix una eina fonamental en l'establiment de relacions comercials via Internet, i de fet, les normatives dels diferents països del món, en principi, han anat adreçades especialment a l'ús d'aquest sistema de seguretat dins d'aquest àmbit.

Simultàniament, les administracions públiques de la Comunitat Europea, de l'Estat espanyol i de les Comunitats Autònomes i els Ens Locals han anat introduint l'ús de les TIC en les seves relacions internes i interadministratives.

La signatura electrònica contribueix a la modernització del procediment administratiu, tant pel que fa en les relacions interadministratives, de l'administració pública amb els ciutadans, i en el sí d'aquesta mateixa administració.

De la importància de l'aplicació de la signatura electrònica adquirida com a sistema de seguretat dintre de la implantació generalitzada de les TIC a les administracions públiques constitueixen bons exemples els diferents congressos i trobades realitzats aquests darrers anys per tal d'intercanviar experiències sobre un tema tant important i alhora tan poc desenvolupat tècnicament, com veurem. Els exemples són diversos: dintre del programa "Euskadi en la sociedad de la información", l'administració autonòmica del País Basc va organitzar unes jornades sobre la signatura electrònica els dies 9 i 10 d'octubre de 2001, en els transcurso de les quals es van presentar diversos projectes pilot engegats en diferents administracions públiques, entre elles l'administració de la Generalitat de Catalunya; la darrera trobada celebrada sobre la signatura electrònica s'ha dut a terme a Sabadell, en forma del seminari anomenat "La signatura electrònica en la transformació de l'administració local", coordinat per Xavier Tarrés, de l'Ajuntament de Sabadell i patrocinat, entre d'altres entitats pel Col·legi Oficial d'Enginyers Industrials de Catalunya amb la col·laboració de la Diputació de Barcelona, els dies 9 i 10 de juliol d'enguany. També en aquestes jornades –a les quals, tot s'ha de dir, no he tingut el plaer d'assistir per trobar-me de vacances- s'han presentat diferents projectes pilot, i alhora s'han valorat els projectes engegats anys enrera. D'aquí uns dies (concretament, del 15 al 18 d'octubre) se celebraran a La Corunya les

VII Jornadas sobre Tecnologías de la Información para la Modernización de las Administraciones Públicas (TECNIMAP' 2002), en el transcurso de las cuales se hablará de la implantación de l'ús de la signatura electrònica en les Administracions Públiques.

2. Què és i per què serveix la signatura electrònica?

La desaparició del paper i de la signatura manuscrita requereixen de la utilització de mecanismes que donin garanties contra possibles suplantacions i alteracions en la comunicació via Internet. Així mateix, quan des de l'administració pública hem acceptat aquesta via per a la modernització en les nostres relacions, necessitem assegurar la identitat i la voluntat d'aquells que participen en l'intercanvi electrònic.

Segons els experts, la seguretat en les xarxes telemàtiques s'ha de sostenir en quatre principis, els quals s'aconsegueixen amb l'aplicació de diferents mitjans tècnics:

- a) **AUTENTICACIÓ:** S'ha de garantir que un document electrònic és autèntic des del punt de vista de la seva autoria. Tecnològicament, aquest principi s'acredita mitjançant l'emissió de certificats digitals.
- b) **INTEGRITAT:** La comunicació ha d'arribar al receptor tal com la va crear l'emissor, sense manipulació de les dades.
- c) **CONFIDENCIALITAT:** Es tracta d'evitar que el contingut de la comunicació sigui vist per a persones diferents al destinatari de la tramesa. Això s'aconsegueix mitjançant l'encriptació. Per a la comunicació encryptada és necessària l'existència de dues claus: una clau pública i una altra privada, que han de conèixer cadascuna de les parts implicades per tal de xifrar i desxifrar la comunicació.
- d) **NO REBUIG O NO REPUDI:** Per dificultar que l'autor de la transacció negui l'autoria de la comunicació.

El concepte de signatura electrònica no fa referència a cap tecnologia concreta, i és la manera de referir-se, de forma genèrica, a qualsevol sistema que busqui una equivalència funcional amb la signatura manuscrita. Breument: és la manera de referir-se a la signatura emesa per mitjans electrònics. En aquest sentit, la signatura electrònica ha de poder acreditar que compleix amb els principis esmentats, ja que forma part de l'intercanvi comunicatiu en xarxes obertes com Internet.

Com s'ha dit al principi, podem distingir diferents tipus de signatures electròniques:

2.1. SIGNATURA ELECTRÒNICA ORDINÀRIA

Està definida, en primer lloc, per la Directiva 1999/93/CE del Parlament Europeu i del Consell, de 13 de desembre de 1999 (a partir d'ara D 1999/93/CE), per la qual s'estableix un marc comunitari per a la signatura electrònica. La normativa elaborada a l'Estat espanyol obeeix a aquest marc comunitari. De fet, la definició que es troba a l'art. 2 lletra a del Reial Decret Llei 14/1999, de 17 de setembre, sobre signatura electrònica, no difereix gens de l'establerta en la directiva comunitària: aquella és un conjunt de dades, com codis o claus criptogràfiques privades, en forma electrònica, que s'associen inequívocament a un document electrònic (és a dir, contingut en un suport

magnètic, com un disquet, CD-Rom o disc dur d'un ordinador, però no paper), que permet identificar el seu autor.

Si interpretem correctament aquesta definició, la característica principal de la signatura electrònica ordinària és la creació d'un vincle estàtic i irrevocable entre el signatari i el document que signa. És a dir: busca l'acceptació i l'ús amb la finalitat d'acreditar una entitat (o un particular) i associar-la unes dades concretes, però no busca acreditar la fiabilitat.

La voluntat d'usar un mecanisme electrònic com equivalent de la signatura manuscrita, li atorga la condició de signatura electrònica. Els diferents mecanismes són:

1. Signatura electrònica digitalitzada a través d'un escàner.
2. La signatura digital, és a dir, una signatura electrònica associada a l'ús de la criptografia asimètrica o de clau pública. La criptografia desenvolupa diferents mecanismes de xifratge (un d'ells, el més usat actualment, és l'algoritme HASH, amb el qual es transforma un text de longitud arbitrària a un nombre fix de bits.
3. Mecanismes d'autenticació: És el més habitual en l'àmbit del comerç electrònic. Entenem per autenticació, seguint a l'investigador Arturo Ribagorda, un servei de seguretat l'objecte del qual es corrobora la identitat al·legada per un usuari que participa en una sessió. Ribagorda considera que hi ha tres procediments habituals d'autenticació:

-El que ell defineix com QUÈ SÉ?: un password, contrasenya o PIN (número d'identificació personal).

-El que respon a la pregunta QUÈ TINC?: un objecte en el nostre poder (una targeta, per exemple) que conté dades nostres.

-El que respon a la pregunta QUÈ SOC?: un procediment biomètric de reconeixement d'alguna cosa que no té cap altre persona (l'iris, l'empremta digital), o un tret de comportament (reflectit a la signatura manuscrita).

Si analitzem aquests tres procediments d'autenticació, podem dir que vinculen efectivament la persona amb el missatge que transmet? És habituals que les entitats d'estalvi ens proporcionin dos mitjans d'autenticació: un, la targeta amb banda magnètica (objecte en el nostre poder), i l'altre, un PIN (o número d'identificació personal). Molts contractes financers estableixen un dels dos mitjans com a signatura electrònica del usuari.

Malgrat l'art. 5.2. de la D 1999/93/CE estableix que els Estats membres vetllaran per tal de no negar eficàcia jurídica ni admissibilitat com a prova en procediments judicials a la signatura electrònica pel fet de ser-ho i no basar-se en certificat reconegut ni expedit per un proveïdor de serveis de certificació acreditat, o no estigui creada per un dispositiu segur de creació de signatura, el sentit comú ens permet pensar que no en tots els casos l'ús d'un procediment habitual d'autenticació, com els que he esmentat, tindrà els efectes immediats d'una signatura manuscrita.

2.2. SIGNATURA ELECTRÒNICA AVANÇADA

També definida en la Directiva comunitària i en el Reial Decret Llei estatal, en l'article 2 lletra b.

Quan la identificació entre el signatari i el missatge signat és altament fiable i permet detectar qualsevol alteració no autoritzada del missatge o del document, perquè els dispositius emprats en la creació de la signatura són segurs, i perquè en el procés ha intervingut un prestador de serveis de certificació acreditat, parlem de signatura electrònica avançada.

Les propietats de la signatura electrònica avançada són les següents:

1. Vincula la signatura al signatari de manera única.
2. Identifica el signatari.
3. Està creada amb mitjans que el signatari manté sota el seu control.
4. Està vinculada a les dades a les que es refereix, de manera que es pot detectar qualsevol canvi ulterior.

Aquestes propietats s'aconsegueixen amb dos mitjans tecnològics principalment:

-Amb el certificat digital, proporcionat per una Entitat de Certificació. Aquesta és la que alguns autors anomenen "tercera part de confiança", ja que garanteix que una determinada clau pública, vinculada a una de privada, són d'una persona en concret i no d'una altra. L'Entitat de Certificació signa digitalment la identitat més la clau pública i genera el certificat digital.

El certificat digital pot estar ubicat en diferents suports físics: el disc dur de l'ordinador, un disquet, una targeta intel·ligent o qualsevol dispositiu (token) que permeti emmagatzemar un certificat digital.

-Amb una infraestructura de clau pública (PKI), la qual pot definir-se,

*"com el conjunt de maquinari, programari, persones, polítiques d'actuació, normativa i procediments necessaris per crear, gestionar, emmagatzemar, distribuir, renovar i revocar certificats digitals basats en criptografia de clau pública, en resum, parlem de la "fàbrica" de certificats digitals en el sentit més ampli de la paraula, que inclou tant la xarxa de distribució com el servei de suport i manteniment."*¹

La infraestructura de clau pública o PKI ha de proporcionar garanties a tercer respecte dels certificats digitals emesos i evitar que els titulars d'aquests puguin repudiar les signatures realitzades.

Jurídicament, la signatura electrònica avançada no té equivalència immediata amb la signatura manuscrita, i té una càrrega de prova tradicional. Permet que diferents tecnologies, com la signatura digital (a la qual m'he referit en parlar de la signatura electrònica ordinària) rebin efectes jurídics equivalents.

¹ Document informatiu: assegurement de les relacions electròniques. El certificat digital i la signatura electrònica, Consultoria de sistemes i Tecnologies de la Informació, Centre de Telecomunicacions i Tecnologies de la Informació, Generalitat de Catalunya, Abril de 2001, p.19.

2.3. SIGNATURA ELECTRÒNICA RECONEGUDA

Malgrat no està definit en la normativa vigent, la signatura electrònica reconeguda és un concepte elaborat per la doctrina a partir de l'article 5.1. de la D 1999/93/CE:

“ [...] los Estados miembros garantizaran que la firma electrònica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma :

a) satisfaga el requisito jurídico de una firma en relación con los datos en forma electrònica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel; y

b) sea admisible como prueba en procedimientos judiciales.”

Es tracta, doncs, d'un tipus de signatura electrònica avançada, la qual, a més de complir amb els requisits d'aquesta, ha de basar-se en un certificat digital reconegut i creada per un dispositiu segur, que permeti que l'autor no rebutgi la signatura (un programa o un aparell informàtics configurats per aplicar les dades de creació de firma, per exemple). La normativa estatal, en el Reial Decret esmentat, estableix els requisits i característiques que han de complir tant els certificats reconeguts com els prestadors de serveis de certificació (arts. 8 a 12).

En l'aspecte jurídic, rep els efectes directament de la Llei, i així s'equipara immediatament a la signatura manuscrita.

Atesa la seva importància pública, la doctrina es mostra divergent pel que fa a qui ha de ser el signatari en la firma electrònica reconeguda: Ignacio Alamillo sosté que ha de ser una persona física, el qual no és necessàriament el titular o subscriptor del certificat – que pot ser una persona jurídica-, amb la qual cosa el signatari es el posseïdor de la clau privada de signatura del subscriptor, amb la seva autorització, expressa o tàcita. Alamillo considera que es llavors quan es pot parlar de que la signatura electrònica equival a la signatura manuscrita, i compleix amb el requisit de l'article esmentat a la directiva comunitària. En cas contrari, si la signatura electrònica la fa una màquina, tornem a trobar-nos amb la signatura electrònica avançada, la qual no s'equipara directament a la signatura manuscrita. Agustín Madrid fa una altra lectura de l'article esmentat de la directiva comunitària i considera que el signatari pot ser directament una persona jurídica.

De fet, l'esborrany de l'avantprojecte estatal de llei de firma electrònica es decanta per aquesta última interpretació, com veurem més endavant, i preveu la possibilitat d'expedir certificats a persones jurídiques i considerar-les en conseqüència com a signataris.

2.4. SIGNATURA ELECTRÒNICA ACREDITADA

Aquest concepte no està definit en cap text legal de la Unió Europea: només vigent a l'Estat espanyol, la seva definició i característiques s'han elaborat a través de

l'existència dels sistemes voluntaris d'acreditació. Segons l'art. 2.13 de la directiva comunitària, l'acreditació voluntària és:

“todo permiso que establezca derechos y obligaciones específicas para la prestación de servicios de certificación, que se concedería, a petición del proveedor de servicios de certificación interesado, por el organismo público o privado encargado del establecimiento y supervisión del cumplimiento de dichos derechos y obligaciones, cuando el proveedor de servicios de certificación no esté habilitado para ejercer los derechos derivados del permiso hasta que haya recaído la decisión positiva de dicho organismo”.

Un exemple de signatura electrònica acreditada pot ser el sistema definit per un sector de la indústria de serveis financers, per exemple, per a les operacions d'intercanvi de grans quantitats de fons monetaris.

Un altre exemple pot ser el de la signatura de documents públics, en els quals, a més dels requisits de la signatura electrònica reconeguda, es demanen requisits addicionals, per exemple, l'ús de segells de temps fiables, l'arxiu del document i la verificació de la capacitat del signatari per notari públic.

L'ús de la signatura electrònica per part de les administracions públiques requereix condicions addicionals, per la qual cosa, potser seria una bona idea establir sistemes voluntaris d'acreditació. A l'administració estatal espanyola, el sistema voluntari d'acreditació es correspon únicament als requisits de la signatura electrònica reconeguda, i concretament amb l'acreditació del prestador de serveis de certificació que expedeix certificats reconeguts al públic. En aquest casos, sembla que es confon la figura de la supervisió amb la de l'acreditació, ja que el prestador que declara emetre certificats reconeguts es supervisat per l'autoritat competent i si la seva declaració és incorrecta, se'l pot sancionar (arts. 16 a 18 del RDLI 14/1999).

El sistema voluntari d'acreditació reforça la signatura electrònica reconeguda. A continuació, seguint a Ignacio Alamillo, cito una petita llista d'elements que poden configurar una signatura electrònica acreditada:

1. Segell de temps.
2. Presència personal del firmant en el moment de signar.
3. Arxiu del document signat.
4. Inclusió d'informació sobre el firmant a la signatura (poders, representació, etc.)
5. Reforç dels algoritmes de signatura.
6. Múltiples signatures requerides.
7. Restriccions pel que fa als firmants.

Alguns d'aquests elements estan pensats per al nou DNI electrònic que preveu la futura llei estatal de firma electrònica.

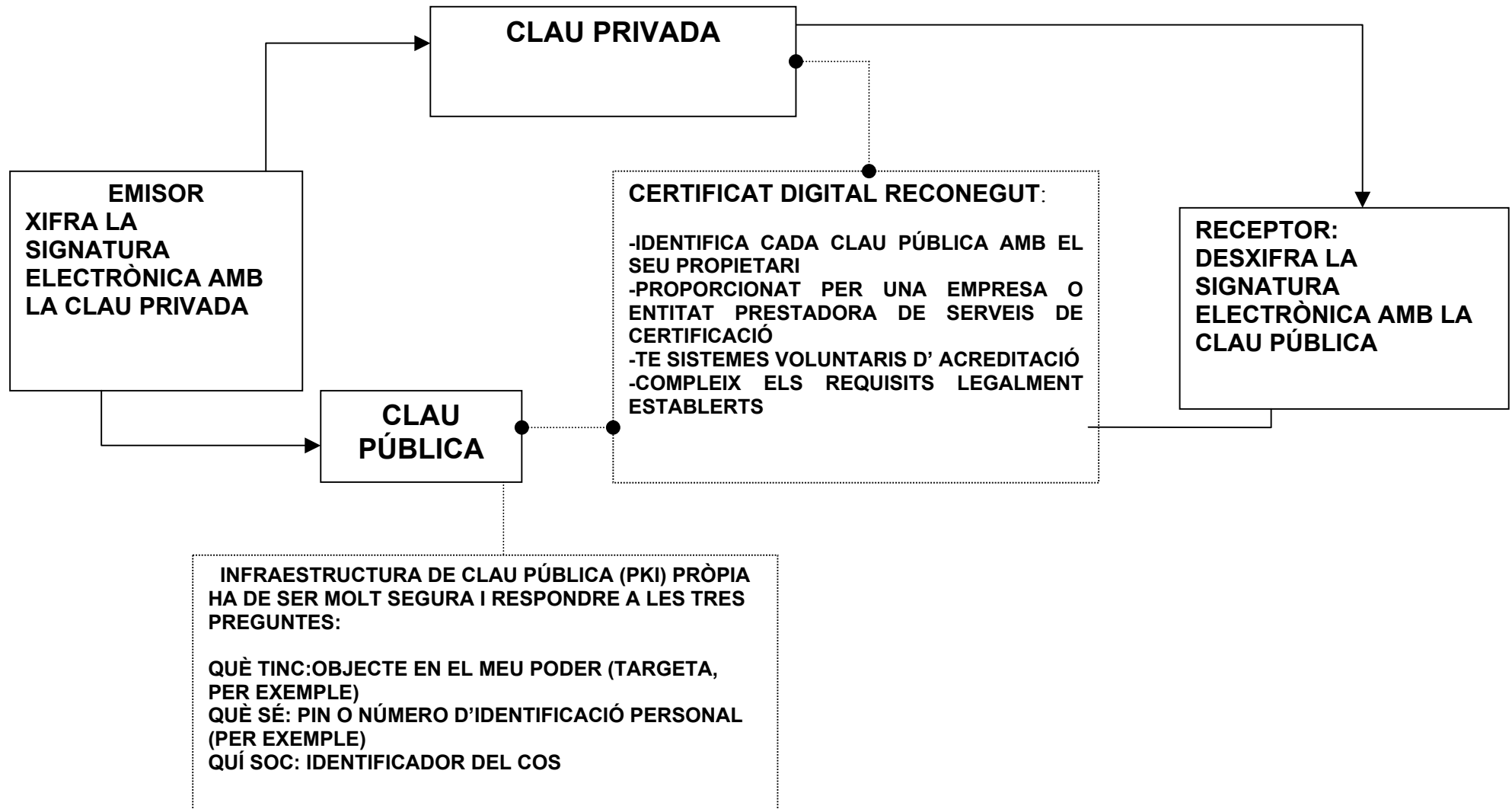
Aquest tipus de firma és l'únic que permet equiparar a tots els efectes jurídics la signatura electrònica a la manuscrita, amb càrrega de prova invertida.

A Itàlia s'ha implantat recentment una proposta doctrinal de signatura electrònica, que s'ha denominat SIGNATURA ELETTRÓNICA LEGITIMADA. Igual que la signatura

electrònica acreditada, jurídicament té una equivalència immediata a la signatura manuscrita, i a més – i aquesta és la novetat- equival a un document públic.

A la pàgina següent, hem elaborat un esquema del concepte de signatura electrònica acreditada.

LA SIGNATURA ELECTRÓNICA ACREDITADA



3. Com s'apliquen els diferents tipus de signatures electròniques a les Administracions Públiques i quina és la seva regulació jurídica?

A l'administració de la Generalitat de Catalunya, la implantació de l'ús de la signatura electrònica en els tràmits administratius, interns i en relació amb els ciutadans, s'emmarca en el projecte Administració Oberta de Catalunya (AOC), el qual va ser aprovat pel Govern de Catalunya el 13 de juliol de 1999, i que està sent dirigit pel Comissionat per a la Societat de la Informació (CSI), dependent del Departament de Universitats, Recerca i Societat de la Informació (DURSI).

El projecte té diverses fases, la primera de les quals consisteix en la generalització de les TIC dintre de la mateixa administració: la creació d'una Intranet corporativa (pàgina web comuna a tots els departaments i que permet als empleats públics compartir recursos comuns i accedir a tota la informació que necessiten), i d'Intranets d'àmbit departamental, la implantació de l'ús generalitzat d'un correu electrònic segur i, finalment, la generalització de l'ús de la signatura electrònica.

Pel que fa a l'ús de la signatura electrònica, el mes de setembre de l'any 1999, es va posar en marxa una prova pilot, amb la qual 1500 funcionaris i funcionàries dels Departaments de Presidència i d'Economia i Finances van disposar de signatura electrònica. La pretensió de la prova era que ambdós departaments es comunicessin tant de forma interna com entre ells a través de documents firmats electrònicament.

En la prova pilot, els treballadors i treballadores públics s'havien d'identificar a través d'un certificat electrònic ubicat en un disquet. Aquest certificat garantia la identitat de qui emetia el document, la integritat de la documentació que es trametia i la seva confidencialitat.

Observem que quan es va engegar aquesta prova pilot tot just s'havia publicat o estava a punt de publicar-se el RDL 14/1999 estatal, i estava prevista la publicació de la directiva comunitària 1999/93/CE el desembre d'aquell mateix any. Les iniciatives, en l'àmbit de la comunitat europea i de l'estat espanyol, no van començar fins uns mesos més tard: la presentació del projecte e-Europe, gestionat per la Comissió de les Comunitats Europees, es va fer el mes de desembre de 1999, mentre que el projecte Info XXI, gestionat per la Comisión Interministerial de la Sociedad de la Información de las Nuevas Tecnologías, del Govern espanyol, no es va presentar fins a gener del 2000.

En aquest sentit, i tenint en compte que no havia un marc jurídic regulador, podem dir que el projecte AOC va ser pioner i, en cert sentit, agosarat.

L'11 de gener de 2000, el CSI va publicar el balanç de la primera fase del projecte AOC, la qual es cloïa el mes de març d'aquell mateix any amb un informe adreçat al Govern de la Generalitat.

Al mateix temps, el projecte AOC entrava a formar part d'un Pla més ambiciós, per més extens i més llarg en el temps: "Catalunya en Xarxa. Pla estratègic per a la Societat de la Informació", del qual formen part totes les administracions que hi ha a Catalunya. Aquest Pla estratègic està gestionat pel CSI i Localret, consorci local que agrupa la majoria de municipis de tot Catalunya.

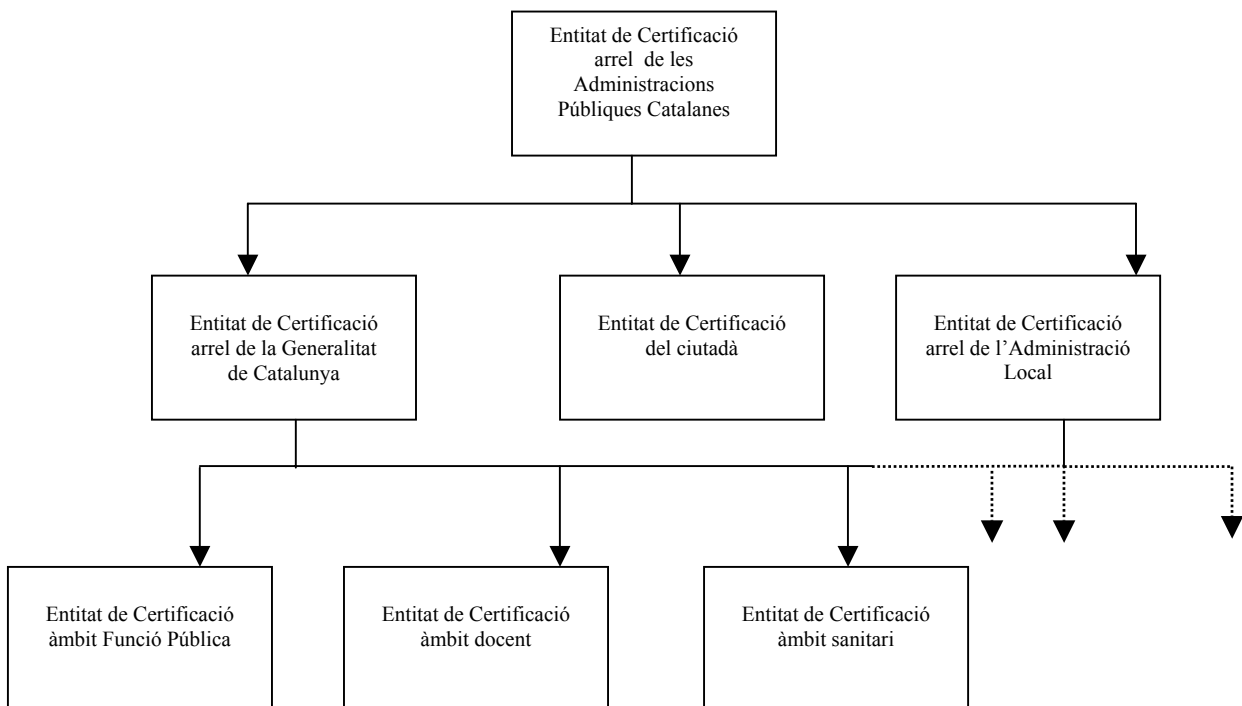
El document, que constitueix una reflexió sobre el pla estratègic, presentat al Parlament de Catalunya el 14 d'abril de 1999, s'estructura en set grans àmbits d'actuació, dels

quals ens interessa el referent a Administració i Serveis al Ciutadà. De les iniciatives previstes en aquest àmbit, la tercera es refereix a la signatura electrònica qualificada del ciutadà. Malgrat no concretar-ho, el projecte es refereix a allò que més amunt hem anomenat signatura electrònica reconeguda.

Així preveu un sistema d'identificació electrònica que inclogui la implantació progressiva d'una targeta electrònica per al possible ús multifuncional (targeta de tràmits amb l'administració, ús sanitari...) i la creació d'entitats certificadores o acreditadores de les persones o ens.

Finalment, per acord del Govern de 6 de febrer de 2001, es va encarregar al Centre de Telecomunicacions i Tecnologies de la Informació (CTTI) la creació d'una infraestructura de clau pública per a l'Administració de la Generalitat. El CTTI és el titular de la certificació arrel de la jerarquia.

En els jornades esmentades més amunt sobre signatura electrònica organitzades per l'Administració del Govern d'Euskadi, Ramon Martín Miralles López, ponent i representant de CTTI, va mostrar la jerarquia de les certificacions públiques segons el projecte AOC i el pacte LOCALRET per a les Administracions Públiques catalanes, i que reproduïxo a continuació:



El model d'infraestructura de clau pública (PKI), creat pel CTTI, es basa en tres principis generals:

- a) Preveure la creació d'una entitat de certificació per als empleats públics de l'Administració de la Generalitat.
- b) Preveure la possibilitat de creació d'entitats de certificació sectorials, per tal de satisfer les necessitats de col·lectius concrets: docents, sanitaris, policia autonòmica, justícia, etc.
- c) Preveure la seva vinculació a una entitat catalana de certificació, a la que també es vincularien la entitat de certificació dels ens locals, com la dirigida a la emissió de certificats digitals als ciutadans (targeta unificada de serveis –TUS- o targeta intel·ligent).

La infraestructura creada pel CTTI conté els elements següents:

- 1) Elements físics: centre de certificació digital amb grans mesures de seguretat i equipaments.
- 2) Elements tecnològics: seleccionant els programes que han de prestar serveis a la certificació digital.
- 3) Elements organitzatius: documentant i implantant tots els aspectes vinculats a l'activitat pròpia de la prestació de serveis de certificació digital (polítiques i plans de seguretat, arxiu, pràctiques i polítiques de certificació, etc.).

Aquestes infraestructures són comuns per a totes les entitats de certificació. El suport físic dels certificats digitals són les targetes criptogràfiques, formatejades per tal de poder incorporar-hi diferents certificats digitals i serveis complementaris. La imatge física de la targeta es el d'una targeta ordinària, però s'hi poden incorporar alguns elements de personalització en funció de l'entitat de certificació.

El Pacte per a la promoció i el desenvolupament de la societat de la informació a les Administracions Públiques Catalanes, subscrit pels partits polítics presents al Parlament de Catalunya, el dia 23 de juliol de 2001, preveia dintre del projecte AOC (Administració Oberta de Catalunya, ja esmentat), que a finals del 2001 i a principis del 2002, els treballadors i treballadores de les administracions públiques catalanes disposessin en primer lloc de formació suficient en l'àmbit de l'administració electrònica, i en segon lloc, de certificat i de signatura digital.

Els tipus de certificats emesos són tres:

- El certificat que compleix amb els requisits previstos al Reial Decret estatal i a la directiva europea, i que per tant genera signatura electrònica reconeguda.
- El certificat de identificació personal: per generar signatura electrònica avançada.
- El certificat de xifrat: per tal de preservar la confidencialitat en aquells intercanvis en els quals sigui necessari protegir les dades d'accés per part de tercers. Això generaria una signatura electrònica reconeguda.

Actualment, ja s'està duent a terme l'emissió de certificats en forma de lots: l'exemple més recent el tenim en els concursos generals de mèrits i capacitats (de trasllats) en els

quals s'ha pogut participar telemàticament, ja que als participants s'els va proporcionar un certificat que va generar una signatura electrònica reconeguda.

Normativament, el Decret 324/2001, de 4 de desembre, relatiu a les relacions entre els ciutadans i l'administració de la Generalitat de Catalunya a través d'Internet, ja regula els procediments telemàtics que requereixen o no, certificat digital (arts. 15 i 16) i , el que més ens interessa: dóna competència als consellers dels diferents departaments de la Generalitat per aprovar els procediments que es poden realitzar per sistemes telemàtics i els programes i aplicacions que s'han d'utilitzar en la seva tramitació (art. 11), així mateix, es preveu que, prèvia consulta amb les assessories jurídiques de cada departament, es publiquin aquest procediments al DOGC.

Ja s'han creat diferents agències catalanes de certificació: l'Agència Catalana de Certificació Digital, i l'Empresa de Serveis Públics Electrònics, per exemple. En l'àmbit estatal podem posar altres exemples: la Fàbrica Nacional de Moneda i Timbre (FNMT) té en marxa el projecte CERES (Certificación Española) i que consisteix en una PKI dotada d'una entitat pròpia de certificació que permet autenticar i garantir la confidencialitat i integritat de les comunicacions entre ciutadans, empreses i altres institucions i administracions a través de xarxes obertes de comunicacions. La FNMT ha signat convenis per a la prestació de serveis de seguretat en les transaccions telemàtiques amb les administracions de diferents comunitats autònomes i ajuntaments arreu de l'Estat².

CERES utilitza termes i sistemes criptogràfics basats en criptosistemes de clau pública amb dues característiques bàsiques:

-La identitat de l'usuari, igual que la seva capacitat de signatura, es troba emmagatzemada en una targeta intel·ligent (el document d'identificació electrònica, informàtica i telemàtica), que no pot ser accessible excepte pel propietari quan introdueix el seu PIN , similar a la clau d'una targeta de crèdit.

-El sistema és completament transparent a l'usuari, és a dir, no necessita cap tècnica criptogràfica per realitzar o verificar una signatura electrònica o desxifrar un missatge.

Pel que fa a la legislació en l'àmbit de l'Administració estatal, podem consultar l'esborrany de l'avantprojecte de Llei de signatura electrònica, la principal novetat del qual és la regulació del Document Nacional d'Identitat electrònic (DNI) i dels certificats de persones jurídiques. En l'exposició de motius es posa èmfasi en les novetats dirigides a impulsar l'ús generalitzat de la signatura electrònica en tots els àmbits de l'activitat econòmica i social. Per exemple, es preveu la incorporació de facilitats d'identificació i signatura electròniques al DNI, per tal que es pugui usar en l'àmbit telemàtic per identificar el seu titular i permeti signar i verificar la signatura electrònica en aquelles circumstàncies en que s'hagi d'emprar.

El DNI electrònic inclourà els elements tecnològics necessaris per signar i verificar la signatura de documents electrònics, però l'òrgan emissor haurà de procurar la interoperabilitat amb les productes de firma electrònica de més gran acceptació del mercat. Els certificats continguts en els DNI electrònics coexistiran i fins i tot podran utilitzar-se amb altres productes, com els anomenats "certificats d'atributs" que indiquen una circumstància específica del seu titular, o els certificats de persones jurídiques, novetat de la futura llei de signatura electrònica.

² Apud. *Libro blanco para la mejora de los servicios públicos*, Ministerio de Administraciones Públicas, Madrid, 2000, p. 135.

La possibilitat de donar certificats a persones jurídiques i de considerar-les, conseqüentment com a firmants, es fonamenta en la diferencia existent entre els mecanismes de signatura electrònica i els de signatura manuscrita, i en la necessitat de reconèixer l'existència de certificats els quals, emesos a nom de persones jurídiques, s'utilitzen habitualment per diferents finalitats.

Però també l'exposició de motius de la llei ja estableix que només podrà haver per cada certificat emes a nom d'una persona jurídica una persona física autoritzada per utilitzar les dades de signatura de l'entitat, la qual es responsabilitzarà del compliment dels deures de diligència inherents a la condició de signatari, malgrat que no ho sigui "strictu sensu".

El *Libro blanco para la mejora de los servicios públicos* preveu que cap a desembre de l'any 2004 s'estengui l'ús de la firma electrònica i els sistemes de seguretat en les transaccions que efectuïn els ciutadans amb l'Administració, per tal de garantir la seva autenticitat i privacitat (p. 169).

Amb la finalitat de compartir esforços i recursos, el 3 de juny d'enguany, el ministre d'Administracions Públiques, Jesús Posada i la consellera de Governació i Relacions Institucionals, Núria de Gispert, van signar un conveni de col·laboració amb la finalitat de fer possible una nova etapa en les relacions interadministratives.

En relació a la signatura electrònica, el conveni preveu que es concretin els detalls tècnics i reglamentaris que garanteixin la interoperabilitat entre els centres de certificació de l'administració de l'Estat i els de la Generalitat, i que els ciutadans i les empreses puguin utilitzar la signatura electrònica en condicions d'igualtat i de màxima facilitat quan intervingui més d'una Administració en la prestació de serveis.

L'ús de les TIC i especialment de la signatura electrònica obligarà en un futur no molt llunyà a modificar la legislació vigent pel que fa al procediment administratiu, El Pla estratègic Catalunya en Xarxa es preveu la possibilitat de modificar la Llei de Règim Jurídic de les Administracions Públiques (Llei 30/1992) i el Text Refós de la Llei de Contractes de l'Estat.

4. Conclusions

Deixant de banda els panorames exclusivament legals i tècnics, els quals, com es pot apreciar, es troben en vies d'un ràpid desenvolupament, hem de qüestionar-nos si la implantació de la signatura electrònica, així com d'altres eines de les TIC a les administracions públiques servirà per canviar l'estructura organitzativa tradicional (i, tot s'ha de dir, anquilosada). L'esperit de la directiva europea, concretament el "considerando" núm. 20,

"Unos criterios armonizados en relación con la eficacia jurídica de la firma electrónica mantendrán un marco jurídico coherente en toda la Comunidad. Las legislaciones nacionales establecen requisitos divergentes con respecto a la validez jurídica de las firmas manuscritas[...]"

ha de poder aplicar-se a casa nostra. Hem vist les darreres iniciatives per acostar les administracions públiques autonòmiques i locals a l'administració estatal, però hem de dir –i en això coincideixo plenament amb Juan Ignacio Criado i M. Carmen Ramilo

(2001), en que si no hi ha un compromís polític exprés per liderar els processos de canvi, les iniciatives i innovacions tecnològiques dintre de l'administració pública no serviran per res més que per constituir una font d'ingressos per a les empreses que instal·len les aplicacions informàtiques, proporcionen les certificacions digitals, les agències de protecció de dades, etc. La signatura electrònica, així com les altres TIC en els administracions públiques seran útils mitjançant un nou disseny estratègic de l'organització. Possiblement, aquest nou disseny portarà implícits una redefinició dels objectius, les estructures organitzatives i les fórmules de gestió dels serveis, i el que és més important, aquests fets no solament han de donar-se en l'entorn d'Internet, o virtual, sinó també s'han d'estendre a l'administració tradicional.

Barreres n'hi ha moltes: les lleis, com hem vist, són molt recents, la més important encara està en fase d'avantprojecte (la Llei estatal de firma digital). Molts cops, dintre de la mateixa organització administrativa, les assessories jurídiques i el personal al servei de l'administració pública recela dels nous sistemes, per la manca de formació i l'escassa experiència. D'aquesta manera, una nova tecnologia, com la signatura electrònica pot arribar a complicar-se, ja que se l'imposen requisits més severos que els utilitzats amb els mètodes tradicionals (qui no ha sentit dir a un company o companya de treball la frase: "prefereixo presentar els papers signats manualment, i així acabaré abans"?).

El que és més important, i repetim: el marc tecnològic avança més ràpidament que el marc normatiu.

El procediment administratiu tradicional està dissenyat en funció de les necessitats dels òrgans de gestió. Un mateix fet pot generar a la mateixa Administració expedients diferents, però que contenen les mateixes dades, la mateixa documentació etc. Un clar exemple el constitueix la gestió del personal al servei de l'administració pública. Qui no ha tingut – i, per desgràcia, segueix tenint- problemes quan ha canviat de departament, dintre d'una mateixa administració?(triennis no pagats, serveis prestats no reconeguts, i un llarg etcètera). Enguany, a l'administració de la Generalitat de Catalunya, tot just s'ha implantat la participació telemàtica en els concursos generals de mèrits i capacitats, popularment coneguts com a concursos de trasllats.

Ciudadans i ciutadanes ensopeguen un cop i un altre amb un sistema tradicional de registre, el qual segueix demanant-los la mateixa documentació, malgrat ja tenir-la arxivada, etc.

Els procediments, en definitiva, no es redissenyen contínuament, com seria desitjable, amb l'objectiu de ser útils als gestors públics i als ciutadans.

Finalment, com a gestora pública, m'agradaria reproduir, sense que això portés a interpretacions equívokes, una cita del clarividient treball de Juan Ignacio Criado i M. Carmen Ramilo, per tal de que serveixi de reflexió en aquesta taula:

" [...] si bien las TIC e Internet son herramientas con un enorme potencial para racionalizar el funcionamiento de las Administraciones públicas, es necesaria una clara apuesta al más alto nivel político y directivo para afrontar el reto de la e-Administración y superar los problemas, barreras y amenazas para su desarrollo. De ahí el interés del estudio de los proyectos para la promoción de la e-Administración desde una perspectiva politológica. "

A bon entenedor...

Moltes gràcies.

BIBLIOGRAFIA

PÀGINES WEB CONSULTADES

- Autoritat de Certificació de la Generalitat de Catalunya (AC-GenCat). <http://portal.gencat.intranet>.
- Comissionat per a la Societat de la Informació. <http://www.gencat.es/csi>
- Euskadi en la Sociedad de la Información. <http://www.ivap.com>
- Generalitat de Catalunya. Departament de Governació i Relacions Institucionals. <http://www.gencat.es/governacio-ri>
- Generalitat de Catalunya. Departament de Universitats, Recerca i Societat de la Informació. <http://dursi.gencat.es>
- LocalRet. <http://www.localret.es>
- Sabadell Universitat. La signatura electrònica en la transformació de l'administració local. <http://www.sabadelluniversitat.org>.
- Projecte INFO XXI: <http://www.infoxxi.es>
- TECNIMAP'2002: <http://www.tecnimap.com>
- Tutorial de firma electrònica. <http://www.ingenieroseninformatica.org>

LLIBRES, ARTICLES I DOCUMENTS DE CONSULTA

- Alamillo, Ignacio: "Tipología legal de la firma electrónica en la Unión Europea"(2001), Libro ALFA-REDI.
- Catalunya en xarxa. Pla Estratègic per a la Societat de la Informació* (1999), Comissionat per a la Societat de la Informació.
- Criado Grande, Juan Ignacio- M. Carmen Ramilo Araujo (2001): "e-Administración: ¿un reto o una nueva moda? Problemas y perspectivas de futuro en torno a Internet y las Tecnologías de la Información y la Comunicación en las Administraciones Públicas del siglo XXI", Instituto Vasco de Administración Pública.
- Document informatiu: assegurament de les relacions electròniques. El certificat digital i la signatura electrònica* (2001), Consultoria de sistemes i Tecnologies de la Informació, Centre de Telecomunicacions i Tecnologies de la Informació, Generalitat de Catalunya, Abril de 2001.
- Libro blanco para la mejora de los servicios públicos* (2000), Ministerio de Administraciones Públicas.
- Madrid, Agustín (2001): "Aspectos jurídicos de la identificación en el comercio electrónico", *Derecho del Comercio Electrónico*, La Ley.
- Ribagorda, Arturo (2001): "Seguridad informática", *Derecho del Comercio Electrónico*, La Ley.

LEGISLACIÓ I NORMATIVA

- Borrador de Anteproyecto de Ley de firma electrónica (consultable a través de la pàgina web del Ministerio de Administraciones Públicas: <http://www.map.es>).
- Decreto 324/2001, de 4 de diciembre, relativo a las relaciones entre los ciudadanos y la Administración de la Generalitat a través de Internet.
- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 11 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica.

PACTES, CONVENIS I ACORDS DE GOVERN INTERADMINISTRATIUS

-Conveni de col·laboració entre el Ministerio de Administraciones Públicas i el Govern de la Generalitat, per al desenvolupament de l'Administració Electrònica (3 de juny de 2002).

-Pacte per a la promoció i el desenvolupament de la Societat de la Informació a les Administracions Públiques catalanes (entre el Govern de la Generalitat i els Ajuntaments i Corporacions Locals, agrupats en el consorci Localret) (23 de juliol de 2001).