



**Agència Catalana
de Certificació**

Normativa de signatura electrònica:
Publicació (genèrica)

Referència:
Versió: 1.0
Data: 29/02/2008

Informació general

Control documental

Projecte:	N/A
Entitat de destinació:	Públic
Títol:	Normativa de signatura electrònica: Publicació (genèrica)
Codi de referència:	
Versió:	1.0
Data:	29/02/2008
Fitxer:	NSE Publicació v1r1.doc
Eina/es d'edició:	Word 2002
Autor/s:	Nacho Alamillo
Resum:	

Estat formal

Preparat per:
Nom: Nacho Alamillo Data: 29/02/2008

Control de versions

Versió	Parts que canvien	Descripció del canvi	Data
1.0	Tot	Creació del document	29/02/2008

Índex

1. Introducció	5
1.1 Objecte i abast	5
1.2 Contingut	5
2. Normativa de signatura electrònica de publicacions	6
2.1 Especificacions de la normativa de signatura	6
2.2 Protecció de la normativa de signatura	6
2.3 Referències	6
2.4 Continguts generals de la normativa de signatura	7
2.4.1 Descripció de la normativa de signatura electrònica.....	7
2.4.2 Continguts generals de la normativa	7
2.5 Normativa de validació de signatura electrònica	7
2.5.1 Normes sobre el període autoritzat de signatura	8
2.5.2 Normes comunes a tots els compromisos	8
2.5.2.1 Normes de signatari i verificador.....	8
2.5.2.1.1 Normes del signatari.....	8
2.5.2.1.2 Normes de verificador	8
2.5.2.2 Normes de confiança de certificats del signatari	9
2.5.2.2.1 Normes de processament de la cadena de certificació	9
2.5.2.2.2 Normes de comprovació d'informacions de revocació de certificats.....	9
2.5.2.3 Normes de confiança de segells de data y hora	9
2.5.2.3.1 Normes de processament de la cadena de certificació	9
2.5.2.3.2 Normes de comprovació d'informacions de revocació de certificats.....	10
2.5.2.3.3 Termini màxim de verificació de la signatura	10
2.5.2.4 Normes d'ús d'algorismes	10
2.5.2.4.1 Algoritmes de signatura.....	10
2.5.2.4.2 Algoritmes de certificat del signatari.....	10
2.5.2.4.3 Algoritmes de certificat de les entitats de certificació.....	11
2.5.3 Normes específiques de compromisos	11
3. Mesures tècniques per garantir el moment de publicació d'un document	12
3.1 Consideracions prèvies	12
3.1.1 Perfil del contractant	12
3.1.2 Requeriments.....	12
3.2 Recomanacions per a la implantació	13

1. Introducció

1.1 Objecte i abast

Aquest document defineix, en primer lloc, la **normativa de signatura electrònica** - o conjunt de normes de seguretat, d'organització, de negoci, tècniques i legals - **aplicable a** la generació, verificació i gestió de les signatures electròniques de **documents que esdevenen publicacions**.

Aquesta política es pot emprar, per exemple, per signar diaris i butlletins oficials i altra informació que s'hagi de publicar en el taulell d'anuncis electrònic d'una Administració.

En segon lloc, es formulen recomanacions referents a les **mesures tècniques necessàries per garantir el moment de publicació d'un document**. En el ben entès que aquest document pot haver estat signat, prèviament a la seva publicació, conforme a la normativa de signatura electrònica abans esmentada, de publicacions, o conforme a altra que resulti aplicable; per exemple, si es tracta d'un document administratiu, hauria d'haver estat signat conforme a la política de l'acte administratiu corresponent, si és un document còpia d'altre hauria d'haver estat signat conforme a una política de còpia autèntica, etc.

L'objectiu de l'aplicació d'aquestes mesures és generar evidències de que cert document ha estat publicat en un cert moment en un àmbit concret – sigui aquest una seu electrònica, un perfil d'Administració contractant, un taulell d'anuncis electrònic d'un ens, etc.

1.2 Contingut

Aquest document conté:

1. Introducció (aquesta secció).
2. Normativa de signatura electrònica de publicacions
 - 2.1 Continguts generals de la normativa de signatura electrònica.
 - 2.2 Normativa de validació de signatura electrònica – la qual inclou normes específiques referents als compromisos del signatari.
3. Mesures tècniques per garantir el moment de publicació d'un document.

2. Normativa de signatura electrònica de publicacions

2.1 Especificacions de la normativa de signatura

La normativa de signatura electrònica es podrà especificar de les següents formes:

- Especificació en llenguatge natural, per a la seva lectura per persones físiques (aquest document).
- Especificació en llenguatge XML, d'acord amb el que estableix l'especificació tècnica ETSI TR 102 038 v1.1.1, per al seu processament automàtic.

2.2 Protecció de la normativa de signatura

La normativa de signatura electrònica ha de ser protegida mitjançant la creació del resum criptogràfic de la mateixa, per a la qual cosa seran acceptables els següents algoritmes:

- SHA-1.

Aquest resum criptogràfic ha de ser inclòs a la pròpia normativa de signatura (per exemple, en forma de PDF signat o com a part de l'especificació XML de la normativa).

2.3 Referències

- ETSI TR 102 038 v1.1.1 (2002-04). Electronic Signatures and Infrastructures (ESI); XML format for signature policies.
- ETSI TR 102 041 v1.1.1 (2002-02). Electronic Signatures and Infrastructures (ESI); Signature policies report.
- ETSI TR 102 045 V1.1.1 (2003-03). Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model.
- ETSI TR 102 272 v1.1.1 (2003-12). Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies.
- ETSI TS 101 733 v1.6.3 (2005-09). Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAAdES).
- ETSI TS 101 903 v1.3.2 (2006-03), Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES).

-
- IETF RFC 3280, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile, April 2002.
 - Guia de normatives de signatura electrònica. Agència Catalana de Certificació. 2007.

2.4 Continguts generals de la normativa de signatura

2.4.1 Descripció de la normativa de signatura electrònica

Aquesta normativa regula la signatura electrònica de documents que corresponen a publicacions d'informacions, de tot tipus

2.4.2 Continguts generals de la normativa

La normativa de signatura contindrà la següent informació:

- El identificador de la normativa de signatura és:
urn:catcert:normatives:signatura:publicacio_generica.
- La data d'emissió de la normativa de signatura és 26/02/2008.
- L'emissor de la normativa de signatura és l'Agència Catalana de Certificació.
- L'àmbit d'aplicació de la normativa de signatura és l'autenticació de publicacions d'informacions.
- La normativa de validació de signatura electrònica, que inclourà les normes que s'exposen a la secció 0.

2.5 Normativa de validació de signatura electrònica

La validació de la signatura electrònica requerirà el compliment de les següents normes, per part del productor del document (signatari) i del receptor del document (verificador):

- Normes sobre el període autoritzat de signatura.
- Normes comunes a tots els compromisos.
- Normes específiques de compromisos.
- Normes addicionals.

2.5.1 Normes sobre el període autoritzat de signatura

Aquesta normativa serà vàlida des del dia 26/02/2008, des de les 00:00 hores, i serà vàlida indefinidament, mentre no sigui substituïda o derogada per una altra política posterior.

2.5.2 Normes comunes a tots els compromisos

Les normes comunes a tots els compromisos són aplicables a qualsevol dels compromisos d'una signatura electrònica. S'agrupen en els següents apartats:

- Normes de signatari i verificador.
- Normes de confiança de certificats del signatari.
- Normes de confiança de segells de data y hora.
- Normes d'ús d'algorismes.

2.5.2.1 Normes de signatari i verificador

2.5.2.1.1 Normes del signatari

El signatari ha de complir les següents normes:

- La signatura i el document podran ser objectes independents.
- El signatari ha d'incorporar els següents atributs i signar-los:
 - o La data i l'hora en que declara la creació de la signatura.
 - o El certificat emprat per a la creació de la signatura.
 - o El identificador d'aquesta normativa de signatura electrònica.
 - o Un segell criptogràfic de data i hora sobre la signatura electrònica.
- El signatari pot incloure, opcionalment, els següents atributs i signar-los:
 - o La indicació del compromís que assumeix en la creació de la signatura electrònica.
 - o La localitat a la quan es produeix la signatura electrònica.
 - o El rol en que actua el signatari quan crea la signatura electrònica.

2.5.2.1.2 Normes de verificador

El verificador ha de complir les següents normes, en la seva verificació de la signatura electrònica:

-
- El verificador pot incorporar els següents atributs, que no seran signats:
 - o El joc complet de referències a la cadena de certificats emprada.
 - o El joc complet de referències a les informacions de revocació dels certificats emprats.

2.5.2.2 Normes de confiança de certificats del signatari

2.5.2.2.1 Normes de processament de la cadena de certificació

La signatura electrònica s'ha de poder verificar mitjançant la construcció d'una ruta fiable de certificació, amb les següents característiques:

- Els certificats que es consideren punts de confiança per a aquesta signatura electrònica seran els següents:
 - o "CN = EC-ACC, OU = Jerarquia Entitats de Certificacio Catalanes, OU = Vegeu <https://www.catcert.net/verarrel> (c)03, OU = Serveis Publics de Certificacio, O = Agencia Catalana de Certificacio (NIF Q-0801176-I), C = ES".
- Les normatives de certificació que es consideren vàlides per a aquesta signatura electrònica son les següents:
 - o Certificats CPISR-1, amb OID 1.3.6.1.4.1.15096.1.3.1.81.1.
 - o Certificats CPISR-1 amb Càrrec, amb OID 1.3.6.1.4.1.15096.1.3.1.81.2.
 - o Certificats CPISR-1 amb Càrrec per a Ús concret, amb OID 1.3.6.1.4.1.15096.1.3.1.81.3, sempre que l'ús concret ho permeti.
 - o Certificats CEISR-1, amb OID 1.3.6.1.4.1.15096.1.3.1.121
 - o Certificats CESR-1, amb OID 1.3.6.1.4.1.15096.1.3.1.151

2.5.2.2.2 Normes de comprovació d'informacions de revocació de certificats

La signatura electrònica s'ha de verificar d'acord amb les següents normes:

- Els certificats del signatari s'han de verificar emprant OCSP o llistes de revocació de certificats (CRL).
- Els certificats de les entitats de certificació s'han de verificar emprant OCSP o llistes de revocació de certificats (CRL).

2.5.2.3 Normes de confiança de segells de data y hora

2.5.2.3.1 Normes de processament de la cadena de certificació

La signatura electrònica del segell de data i hora s'ha de poder verificar mitjançant la construcció d'una ruta fiable de certificació, amb les següents característiques:

- Els certificats que es consideren punts de confiança per a aquesta signatura electrònica seran els següents:
 - o "CN = EC-ACC, OU = Jerarquia Entitats de Certificacio Catalanes, OU = Vegeu <https://www.catcert.net/verarrel> (c)03, OU = Serveis Publics de Certificacio, O = Agencia Catalana de Certificacio (NIF Q-0801176-I), C = ES"
- Les normatives de certificació que es consideren vàlides per a aquesta signatura electrònica son les següents:
 - o Certificats CIT, amb OID 1.3.6.1.4.1.15096.1.3.1.111.

2.5.2.3.2 Normes de comprovació d'informacions de revocació de certificats

La signatura electrònica del segell de data i hora s'ha de verificar d'acord amb les següents normes:

- Els certificats de l'entitat de segellament de data i hora s'han de verificar emprant OCSP o llistes de revocació de certificats (CRL).
- Els certificats de les entitats de certificació en que es basa el certificat de l'entitat de segellament de data i hora s'han de verificar emprant OCSP o llistes de revocació de certificats (CRL).

2.5.2.3.3 Termini màxim de verificació de la signatura

La signatura electrònica no es podrà verificar un cop hagi expirat el segell de data i hora.

2.5.2.4 Normes d'ús d'algorismes

2.5.2.4.1 Algoritmes de signatura

Es podran emprar els següents algoritmes:

- Resum: SHA-1.
- Signatura: RSA-SHA-1, amb longitud mínima de 1024 bits.

2.5.2.4.2 Algoritmes de certificat del signatari

Es podran emprar els següents algoritmes:

-
- Resum: SHA-1.
 - Signatura: RSA-SHA-1, amb longitud mínima de 1024 bits.

2.5.2.4.3 Algoritmes de certificat de les entitats de certificació

Es podran emprar els següents algoritmes:

- Resum: SHA-1.
- Signatura: RSA-SHA-1, amb longitud mínima de 1024 bits.

2.5.3 Normes específiques de compromisos

La definició dels compromisos inclosos pel signatari a la signatura serà la següent:

- Publicació genèrica.
 - o Aquest compromís s'identifica amb el següent identificador: urn:catcert:compromisos:signatura:publicacio.
 - o L'àmbit d'aplicació del compromís és el procediment administratiu electrònic.
 - o El significat del compromís és l'autenticació de publicacions d'informacions.

3. Mesures tècniques per garantir el moment de publicació d'un document.

3.1 Consideracions prèvies

3.1.1 Perfil del contractant

Sembla una qüestió d'interès determinar quina relació hi ha entre la "seu electrònica" – tal com es preveu a l'article 10 de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics – i les "pàgines web institucionals que mantinguin els ens del sector públic" – segons l'apartat 1 de l'article 42 de la Llei 30/2007, de contractes del sector públic. És el "perfil del contractant accessible a través de la web institucional" quelcom diferent a una secció particular de la "seu electrònica"? En general, sembla que no – exceptuant els contractants que estiguin exclosos de l'aplicació de la Llei 11/2007, com ara les societats mercantils vinculades al sector públic.

De manera que es pot considerar que **la pàgina web institucional d'una Administració Pública contractant a la que fa referència l'article 42 de la Llei 30/2007 és la seva seu electrònica, conforme als requeriments de l'article 10 de la Llei 11/2007.**

3.1.2 Requeriments

L'article 42 de la Llei 30/2007, de contractes del sector públic, en el seu apartat 3, estableix la necessitat de disposar de "un dispositivo que permita acreditar fehacientemente el momento de inicio de la difusión pública de la información que se incluya en el mismo".

Resulta curiós que la Llei faci referència explícita a la necessitat que el sistema informàtic que suporti el perfil del contractant hagi de disposar d'un dispositiu que acrediti de manera fefaent el moment d'inici de la difusió pública de la informació; quan es podria haver establert, simplement, la necessitat de datar electrònicament els documents que es publiquin, afegint-los un segell de data i hora protegit criptogràficament. I quan en altres apartats de la mateixa Llei s'exigeix aquesta garantia de data i hora (article 132.6 o disposició addicional 19^a e).

Sembla clar que el legislador ha volgut, senzillament, indicar que s'ha d'acreditar l'instant d'inici de la difusió, més que afegir la data i hora al document. Potser perquè el concepte de segellat de data i hora s'associa de seguida amb la garantia del document electrònic (normalment el signat electrònicament, ja que aquest segellat del data i hora és una condició típica – segons es desprèn de l'article 4 de la Llei 59/2003 de signatura electrònica). I perquè el fet que el contractant afegeixi la data i hora criptogràfica a un document (signat o no) no acreditaria que el document hagi

estat difós per l'òrgan mitjançant el perfil; només indicaria que el document existia abans de la data de segellat, res més.

Per tant, el que és realment important és poder **acreditar que realment el sistema informàtic que suporta el perfil difon (publica a través d'Internet) els documents que rep.**

La problemàtica de prova és similar a la que es presenta en el cas de les comunicacions i les notificacions telemàtiques (article 27 de la Llei 11/2007), en la publicació de diaris oficials (article 11 de la Llei 11/2007), en la publicació en el taulell d'anuncis accessible mitjançant la seu electrònica (article 12 de la Llei 11/2007) o, en general, en la publicació de qualsevol informació administrativa a la seu electrònica.

Conseqüentment, i d'acord amb el que s'exposa a l'apartat anterior, la problemàtica d'acreditar el moment en que s'inicia la difusió pública d'una informació de contractació en el perfil és la mateixa que la d'acreditar el moment en que es publica qualsevol altra informació de l'Administració a la seu electrònica, i s'ha de resoldre de la mateixa forma.

Per tant, tot acaba sent una qüestió de disseny de la seu electrònica de l'Administració, que haurà de garantir en quin moment es publiquen els document – a més de quina és la seva data.

3.2 Recomanacions per a la implantació

Les recomanacions de CATCert per complir amb els requeriments identificats anteriorment són:

1. **Els documents a publicar/difondre públicament han d'estar signats electrònicament per l'Administració**, a l'efecte de garantir la seva autenticitat – tal com disposa l'article 29.1 de la Llei 11/2007. Aquesta signatura electrònica podrà ser realitzada mitjançant un segell d'actuació administrativa automatitzada (article 18 de la Llei 11/2007) o per una persona al servei de l'Administració, sempre en l'exercici de les seves competències (article 19 de la Llei 11/2007).
2. **Els document podran o no incorporar un segell de data i hora**, com autoritza l'article 29.2 de la Llei 11/2007. CATCert recomana incorporar sempre un segell de data i hora al document, per garantir el moment de la seva creació i que la signatura era vàlida en aquell moment. En aquest sentit, alguna legislació europea – com ara l'alemanya – exigeix sempre segellat de data i hora.
3. **La seu electrònica ha d'incorporar un "registre de publicacions" (log) que garanteixi les publicacions que es realitzin.** Per exemple, si la seu electrònica empra un gestor de continguts, aquest es pot programar per tal que afegeixi al seu log cada document que es publica.

-
4. **Cada entrada del log ha d'incorporar un segell de data i hora de dita entrada.** Amb això es garanteix que, realment, aquesta entrada de *log* referint la publicació d'un document concret existia en aquell moment.
 5. A més, es recomana que **cada entrada del log incorpori un resum criptogràfic de l'entrada anterior**; de manera que es pugui garantir l'ordre de publicació, perquè no és possible eliminar entrades intermèdies ni tampoc es poden inserir entrades falses. Es tracta d'una tècnica matemàtica basada en encadenament de resums criptogràfics que realment fa impossible alterar fraudulentament el registre de publicacions i que aporta una elevada credibilitat al sistema.
 6. **Es logs s'hauran de protegir convenientment per tal d'evitar la seva pèrdua.** En escenari d'alt risc, es pot considerar el seu emmagatzemament en un tercer de confiança - de manera que, per exemple, al final del dia s'enviïn les proves a un tercer – que garanteixi als ciutadans la conservació independent d'aquests logs.