BOPB Butlletí Oficial de la Província de Barcelona Diputació Barcelona

Dijous, 3 d'abril de 2014

ADMINISTRACIÓ LOCAL

Diputació de Barcelona. Àrea d'Hisenda i Recursos Interns i Noves Tecnologies

ANUNCI d'aprovació de la política de signatura electrònica de la Diputació de Barcelona

Als efectes de coneixement general es fa públic que per Decret de data 24 de març de 2014 de la Presidència de la Diputació de Barcelona, s'aprova la política de signatura electrònica de la Diputació de Barcelona, en els següents termes:

"Primer.- APROVAR la Política de Signatura Electrònica de la Diputació de Barcelona aplicable a les relacions entre la Diputació de Barcelona i els seus ens dependents, i els ciutadans i la resta d'administracions públiques.

"POLÍTICA DE SIGNATURA ELECTRÒNICA DE LA DIPUTACIÓ DE BARCELONA

TÍTOL I. ABAST DE LA POLÍTICA DE SIGNATURA ELECTRÒNICA

L'objectiu d'aquesta política és el de detallar les condicions generals que s'hauran de respectar en els processos de generació, validació i conservació de la signatura electrònica, així com determinar els formats dels objectes binaris i dels fitxers que hauran de ser admesos per les plataformes implicades en les relacions electròniques de la Diputació de Barcelona amb la ciutadania, les empreses i els seus organismes autònoms, ens públics de dret privat i la resta d'entitats incloses en l'àmbit d'aplicació del Decret d'aprovació d'aquesta Política de Signatura Electrònica.

Per a la seva identificació unívoca, a la Política de Signatura Electrònica de la Diputació de Barcelona se li ha assignat un identificador únic del tipus OID, el qual s'haurà d'incloure obligatòriament a la signatura electrònica mitjançant l'ús del camp corresponent per identificar la política aplicable i la seva versió, amb les condicions generals i específiques d'aplicació per a la seva validació.

L'Identificador únic de la Política de Signatura Electrònica de la Diputació de Barcelona serà l'OID 1.3.6.1.4.1.40236.1.9 quedant assignat l'OID 1.3.6.1.4.1.40236.1 a la branca dedicada a les polítiques de signatura electrònica i altres polítiques relacionades amb aquestes.

Correspon a la Direcció de Serveis de Tecnologies i Sistemes Corporatius el manteniment, actualització i difusió del catàleg d'Identificadors d'objecte (OIDs) de la Diputació de Barcelona.

La present Política de Signatura Electrònica estarà disponible en format llegible per tal que pugui ser aplicada en un context concret per a complir amb els requeriments de creació i validació de signatura electrònica, tant en un entorn de processament individualitzat com automatitzat.

1. Actors involucrats

Els actors involucrats en el procés de creació i validació de signatura electrònica són:

- Signant: persona que disposa d'un dispositiu de creació de signatura i que actua en nom propi o en nom d'una persona física o jurídica a la que representa.

- Verificador: entitat, persona física o jurídica, que valida o verifica una signatura electrònica mitjançant el contrast amb les condicions exigides per una Política de Signatura concreta. Pot ser una entitat de validació de confiança o una tercera part que estigui interessada en conèixer la validesa d'una signatura electrònica.

- Prestador de serveis de signatura electrònica: La persona física o jurídica que expedeix certificats electrònics o presta altres serveis en relació amb la signatura electrònica.

- Emissor de la Política de Signatura Electrònica: entitat que s'encarrega de generar o gestionar el document de Política de Signatura, mitjançant el qual quedaran vinculats el signant i el verificador en els processos de generació i validació de la signatura electrònica.

2. Formats admesos

El format dels documents electrònics amb signatura electrònica avançada i reconeguda, aplicada mitjançant els certificats electrònics admesos, i utilitzats en l'àmbit de les relacions amb o dins de l'Administració, s'hauran d'ajustar a

CVE-Núm. de registre: 022014008181

les especificacions dels estàndards europeus relatius als formats de signatura electrònica, i a la legislació espanyola en el cas de signatura electrònica reconeguda.

La Direcció de Serveis de Tecnologies i Sistemes Corporatius (DSTSC) serà l'encarregada de publicar i actualitzar a la Seu electrònica corporativa la relació de les especificacions relatives als formats admesos per aquesta Política de Signatura.

La DSTSC, o l'entitat designada a l'efecte, conservarà un repositori amb l'historial de les versions de la Política de Signatura Electrònica i de certificats que s'aprovin. La consulta a aquest repositori permetrà verificar una signatura electrònica anterior a la política vigent en cada moment. En el moment de la signatura s'haurà d'incloure la referència de l'identificador de la versió de la Política de Signatura electrònica i de certificats on es determinaran les condicions que haurà de complir la signatura electrònica en cada moment.

En relació amb els actes administratius i amb els actes de tràmit, tots els documents originals que hagin de restar en poder de l'administració (Resolucions, actes, convenis, informes, entre d'altres) s'han de produir, sempre que sigui possible, amb signatura electrònica independent del document, evitant l'ús de signatures embolcallades a formats documentals.

Els documents originals a lliurar al ciutadà (certificacions, notificacions, entre d'altres) han d'incloure, sempre que sigui possible, la signatura embolcallada al propi format documental; alternativament es podrà incorporar un codi segur de verificació electrònica (CSV) que permeti la seva consulta en línia i la impressió en concepte de còpia autèntica, d'acord amb la corresponent NTI.

En relació amb els actes dels ciutadans o ens públics que es relacionin amb la Diputació de Barcelona, sempre que sigui possible, s'hauran d'utilitzar formularis confeccionats per a ser signats electrònicament, sempre respectant l'esmentada independència entre el formulari i la signatura del document.

Per tal de protegir la signatura electrònica de la possible obsolescència dels algorismes i poder continuar garantint les seves característiques al llarg de la seva vida útil, s'hauran d'aplicar mecanismes de ressegellat, afegint de forma periòdica un segell de data i hora d'arxiu amb un algorisme més resistent.

Per a l'arxiu i gestió de documents electrònics se seguiran les recomanacions de les guies tècniques de desenvolupament de l'Esquema Nacional d'Interoperabilitat així com les prescripcions de la Política de gestió de documents electrònics aprovada a l'efecte.

3. Creació de la signatura electrònica

Les plataformes que presten el servei de creació de signatura electrònica proporcionaran les funcionalitats necessàries per a suportar un procés de creació de signatures basat en els punts següents:

1.- Selecció dels documents a signar per l'usuari. Els formats de fitxer admesos a les plataformes seran els publicats a la seu electrònica corporativa.

La persona signant dels documents garantirà que el document a signar no incorpora contingut dinàmic que pugui afectar a la seva validesa i que pugui modificar el resultat de la signatura al llarg del temps.

2.- El servei de signatura electrònica executarà un conjunt de verificacions prèvies a la creació de la signatura:

• La signatura electrònica pot ser validada per al format de fitxer específic a signar, d'acord amb aquesta política.

• Que els certificats a utilitzar hagin estat expedits i vinculats a una declaració de polítiques de certificació admesa. A la seu electrònica corporativa es publicarà la relació dels sistemes de signatura i certificats electrònics admesos, els procediments per als quals són vàlids i les especificacions de la signatura electrònica que es puguin realitzar amb ells.

• La validesa del certificat, comprovant si ha estat revocat o no, suspès i si està en vigor, així com validar la cadena de certificació, incloent la validació de tots els certificats de la cadena.

• Quant una d'aquestes verificacions sigui errònia, el procés de signatura quedarà interromput.

CVE-Núm. de registre: 022014008181

En el cas que no fos possible fer aquestes validacions en el moment de la signatura, els sistemes corresponents podran no acceptar el fitxer signat, o bé esperar un període de temps, no superior a les 24h des de la presentació del document signat, fins que les validacions esmentades es puguin realitzar.

Els processos de validació i verificació seran suportats per la plataforma de validació de la Diputació de Barcelona, o pel verificador autoritzat; actualment el verificador autoritzat, és el servei Validador facilitat pel Consorci AOC.

4. Verificació de la signatura electrònica

El verificador pot utilitzar qualsevol mètode per verificar la signatura creada segons la present política. Les condicions mínimes que s'han de produir per validar la signatura són les següents:

1.- Garantia de què la signatura és valida pel document específic signat.

2.- Validesa dels certificats en el moment en que es produí la signatura en el cas que aquesta incorpori informació sobre revocació de certificats, o en cas contrari, validesa dels certificats en el moment de la seva validació: certificats no revocats, suspesos, o caducats, i la validació de la cadena certificació (inclosa la validació de tots els certificats de la cadena). Aquesta informació pot estar continguda en la pròpia signatura en el cas de les signatures longeves.

3.- Certificat expedit vinculat amb la declaració de pràctiques de certificació admesa en el moment en què es produí la signatura.

La llista dels certificats admesos podrà ser consultada a l'apartat corresponent de la seu electrònica corporativa.

4.- Verificació, si existeixen, dels segells de temps dels formats implementats, incloent la verificació dels períodes de validesa dels segells.

Sempre que sigui possible, la Diputació de Barcelona o l'entitat encarregada, procedirà a verificar els certificats mitjançant mecanismes en línia que responguin en temps real, com per exemple el servei Validador del Consorci AOC, o en el seu defecte utilitzant els servidors OCSP (Protocol en línia d'estat dels certificats).

Quan no resulti possible la consulta en línia, la Diputació de Barcelona o l'entitat encarregada, emprarà llistes de revocació de certificats emeses pel prestador de serveis de certificació corresponent.

5. Signatures electròniques perdurables en el temps

El procés de manteniment de la validesa de la signatura electrònica al llarg del temps (signatura longeva) per a un tipus de contingut concret en el moment de la seva recepció, consisteix en l'addició de garanties criptogràfiques (informacions addicionals, i/o segells de temps) que permetin acreditar la validesa d'una signatura en un moment concret del temps, fins i tot en cas de ruptura o obsolescència matemàtica dels algorismes de signatura electrònica utilitzats.

Això vol dir que, si es vol tenir una signatura que pugui ser validada al llarg del temps, la signatura electrònica que es generi haurà d'incloure evidències de la seva validesa per tal que no pugi ésser repudiada un cop es produeixi la seva obsolescència tecnològica.

Per aquesta tipologia de signatures existirà un servei, propi o gestionat per tercers, encarregat de mantenir aquestes evidencies, essent necessari sol·licitar i/o preveure l'actualització de les signatures abans de què les claus i el material criptogràfic associat sigui vulnerable.

TÍTOL II. DIRECTRIUS DE SIGNATURA ELECTRÒNICA

6. La signatura electrònica en relació amb la tipologia d'acte

La signatura electrònica és un mecanisme per a securitzar la informació transmesa a través dels canals telemàtics. L'objectiu de la política de signatura electrònica és indicar els usos que es contemplen per a un àmbit i abast concrets, especificant les condicions requerides i necessàries per a cada un dels usos que correspongui, d'acord amb les normes següents:

- La Diputació de Barcelona ha d'establir estàndards per a la signatura dels diferents tipus d'actes jurídics documentats.

CVE-Núm. de registre: 022014008181

- Els actes administratius realitzats pels òrgans administratius s'han de documentar en un document ofimàtic o llibre-registre electrònic de forma autenticada amb signatura electrònica reconeguda (en el cas de l'actuació manual), o amb un segell d'Administració, òrgan o entitat de dret públic de nivell mig o alt (en el cas de l'actuació automatitzada), per tractar-se en general d'actius la categoria de seguretat dels quals en les dimensions d'integritat i autenticitat és de nivell mig[1].

- Els actes administratius que es considerin de nivell alt s'han d'autenticar necessàriament utilitzant sistemes de signatura electrònica reconeguda (en cas d'actuació manual) o amb un segell d'Administració, òrgan o entitat de dret públic de nivell alt (en cas d'actuació automatitzada), en ambdós casos amb utilització preferentment de dispositius certificats[2].

- Els actes de tràmit i, en general, els actes sense transcendència externa, es poden documentar amb signatura electrònica avançada i, en concret, generar entrades en registres electrònics d'activitat sempre que la persona s'hagi autenticat amb certificat electrònic reconegut.

- Els actes d'intercanvi de dades entre administracions públiques o l'accés a dades d'altres administracions públiques, exigirà el nivell mínim exigit per cada administració que cedeix dades o dóna accés a dades.

- Els actes dels ciutadans s'han de basar, en general, en la signatura electrònica avançada i/o reconeguda admesa d'acord amb el punt 8 Ús de certificats d'identitat i signatura electrònica.

- En tots els casos s'han d'emprar algorismes aprovats admesos d'acord amb el que disposa aquesta resolució, i la normativa que aprova.

7. Tipologia de certificats a emprar

Els actes administratius adoptats pels òrgans competents s'han de documentar de forma autenticada amb signatura electrònica reconeguda quan el procés de signatura és individualitzat, o mitjançant un segell d'administració, òrgan o entitat de dret públic de nivell mig o alt quan la signatura és realitzada mitjançant un procés automatitzat. De la mateixa manera s'haurà d'actuar quan els documents a signar tinguin eficàcia davant tercers interessats en el procediment, o bé es tracti de la producció de documents d'emissió obligatòria d'acord amb la normativa vigent.

Els actes de tràmit i, en general, els actes sense transcendència externa (que no afectin a drets i interessos de tercers), es poden materialitzar mitjançant signatura electrònica avançada i, en concret, generar entrades en registres electrònics d'activitat sempre que la persona s'hagi autenticat amb certificat electrònic reconegut.

Els actes d'intercanvi de dades entre administracions públiques, o l'accés a dades on-line requerirà el nivell mínim exigit per l'administració cedent.

Els actes dels ciutadans es podran basar, en general, en la signatura electrònica avançada basada en els certificats reconeguts admesos i publicats a la seu electrònica de la Corporació.

Els certificats a emprar han de ser els següents:

- Actuació administrativa (afecta a drets i interessos de tercers):

• Actuació manual: Certificat personal d'identificació i signatura reconeguda amb la indicació del càrrec (per exemple un CPISR-1 Càrrec emès per CATCert - Consorci AOC) o equivalent.

• Actuació automatitzada: Certificat de segell electrònic, al menys de nivell mig en sistemes d'informació de nivell baix, i nivell alt en sistemes d'informació de nivell alt (per exemple un CDA-1 Segell nivell mig o alt emès per CATCert - Consorci AOC) o equivalent.

- Actuació de tràmit (no afecta a drets i interessos de tercers):

• Actuació manual: Certificat personal d'identificació i signatura reconeguda (per exemple un CPISR-1 emès per CATCert - Consorci AOC) o equivalent.

1 Secció 5.7.4 RDENS.
2 Secció 5.7.4 RDENS.

CVE-Núm. de registre: 022014008181

• Actuació automatitzada: Certificat de segell electrònic, al menys de nivell mig en sistemes d'informació de nivell baix i mig, i nivell alt en sistemes d'informació de nivell alt (per exemple un CDA-1 emès per CATCert - Consorci AOC) o equivalent.

- Actuació d'intercanvi de dades o accés a dades entre administracions:

• Els certificats admesos per cada administració que cedeix o dóna accés a dades a la Diputació de Barcelona.

- Actuació dels ciutadans:

• El certificat de signatura electrònica incorporat en el DNI electrònic.

• Tots els certificats, de nivell 3 o superior, admesos d'acord amb el punt 8 "Ús de certificats d'identitat i signatura electrònica" d'aquesta política.

8. Ús de certificats d'identitat i signatura electrònica

En termes generals, la Diputació de Barcelona ha d'admetre els certificats dels ciutadans, sempre que compleixin amb les condicions establertes a l'art. 21.1 de la LAECSP, i les condicions addicionals establertes per aquesta Política de Signatura Electrònica.

Poden ser prestadors de serveis de certificació totes les entitats que operin a l'Estat Espanyol, en els termes de la legislació vigent de signatura electrònica, i hagin comunicat l'inici de la seva activitat al Ministeri d'Indústria, Energia i Turisme, apareixent inscrits en el llistat electrònic de prestadors de serveis de certificació.

En relació amb els certificats corporatius, el prestador del servei de certificació preferent és l'Agència Catalana de Certificació-CATCert del Consorci AOC. Quan aquesta no subministri un certificat dels previstos per aquesta política, o ho faci en condicions que entrin en contradicció amb el mateix, la Diputació de Barcelona els podrà obtenir a través d'altres prestadors de serveis de certificació.

Els tipus de certificats a utilitzar en la tramitació electrònica a la Diputació de Barcelona, són:

- Certificats de ciutadans:

• Certificat-tipus de persona física.
• Certificat-tipus de persona jurídica.
• Certificat-tipus d'entitat sense personalitat jurídica.
• Certificat-tipus de representant.

- Certificats corporatius de la Diputació de Barcelona:

• Certificat-tipus de seu electrònica.
• Certificat-tipus de segell electrònic d'Administració, òrgan o entitat de dret públic.
• Certificat-tipus de personal al servei de l'Administració.

- Certificats tècnics:

• Certificat-tipus d'entitat de segellament de data i hora.
• Certificat-tipus de servidor segur.
• Certificat-tipus d'aplicació segura.
• Certificat-tipus de signatura de programari.

La Diputació de Barcelona utilitza o admet certificats X.509v3 per a la signatura electrònica avançada o reconeguda.

En termes generals, la Diputació de Barcelona ha d'admetre els certificats de ciutadans i de la resta d'Administracions Públiques, sempre que es donin les següents condicions:

- Que els prestadors hagin comunicat l'inici de la seva activitat al Ministeri d'Indústria, Turisme i Comerç.

CVE-Núm. de registre: 022014008181

Quan es tracti de certificats de signatura electrònica, que aquests hagin estat publicats en una llista de les llistes estatals incloses en la "EU Trusted Lists of Certification Service Providers"[3].

- Que els certificats compleixin les condicions addicionals establertes per aquesta política i la seva normativa de desenvolupament.

9. Relació entre la signatura i el document signat

- El format de la signatura, sempre que sigui possible, ha de ser independent del format del document o registre signat, amb l'objectiu de reduir al màxim la dependència entre tots dos objectes de negoci.

- La relació entre el document signat i la signatura s'ha d'establir mitjançant l'ús de metadades del document.

Els documents originals a lliurar al ciutadà, a títol no exhaustiu, certificacions i notificacions, han d'incloure, sempre que sigui possible, la signatura embolcallada al propi format documental, o bé incorporar un codi segur de verificació electrònica, que permeti la seva consulta en línia i la impressió en concepte de còpia autèntica, d'acord amb la corresponent NTI.

- En relació amb els actes d'intercanvi de dades o accés a dades entre administracions, la relació entre la signatura electrònica i el document signat serà típicament establerta per cada administració que cedeix dades o dóna accés a dades, sense perjudici d'establir aquestes condicions per conveni.

- En relació amb els actes dels ciutadans, amb caràcter general es faran servir formularis amb signatura electrònica, tret que, d'acord amb la naturalesa de l'acte, expressament se'n determini qualsevol altre mecanisme de relació.

- Respecte dels documents ofimàtics, signats o no, que puguin presentar els ciutadans acompanyant a la sol·licitud administrativa, no se'ls aplicaran aquestes directrius de signatura electrònica sempre que es tracti de documents previs no creats específicament pel ciutadà per a ésser presentats davant l'administració.

- S'accepten i es validen les signatures dels documents ofimàtics que es determinin a l'Esquema Nacional d'Interoperabilitat i a l'Esquema Nacional de Seguretat.

- S'accepten les còpies digitalitzades dels documents en suport paper, produïdes pels ciutadans. Aquests fitxers es protegeixen amb la signatura electrònica de la sol·licitud, mitjançant la inclusió dels resums criptogràfics dels documents en el formulari a signar.

10. Format de la signatura electrònica

El format de la signatura electrònica a utilitzar es determinarà en funció del format del document a signar (com a exemple el format PDF exigeix signar els documents en format de signatura CMS, mentre que els documents en format ODF utilitzaran una variant de signatura en XML DSig).

La Diputació de Barcelona ha de fer servir formats avançats de signatura (CAdES, XAdES i PAdES) sempre que sigui possible, amb les següents restriccions addicionals:

- No s'ha de fer servir certificació d'atributs.

- Respecte als atributs de signatura electrònica avançada (AdES), cada estàndard tècnic de signatura electrònica ha d'identificar els que cal incloure a la signatura.

La Diputació de Barcelona preveurà la migració dels formats de signatura (CMS, XML DSig...) actualment utilitzats, als formats avançats (CAdES, XAdES i PAdES) en el menor temps possible.

Les recomanacions concretes en relació amb la signatura electrònica de cada format documental, s'han d'establir en els corresponents estàndards tècnics de signatura electrònica de format documental.

11. Perfil de la signatura electrònica

- Les signatures dels actes administratius realitzats pels òrgans administratius han de poder ser validades pels ciutadans sense mitjans especialment complexos.

- En general, s'ha de fer servir el perfil AdES-XL amb segell de data i hora per a tota signatura lliurada a un ciutadà.

3 Al web: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/index_en.htm

CVE-Núm. de registre: 022014008181

- En relació a les signatures dels actes de tràmit s'ha de fer servir el perfil AdES-EPES excepte quan no resulti possible per incompatibilitat tècnica.

- La Diputació de Barcelona ha de segellar la signatura electrònica, d'acord amb el perfil AdES-T.

- Les signatures dels actes d'intercanvi de dades entre administracions públiques o l'accés a dades d'altres administracions públiques, s'han d'ajustar al perfil que determini cada administració que cedeix o dóna accés a dades.

- En relació a les signatures dels actes dels ciutadans, la Diputació de Barcelona ha d'admetre documents externs amb signatura conforme al perfil AdES-BES i AdES-EPES amb política implícita, i ha de verificar les signatures d'acord amb el perfil AdES-EPES amb política explícita, sempre que aquesta sigui conforme amb el que estableixen els articles 18 i següents del RDENI.

- La Diputació de Barcelona ha de completar la signatura d'acord amb el perfil AdES-XL amb segell de data i hora.

- Cada estàndard tècnic de seguretat documental ha de concretar el perfil aplicable a una signatura electrònica determinada.

12. Processos de signatura electrònica

La Diputació de Barcelona implantarà els següents processos en relació amb la signatura electrònica:

- Procés de creació de la signatura electrònica:

• Consisteix en la successió de passes necessàries per obtenir una signatura digital per a un tipus de contingut concret. Inclou la possibilitat de seleccionar i visualitzar continguts i atributs de signatura, efectuar fluxos de signatura i veure l'estat d'una signatura realitzada.

- Procés de validació inicial de la signatura electrònica:

• Consisteix en la successió de passes necessàries per verificar una signatura digital per a un tipus de contingut concret, en el moment de la seva recepció. Es tracta d'una verificació parcial, ja que, normalment, a la recepció d'una signatura electrònica no es pot determinar l'estat actual de revocació d'un certificat degut a que la informació de revocació es publica amb unes 24h d'endarreriment. Aquesta verificació no incorpora un segell de data i hora a la signatura, ni la completa.

• Aquest procés s'ha de basar, quan es produeixi, en l'ús de la plataforma de validació de la Diputació de Barcelona, que podrà delegar part del procés de verificació al servei Validador del Consorci AOC, o equivalent.

- Procés de validació definitiva de la signatura electrònica:

• Consisteix en la successió de passes necessàries per verificar una signatura digital per a un tipus de contingut concret, de forma definitiva. Es tracta d'una verificació definitiva, en un moment en que ja es pot determinar l'estat definitiu de revocació d'un certificat, normalment en les 24h següents a la recepció de la signatura. Aquesta verificació podrà incorporar un segell de data i hora a la signatura electrònica, o la completarà amb les dades necessàries per gaudir d'evidència electrònica.

• Aquest procés s'ha de basar, quan es produeixi, en l'ús de la plataforma de validació de la Diputació de Barcelona, que podrà delegar part del procés de verificació al servei Validador del Consorci AOC, o equivalent.

- Procés de manteniment de la validesa de la signatura electrònica:

• Consisteix en la successió de passes necessàries per mantenir al llarg del temps la validesa d'una signatura digital per a un tipus de contingut concret, en el moment de la seva recepció. Es tracta d'un procés d'addició de garanties criptogràfiques, com informacions de contrast i segells de data i hora, mitjançant les quals es pot acreditar la producció d'una signatura en un moment concret del temps, fins i tot en cas de ruptura o obsolescència matemàtica dels algorismes de signatura.

• Aquest procés s'ha de basar, quan es produeixi, en l'ús de la plataforma de validació de la Diputació de Barcelona, que podrà delegar part del procés de verificació al servei Validador del Consorci AOC, o equivalent.

CVE-Núm. de registre: 022014008181

13. Algorismes d'identificació i signatura electrònica aprovats

La Diputació de Barcelona emprarà la criptografia per oferir els següents serveis de seguretat:

- Serveis de confidencialitat.
- Serveis d'integritat de dades.
- Serveis d'autenticació.
- Serveis d'autorització.
- Serveis d'irrefutabilitat.
- Serveis accessoris.

Els serveis de seguretat fan ús dels algorismes criptogràfics estàndard següents:

- Algorismes de resum

• SHA-1[4], definit a la norma internacional ISO/IEC 10118-3 (2004): "Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions" i a la norma FIPS 180-2 (2002): "Secure Hash Standard".

SHA-1 és l'algorisme més utilitzat actualment, tot i que ja no es recomana el seu ús des del 2011[5], per la qual cosa cal anar abandonant-lo per passar a SHA-256, sempre que la infraestructura tecnològica ho permeti.

• SHA-256[6], definit a la norma internacional ISO/IEC 10118-3 (2004): Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions" i a la norma FIPS 180-2 (2002): "Secure Hash Standard".

• SHA-384[7], definit a la norma FIPS 180-2 (2002): "Secure Hash Standard".

• SHA-512[8], definit a la norma FIPS 180-2 (2002): "Secure Hash Standard".

- Algorismes simètrics

• AES[9], definit a la norma FIPS 197 (2001): "Specification for the Advanced Encryption Standard (AES)".

• TDEA[10] (per exemple, Triple DES), definit a l'especificació NIST SP 800-67 (2004, revisat el 2008): "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", amb la recomanació d'emprar tres claus diferents.

Es recomana emprar els modes criptogràfics d'operació definits a l'especificació NIST SP 800-38A (2001): "Recommendation for Block Cipher Modes of Operation - Methods and Techniques".

- Algorismes asimètrics

• RSA[11], definit a l'especificació tècnica IETF RFC 3447 (2003): "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1".

RSA és l'algorisme asimètric més recomanat actualment.

• DSA[12], definit a la norma internacional ISO/IEC 14888-3 (2006): "Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms" i a la norma FIPS 186-2 (2000): "Digital Signature Standard".

4 Secció 1.2.1.k) CCN STIC 807.
5 http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf.
6 Secció 1.2.1.k) CCN STIC 807.
7 Secció 1.2.1.k) CCN STIC 807.
8 Secció 1.2.1.k) CCN STIC 807.
9 Secció 1.2.1.b) CCN STIC 807.
10 Secció 1.2.1.a) CCN STIC 807.
11 Secció 1.2.1.i) CCN STIC 807.
12 Secció 1.2.1.g) CCN STIC 807.

CVE-Núm. de registre: 022014008181

• EC-DSA[13], en les seves dues variants E(Fp) i E(F2m), definit a la norma internacional ISO/IEC 14888-3 (2006): "Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms".

• EC-GDSA, en les seves dues variants E(Fp) i E(F2m), definit a la norma internacional ISO/IEC 15946-2 (2002): "Information technology - Security techniques – Cryptographic techniques based on elliptic curves - Part 2: Digital signatures".

- Algorismes d'establiment de claus

• Algorismes DLC, definits a l'especificació NIST SP 800-56A (2007): "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography".

• Algorisme de transport de claus RSA.

• Algorismes d'embolcallament de claus amb clau simètrica.

14. Gestió de les claus criptogràfiques

I.- La Diputació de Barcelona ha d'establir els procediments adients en relació amb els següents aspectes:

- Generació de claus per diferents sistemes criptogràfics i aplicacions, sempre realitzant-se en mitjans aïllats dels sistemes d'explotació[14].

- Generació i obtenció de certificats de clau pública.

- Distribució de claus als usuaris, incloent-hi l'activació una vegada hagin estat rebudes.

- Emmagatzematge de claus, incloent-hi com obtenen accés a les claus els usuaris autoritzats. Aquestes haurien de ser emmagatzemades de forma separada d'altres dades operatives, i arxivades en mitjans aïllats dels d'explotació[15].

- Canvi o actualització de claus, incloent-hi normes sobre quan les claus han de ser canviades o actualitzades, i quin és el procediment aplicable.

- Gestió de claus compromeses.

- Revocació de claus, incloent-hi la seva retirada o desactivació.

- Arxivament de claus, especialment en cas d'informació xifrada que hagi estat arxivada.

- Destrucció de claus.

- Registre i auditoria d'operacions relatives a gestió de claus.

II.- Així mateix, la Diputació de Barcelona ha de:

- Definir períodes d'activació i desactivació de les claus, per reduir el risc de compromís, de forma que les claus només es puguin emprar durant un termini concret, d'acord amb les circumstàncies i l'anàlisi de risc.

- Definir procediments per garantir l'autenticitat de les claus públiques, mitjançant l'ús de les entitats de certificació que resultin adequades.

- Aplicar els controls de seguretat criptogràfics establerts al RDENS, i en les Guies de desenvolupament que dicta el Centre Criptològic Nacional, adscrit al Centre Nacional d'Intel·ligència, d'acord amb allò establert a la Llei 11/2002, de 6 de maig i el Reial Decret 421/2004, de 12 de març, que la desenvolupa.

13 Secció 1.2.1.h) CCN STIC 807.
14 Secció 4.3.11 RDENS.
15 Secció 4.3.11 RDENS.

CVE-Núm. de registre: 022014008181

Establir acords de nivell de servei que considerin de forma específica les qüestions de responsabilitat, la fiabilitat dels serveis i els temps de resposta garantits, en aquells casos en que hi hagin tercers prestadors de serveis relacionats amb la criptografia.

15. Xifratge dels documents electrònics

- Els actes documentats, amb independència del tipus d'acte, requerirà el seu xifratge quan contingui dades personals o informacions sensibles, que hagin de romandre reservades.

- Es podrà escollir entre xifrar la totalitat del document o només la secció o les seccions que continguin dades personals de nivell alt o dades sensibles.

- La informació sensible o amb dades personals de nivell alt, ha d'estar xifrada tant durant la seva transmissió com durant el seu emmagatzematge. Només ha de trobar-se en clar mentre s'està fent ús d'ella[16]. En particular, i amb independència del nivell de seguretat, s'han de xifrar tots els suports d'informació que es poden remoure de l'ordinador, com discos, claus de memòria USB i altres anàlegs, així com i la informació de nivell alt que es contingui en ordinadors portàtils[17]. Addicionalment, quan la informació sigui de nivell alt, s'han d'utilitzar algorismes de xifrat aprovats[18] per la instrucció general de seguretat criptogràfica.

- Els actes de comunicació amb els ciutadans requereixen, en general, de xifratge sempre que es transmetin dades personals, mitjançant les capacitats de xifratge de la seu electrònica.

- Els actes d'intercanvi de dades entre administracions públiques o l'accés a dades d'altres administracions públiques, exigirà el nivell mínim exigit per cada administració que cedeix o dóna accés a dades.

- Els actes ordinaris del personal al servei de la Diputació de Barcelona no han de requerir, en general, del xifratge, que ha de ser expressament autoritzat i exercit d'acord amb aquesta política de signatura electrònica.

- Els certificats a emprar han de permetre, en tot cas, la recuperació de la clau privada, per tal de garantir que en qualsevol cas i situació serà possible accedir a la informació xifrada.

- En general, es poden fer servir els següents tipus de certificats:

• Actuació administrativa formalitzada i actes de comunicació:

Actuació manual: Certificats de personal al servei de la Diputació de Barcelona de nivell 4 (per exemple CPISR-1 Càrrec emès per CATCert) o equivalent.

Actuació automatitzada: Certificats de segell electrònic de la Diputació de Barcelona (per exemple un CDA-1 Segell nivell mig o alt emès per CATCert) o equivalent.

Comunicació web: Certificats de seu electrònica o de servidor segur, almenys de nivell mig en seus de nivell baix o mig, i de nivell alt en bens d'equip criptogràfic en nivell alt.

• Actuació d'intercanvi de dades o accés a dades entre administracions:

Els certificats admesos per cada administració que cedeix o dóna accés a dades a la Diputació de Barcelona.

16. Evidència electrònica de l'actuació administrativa

Els sistemes d'informació que gestionin dades, sigui en format documental, estructurat o de qualsevol altres formes, que hagin de tenir garantit el valor evidencial, han d'avaluar, implementar i documentar els següents controls:

- La captura d'informació, incloent-hi:

• Procediments per a la generació d'informació.
• Procediments per a la importació d'informació.

16 Secció 5.7.3 RDENS; articles 101 i 104 RD 1720/2007.
17 Secció 5.3.3 RDENS; article 101 RD 1720/2007.
18 Secció 5.5.2 RDENS.

CVE-Núm. de registre: 022014008181

• Procediments per a la digitalització de documents.
• Extracció de dades.
• Captura de metadades.

- El tractament dels objectes digitals automodificables, com per exemple, els fitxers amb codi actiu que permeti diferents representacions del contingut.

- El tractament dels objectes digitals compostos, com els expedients electrònics, els documents amb múltiples parts o els registres correlats de diaris d'activitat.

- El tractament del control de versions dels objectes digitals.

- L'emmagatzematge de la informació, incloent-hi:

• Els procediments per demostrar que la informació no ha estat alterada.
• L'ús de tecnologia d'emmagatzematge adequada.
• La implementació de procediments de migració.
• L'ús de formats d'emmagatzematge.
• Els procediments de conversió de fitxers.

- La transferència d'informació, incloent-hi:

• Els procediments de preparació d'objectes digitals, remoció de codi maliciós, ús de tècniques de compressió, ús de xifratge, determinació i verificació de la identitat de les parts, ús de signatures electròniques, conversió a altres formats de fitxers, selecció de canal, procediments d'inici, recepció i control de qualitat d'enviament.

• Els mecanismes i canals de transmissió.

• La regulació jurídica dels sistemes de transmissió, com el correu electrònic o les xarxes interadministratives.

- La indexació de la informació.

- Els procediments de sortida autenticada de la informació emmagatzemada.

- La gestió de la identitat de les parts referides a la captura i transmissió de la informació evidencial.

- La disposició/destrucció de la informació evidencial.

- Els procediments i mesures de seguretat de la informació, incloent-hi:

• El control d'accés a la informació.
• L'ús del xifratge.
• L'ús de les signatures electròniques.
• Les còpies de rescabalament de la informació.
• La planificació de continuïtat del negoci.

- El manteniment del sistema.

- L'ús de proveïdors externs, incloent-hi:

• L'adequació del procediments del tercer.
• El compliment legal.
• La seguretat en la transferència.

- La prova del sistema d'informació.

- L'auditoria interna i externa.

- La millora del sistema.

CVE-Núm. de registre: 022014008181

TÍTOL III. NORMES D'ORGANITZACIÓ I GESTIÓ

17. Proposta de modificacions

Correspon a la director/a de Serveis de Tecnologies i Sistemes Corporatius (DSTSC), o el càrrec directiu que n'assumeixi la funció, l'avaluació i proposta d'aprovació de les modificacions que calgui realitzar a la present Política de Signatura Electrònica, així com de la proposta d'aprovació de polítiques de signatura específiques, si s'escau.

18. Aprovació dels estàndards, guies i procediments d'administració electrònica.

El director/a de Serveis de Tecnologies i Sistemes Corporatius (DSTSC), o el càrrec directiu que n'assumeixi la funció, proposarà l'aprovació de les guies, instruccions, estàndards tècnics i procediments a utilitzar en aplicació del que es disposa en aquesta Política de Signatura Electrònica, i en les polítiques de signatura específiques que es trobin en vigor.

19. Autorització d'ús de tècniques de xifratge

Correspon al Director dels Serveis de Tecnologies i Sistemes Corporatius (DSTSC) o al càrrec directiu que n'assumeixi la funció, la determinació dels instruments de xifratge a utilitzar en aplicació d'aquesta Política de Signatura Electrònica, i l'autorització expressa per al seu ús en cada procediment concret en què sigui requerida aquesta funcionalitat.

20. Aprovació d'aplicacions i sistemes.

L'aprovació de les aplicacions i dels sistemes en suport de procediments administratius queda subjecta al compliment de les normatives, estàndards tècnics, guies, instruccions i procediments indicats en el punt 18è d'aquesta Política de Signatura Electrònica.

21. Gestió de la Política de Signatura Electrònica

El manteniment, actualització i publicació electrònica de la present Política de Signatura Electrònica, correspondrà a la Direcció de Serveis de Tecnologies i Sistemes Corporatius, o unitat orgànica funcional que n'assumeixi les funcions, essent responsable de la seva difusió a la seu electrònica corporativa tant de la seva versió actualitzada, com de l'historial de les versions anteriors.

Amb la publicació de cada actualització caldrà identificar el lloc on un validador podrà trobar totes les versions anteriors per a verificar una signatura electrònica anterior a la política vigent.

En el moment de la signatura s'haurà d'incloure la referència de l'identificador únic de la versió del document de política de signatura electrònica sobre el que s'ha basat la seva implementació, el qual determina les condicions que ha de complir la signatura electrònica en un moment determinat.

22. Protecció de dades de caràcter personal

La Diputació de Barcelona utilitzarà les dades personals contingudes en els certificats electrònics exclusivament per les finalitats de verificació de la identitat personal del subscriptor, i de la signatura electrònica dels seus missatges o documents.

La Diputació de Barcelona exigirà consentiment exprés segons el que indica la normativa en matèria de protecció de dades per a l'ús de les dades personals amb finalitats diferents a les esmentades en el paràgraf anterior. Aquest consentiment exprés podrà ser recaptat i autoritzat per mitjans electrònics.

Així mateix, la Diputació de Barcelona es compromet a protegir les dades personals d'acord amb l'establert a la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de dades de caràcter personal, el Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, i resta de normativa aplicable en la matèria, amb compliment de les adequades mesures de seguretat.

23. Arxiu i custòdia

Per a garantir la fiabilitat d'una signatura electrònica al llarg del temps, aquesta haurà de ser complementada amb la informació de l'estat del certificat associat en el moment de la signatura i/o informació no repudiable incorporant un segell de temps, així com els certificats que conformen la cadena de confiança.

CVE-Núm. de registre: 022014008181

Això implica, que si es vol disposar d'una signatura perdurable, que pugui ser validada al llarg del temps, la signatura electrònica generada per a cada acte administratiu o document en concret, haurà d'incloure evidències de la seva validesa per tal que en cap moment pugui ser repudiada i posada en qüestió la seva autenticitat. Per aquesta tipologia de signatures haurà d'existir un servei que mantingui les evidències esmentades, i caldrà sol·licitar l'actualització de les signatures abans de què les claus i el material criptogràfic associat siguin vulnerables.

Serà necessari que amb posterioritat les signatures es puguin renovar i actualitzar els elements de confiança per garantir la fiabilitat de la signatura electrònica de forma perdurable en el temps.

Per l'arxiu i gestió de documents electrònics se seguiran les recomanacions de les guies tècniques de desenvolupament de l'Esquema Nacional d'Interoperabilitat (RDENI) i les normes i procediments establerts a la Política de gestió documental aprovada a l'efecte."

Segon.- La Política de Signatura Electrònica aprovada per aquest Decret serà d'aplicació preceptiva a tots els instruments de gestió electrònica dels procediments administratius operatius a la Corporació mentre no se n'aprovi una altra, general o específica, que expressament la substitueixi.

Els procediments electrònics existents a la data d'aprovació hauran de ser adaptats a la present Política de Signatura en el termini màxim de 6 mesos a partir de la data de la seva aprovació.

Tercer.- Delegar en el President delegat de l'Àrea d'Hisenda, Recursos Interns i Noves Tecnologies l'aprovació, a proposta de la Direcció de Serveis de Tecnologies i Sistemes Corporatius (DSTSC), de les Instruccions generals, dels instruments de gestió i dels estàndards tècnics necessaris per a la correcta implantació i manteniment de la Política de Signatura electrònica de la Diputació de Barcelona.

Quart.- Publicar la present Resolució en el *Butlletí Oficial de la Província de Barcelona* i en la Seu Electrònica Corporativa."

Barcelona, 27 de març de 2014
La Secretaria delegada, Albert Ortiz Villuendas

CVE-Núm. de registre: 022014008181