Àrea d'Hisenda, Recursos Interns i Noves Tecnologies
Direcció de Serveis de Tecnologies i Sistemes Corporatius

DECRET

Núm. d'expedient	2015/0005627	**Codi XBMQ**	
Promotor	20300-Direcció de serveis de tecnologies i sistemes corporatius		
Tipus d'expedient	Altres		
Objecte	Aprovació de la Instrucció Tècnica per a la preservació de signatures electròniques: ressegellat en el temps.		
Destinataris	Totes les àrees de la Corporació	**NIF/DNI**	
Núm. op. Comptable		**Import total**	
Altres serveis			
Ref. interna		**Acte de referència**	D 2147/14

La Llei 29/2010, de 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya, té per objectiu potenciar l'ús intensiu dels mitjans electrònics per part de les Administracions Públiques per tal d'assolir unes relacions amb la ciutadania i el sector productiu orientades a les seves necessitats, amb plenes garanties de seguretat, transparència i accessibilitat.

L'article 24 de la Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya, en relació al dret a l'ús dels mitjans electrònics, estableix que les administracions públiques han d'habilitar, de la manera que considerin adequada, diferents canals o mitjans per a la prestació dels serveis electrònics, i garantir la seguretat, la confidencialitat i la protecció de les dades de caràcter personal en l'exercici del dret a l'ús dels mitjans electrònics.

D'acord amb l'article 18.2 del Reial Decret 4/2010, de 8 de gener, mitjançant el qual s'aprova l'esquema nacional d'interoperabilitat que preveu *"Las Administraciones Públicas aprobarán y publicaran su política de firma electrónica y de certificados partiendo de la norma técnica establecida a tal efecto en la Disposición adicional 1a, que podrá convivir con otras políticas particulares para una transacción determinada en un contexto concreto"*.

L'article 33.2 del Reial Decret 3/2010, de 8 de gener, mitjançant el qual s'aprova l'Esquema Nacional de Seguretat estableix que *"la política de firma electrónica y de certificados concretará los procesos de generación, validación y conservación de firmas electrónicas, así*

como las características y requisitos exigibles a los sistemas de firma electrónica, los certificados, los Servicios de sellado de tiempo, y otros elementos de soporte de las firmas ...".

Vist el Decret de Presidència de data 24 de març de 2014, publicat en el Butlletí Oficial de la Província de Barcelona de 3 d'abril de 2014, pel qual s'aprova la Política de Signatura Electrònica de la Diputació de Barcelona, en concret els apartats següents:

- Títol I, Abast de la política de signatura electrònica, epígraf 2n, Formats admesos: "*Per tal de protegir la signatura electrònica de la possible obsolescència dels algoritmes 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 algoritme més resistent.*"
- Títol I, Abast de la política de signatura electrònica, epígraf 5è, 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 algoritmes 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 pugui 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 evidències, 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, epígraf 12è, Processos de signatura electrònica; 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 algoritmes 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."

- Títol III, Normes d'organització i gestió, epígraf 17è, Proposta de modificacions: "*Correspon a la director/a de Serveis de Tecnologies i Sistemes Corporatius (DSTSC) o al càrrec directiu que n'assumeixi 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.*"
- Títol III, Normes d'organització i gestió, epígraf 18è, 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.*"
- Títol III, Normes d'organització i gestió, epígraf 21è, 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.*"
- Títol III, Normes d'organització i gestió, epígraf 23è, 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.*
  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 que 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."

Atès que cal procedir a l'aprovació de la corresponent Instrucció Tècnica per a la preservació de signatures electròniques: ressegellat en el temps.

Vist l'apartat tercer, part resolutiva, del Decret de Presidència 2147/14, d'aprovació de la Política de Signatura Electrònica de la Diputació de Barcelona.

En virtut de tot això, es proposa l'adopció de la següent:

RESOLUCIÓ

Primer. Aprovar la Instrucció Tècnica per a la preservació de signatures electròniques: ressegellat en el temps, en relació al contingut següent:

> ***Instrucció Tècnica per a la preservació de signatures electròniques: ressegellat en el temps.***
>
> *S'entén per signatures electròniques longeves aquelles que permeten garantir la seva validesa a llarg termini, fins i tot una vegada vençut el període de validesa del certificat del signatari. Aquestes signatures incorporen informació addicional o evidències que permeten demostrar la validesa i fiabilitat del document signat en un instant de temps determinat, i aquestes evidències poden estar protegides amb un segell de data i hora. Diem així que una signatura electrònica longeva permet incloure tota una cadena d'evidències electròniques en què sustenta la seva validesa.*
>
> *A nivell de format de signatura es consideren signatures longeves aquelles que compleixen els estàndards XAdES (XML Advanced Electronic Signatures), CAdES (CMS Advanced Electronic Signatures) i PAdES (PDF Advanced Electronic Signatures).*
>
> *Tot i que les estratègies per aportar solucions a la problemàtica de la gestió i manteniment de les signatures electròniques encara no estan molt consolidades, n'hi ha tres que s'estan postulant com les estratègies a seguir:*
>
> *a) Manteniment de la validesa tècnica de les signatures mitjançant una política de ressegellat de signatures o addició de segells de data i hora a cada objecte de signatura.*
> *b) Emmagatzemament de les signatures electròniques (i documents) en un magatzem digital o serveis d'arxiu de confiança (Trusted Archives Services).*
> *c) Solució híbrida: arxiu de les signatures electròniques (i documents) en un magatzem digital de confiança amb ressegellat.*

La solució adoptada per la Direcció de serveis de tecnologies i sistemes corporatius, que és sobre la qual es basa aquesta Instrucció Tècnica és el ressegellat de signatures, d'acord amb el contingut següent:

A) Ressegellat de les signatures: <u>Introducció</u>

1. Objectiu

Tenir signatures electròniques longeves que permetin garantir la seva validesa al llarg del temps, fins i tot una vegada vençut el període de validesa del certificat del signatari.

L'objectiu principal d'aquesta tècnica es poder validar la signatura electrònica per mitjans tècnics i de forma automàtica. En aquest sentit, cal tenir present que una signatura longeva que contingui una cadena d'evidències electròniques completa constitueix prova plena davant d'un eventual litigi.

2. Definició

Aquesta estratègia, anomenada ressegellat, consisteix en mantenir la validesa de la signatura incorporant nou material criptogràfic, bàsicament segells de data i hora, dins de la mateixa estructura de la signatura electrònica, i concretament en elements definits per a aquesta finalitat.

Per garantir la fiabilitat i validesa d'una signatura electrònica al llarg del temps cal ressegellar la signatura –actualitzar el segell de data i hora, afegint una nova baula a la cadena d'evidències electròniques- abans que caduqui el certificat de l'autoritat de segellament de data i hora que va realitzar el segell anterior; de forma que sempre sigui possible determinar en quin moment es va

realitzar la signatura i, conseqüentment, verificar que el certificat del signatari era vàlid en aquell moment.

Un segell de data i hora és una signatura electrònica produïda per una autoritat de segellament de data i hora que garanteix la integritat de certa informació en un moment determinat, i on el temps prové d'una font fiable. És a dir, aquest tipus de signatures permeten garantir l'existència d'aquesta informació en una data i hora determinada i, per tant, realitzar la validació de la integritat i autenticitat de la informació en aquell instant.

3. Abast i formats de signatura suportats

Cal destacar que no totes les especificacions tècniques de signatura electrònica existents permeten habilitar la preservació mitjançant aquesta estratègia. Per tant, serà imprescindible que el format en el que estigui basada la signatura electrònica ho permeti.

A nivell europeu, les especificacions tècniques estandarditzades pel ETSI (European Telecomunications Standards Institute) que respecten la Directiva Europea de Signatura Electrònica (1999/93/EC) i que compleixen amb els requisits d'una signatura electrònica longeva en el temps són els següents:

- *ETSI TS 101 903, XAdES (XML Advanced Electronic Signatures).*
- *ETSI TS 101 733, CAdES (CMS Advanced Electronic Signatures).*
- *ETSI TS 102 778, PAdES (PDF Advanced Electronic Signatures).*

Per tant, per tal que aquesta estratègia sigui efectiva, un cop generada la signatura electrònica caldrà crear una cadena de confiança basada en segells de data i hora en què caldrà respectar els dos aspectes comentats anteriorment i que fan vulnerables les signatures. És per això que caldrà:

a) *Incorporar un primer segell de data i hora, que permeti ubicar en el temps l'existència de la signatura i que permeti deslligar la validesa d'aquesta d'estats futurs del certificat digital amb la que s'ha generat. Amb aquest segell de data i hora s'evita que la signatura deixi de ser vàlida un cop es revoca o caduca el certificat digital del signatari que l'ha produït, ja que permet realitzar la validació de la signatura en l'instant de temps indicat pel segell de temps. El primer segell de data i hora d'arxiu s'ha d'incorporar dintre del període de validesa criptogràfica dels elements a protegir.*
b) *Incorporar periòdicament un nou segell de data i hora, seguint les especificacions tècniques descrites en els estàndards d'ETSI, abans de que el darrer segell de data i hora de la cadena de confiança caduqui.*

Si algun dels algoritmes utilitzats en qualsevol dels elements de la cadena de confiança és declarat vulnerable, cal incorporar un nou segell de temps que utilitzi els algoritmes adequats per a que la robustesa de la cadena de confiança no es vegi afectada.

B) Ressegellat de les signatures: Implementació

La implementació de l'estratègia de ressegellat està lligada al Repositori Documental Digital (RDD) de la Diputació de Barcelona i implica dues accions:

a) *Registrar un document: és el punt d'entrada d'un document en el procés de ressegellat i on es verifica que compleix tots els requisits previs per poder aplicar la política de ressegellat.*
b) *Aplicar la política de ressegellat: és el procés que s'encarrega d'aplicar un nou segell de data i hora, seguint les especificacions tècniques descrites en els estàndards ETSI, abans de que el darrer segell de data i hora de la cadena de confiança caduqui.*

1. Registrar un document

Aquest és el punt d'entrada dels documents en el procés de ressegellat. L'origen sempre és el RDD i els passos són:

- *Es rep una petició de registrar un document i es verifica que està autoritzat. Si no està autoritzat retorna un error amb la descripció del problema.*
- *Es verifica que el document és una firma vàlida i compatible amb firma longeva (CAdES, XAdES o PAdES). Aquesta validació es realitza fent una crida al servei Validador (*és un servei que permet realitzar la validació de certificats digitals i signatures electròniques) *del Consorci d'Administració Oberta de Catalunya (CAOC). Si no es valida retorna un error amb la descripció del problema.*
- *Es calcula la data prevista de ressegellat a partir de la data de caducitat de la firma i el temps establert per la DSTSC com a marge del ressegellat (fixat en 6 mesos).*
- *Es notifica al temporitzador i entra en el cicle de ressegellat (informació inclosa en el 2 punt d'aquest apartat B).*
- *Final del procés. On s'informa de l'èxit del registre del document i les següents dades de la firma: data de la signatura, data de caducitat i data prevista de ressegellat.*

2. Aplicar la política de ressegellat: temporitzador

El procés de ressegellar està supervisat per un temporitzador. Es donen dues situacions:

a) *Recepció d'una notificació d'un nou document registrat: Verifica la data prevista de ressegellat i la data actual per programar novament el temporitzador, si cal.*

b) Activar el procés de ressegellat: Això es produeix quan el temporitzador s'activa per coincidir amb la data prevista de ressegellar d'un document registrat.

Quan arriba la data prevista de ressegellat d'un document es realitza el procés següent:

a) Es recupera el document amb firma electrònica del RDD.

b) S'envia al Servei Validador del CAOC per completar la firma. Es donen dues situacions que són totalment transparents:
- *La firma no és longeva (XAdES, CAdES o PAdES): es complementa per obtenir una firma longeva.*
- *La firma és longeva (XAdES-A, CAdES-A o PAdES-LTV): es torna a aplicar una firma longeva sobre l'anterior.*

c) Es retorna el document amb la firma electrònica longeva al RDD.

d) Es programa de nou el temporitzador segons les noves dates previstes de ressegellat calculades.

Segon. Incorporar aquesta Instrucció Tècnica com a Annex a la Política de Signatura Electrònica aprovada.

Tercer. Publicar aquesta resolució en la seu electrònica de la Diputació de Barcelona.

Barcelona, 29 de juny de 2015.
El Director de Serveis de Tecnologies i Sistemes Corporatius

Diputació Barcelona Xarxa de Municipis
Direcció de Serveis de Tecnologies i Sistemes Corporatius

Jordi Pericàs Torguet

Vista l'anterior proposta la RESOLC de conformitat

Barcelona, - 7 JUL. 2015
En dono fe,
La Secretària General

Revisat i conforme
El Secretari delegat
Albert Ortiz Villuendas
Secretaria General
0 3 JUL. 2015

Petra Mahillo García

El President delegat de l'Àrea d'Hisenda, Recursos Interns i Noves Tecnologies, en funcions

Secretaria General
- 8 JUL. 2015

Carles Rossinyol i Vidal