Diputació Barcelona

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

DECRET

Núm. d'expedient	2015/0004624	**Codi XBMQ**	
Promotor	20300-Direcció de serveis de tecnologies i sistemes corporatius		
Tipus d'expedient	900 Altres		
Objecte	Aprovació de la Instrucció Tècnica per a la generació del Codi Segur de Verificació per incorporar en els documents de la Diputació de Barcelona a lliurar als interessats com a còpies autèntiques paper de documents originals electrònics.		
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, "*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.*"
- Títol II, Directrius de signatura electrònica, epígraf 9è, Relació entre la signatura i el document signat, "*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.*"

- 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.*"

Atès que cal procedir a l'aprovació de la corresponent Instrucció Tècnica per a la generació del Codi Segur de Verificació per incorporar en els documents de la Diputació de Barcelona a lliurar als interessats com a còpies autèntiques paper de documents originals electrònics.

La present proposta es justifica en la circumstància derivada de l'existència ja d'aplicacions informàtiques que donen serveis de continuïtat (com el Tediba o el VNIS) que usen l'esmentat codi segur de verificació, i que per tant un cop aprovada la Política de Signatura Electrònica resulta procedent aprovar el més aviat possible aquesta instrucció, raó per la qual la seva tramitació no es pot ajornar sense que se'n derivi un perjudici rellevant per a l'adequada administració de la Direcció i, en conseqüència, per a l'interès públic.

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 generació del Codi Segur de Verificació per incorporar en els documents de la Diputació de Barcelona a lliurar als interessats com a còpies autèntiques paper de documents emesos per mitjans electrònics i signats electrònicament, en relació al contingut següent:

"Instrucció Tècnica per a la Generació del Codi Segur de Verificació a incorporar en els documents a lliurar als interessats com a còpies autèntiques paper de documents originals electrònics.

A) Característiques generals

S'entén per CSV el sistema de firma electrònica vinculat a l'administració pública, òrgan o entitat i, en el seu cas, a la persona signant del document, que permet comprovar la integritat del document mitjançant l'accés a la seu electrònica corresponent.

El procediment d'obtenció de Codi Segur de Verificació (CSV) serà mitjançant algorismes de resum criptogràfic HMAC (Keyed-Hash Message Authentication Code).

Un CSV és un codi de longitud fixa resultant del processament d'un missatge d'entrada de longitud arbitrària. L'objectiu d'un CSV és garantir l'autenticitat i integritat de les dades en base a les quals s'ha calculat, de manera que s'estableix una relació biunívoca entre el CSV i aquest conjunt d'informació. Per tant, en l'àmbit de l'Administració Pública, el codi protegeix les dades contingudes en un document, o el document mateix, de forma que la tècnica de CSV permet detectar si les dades protegides han sofert alguna alteració i invalidar-les.

El CSV, també ha de complir els següents requeriments:

a) El CSV generat ha de ser únic per a cada document.

b) Ha d'estar basat en un espai numèric suficientment gran que eviti la presentació de documents a partir de prova aleatòria per part d'un usuari, o mitjançant operacions simples d'addició o sostracció sobre un CSV conegut.

c) Un cop generat el CSV, el sistema el vincularà al document i al signant, ja sigui aquest electrònic o persona física.

El procediment criptogràfic MAC (Message Authentication Code) garanteix l'autenticació de l'origen d'un missatge, com per exemple, unes dades, un document o una comunicació electrònica, així com la seva integritat, sense haver d'emprar mecanismes de seguretat addicionals.

En general, un MAC es calcula emprant una clau simètrica secreta sobre un missatge, en aquest cas el conjunt d'informació sobre el que s'ha de generar el CSV. Per incrementar la seguretat el procediment es reforça complementant la funció MAC amb algorismes de resum criptogràfic, el que es coneix com HMAC.

Es podrà superposar al CSV una firma amb segell electrònic amb la finalitat de millorar la interoperatibilitat electrònica i possibilitar la verificació de l'autenticitat i integritat dels documents electrònics sense necessitat d'accedir a la seu electrònica corporativa per al seu contrast.

En definitiva, l'objectiu de les següents especificacions és, per una banda, poder disposar d'un rang de diferents valors CSV prou ampli per satisfer les necessitats d'assignació documental corporatives. Amb una longitud de CSV de 20 caràcters i un alfabet de representació de 16 símbols, el rang de diferents valors disponibles és de 16^{20}, la qual cosa ofereix també garanties d'impossibilitat d'accés aleatori a un document.

B) Esquema d'obtenció del CSV

El mecanisme d'obtenció d'un CSV mitjançant funcions criptogràfiques de resum HMAC sobre un conjunt d'informació (INFO) s'esquematitza en les etapes següents.

a) Entrada: INFO.
b) Generar una clau criptogràfica simètrica aleatòria K.
c) Aplicar sobre el conjunt (K,INFO) una funció de resum criptogràfic HMAC obtenint un codi resum H de longitud fixa.
d) Truncar el resum H a la longitud establerta per al CSV.
e) Verificar l'absència de col·lisions de CSV respecte d'altres preexistents al sistema. Cas de duplicitat iterar el procediment a partir de "b)".
f) Preservar al sistema la terna (K,INFO,CSV).
g) Sortida: CSV.

C) Especificacions

Per a la determinació de les especificacions d'obtenció del CSV es segueixen les recomanacions contingudes a la publicació NIST SP 800-107.

1. *Clau simètrica*
   - *Es generarà una clau simètrica aleatòria K per a cada petició d'obtenció de CSV.*
   - *La longitud de la clau serà de 64 bytes.*
   - *El mecanisme d'obtenció serà mitjançant un generador de números aleatoris que compleixi l'especificació RFC 1750.*
2. *Funció de resum*
   - *S'aplicarà l'algorisme SHA-256 generant-se un resum H de 256 bit.*

D) Codi Segur de Verificació

- *El CSV tindrà una longitud de representació de 20 caràcters.*
- *L'alfabet de representació del CSV serà el corresponent als dígits hexadecimals {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f} per a la codificació binària dels quals és suficient amb un codi de 4 bit.*
- *El CSV s'obtindrà truncant els 80 bit més a l'esquerra de la cadena de resum H i traduint-los a l'alfabet de representació.*

E) Missatge de sortida

El missatge de sortida serà el codi CSV.

F) Preservació

El conjunt constituït pel Missatge d'entrada, clau simètrica K i CSV es preservarà en el sistema, que garantirà la privacitat de la clau simètrica K, tot aplicant les mesures de seguretat oportunes que garanteixin la seva inalterabilitat."

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, 25 de maig 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 sobre l'aprovació de la Instrucció Tècnica per a la generació del Codi Segur de Verificació per incorporar en els documents de la Diputació de Barcelona a lliurar als interessats com a còpies autèntiques paper de documents originals electrònics, RESOLC de conformitat

Barcelona, 16 JUNY 2015

En dono fe,
La Secretària General

Petra Mahillo García

El President delegat de l'Àrea d'hisenda, recursos interns i noves tecnologies, en funcions

Carles Rossinyol i Vidal

03 JUNY 2015
Revisat i conforme
El Secretari delegat
Albert Ortiz Villuendas
Secretaria General

DIPUTACIÓ DE BARCELONA

Secretaria General
17 JUNY 2015