Consorci
Administració Oberta
de Catalunya

Informe sobre alternatives a l'ús dels applets de signatura

Generalitat de Catalunya

LOCALRET

Versió: 0.1

Data: 04/06/2015

Index

1 Objectius

L'objectiu d'aquest document és el de posar de manifest la problemàtica existent amb la tecnologia que dona actualment suport a la signatura electrònica personal en entorns web així com proposar alternatives que la mitiguin, i que millorin l'accessibilitat i usabilitat de les aplicacions d'administració electrònica que en fan us.

2 Antecedents

L'ús de la signatura electrònica d'usuari final des d'entorns web sempre ha estat un desafiament, per la necessitat d'accedir als diferents magatzems de certificats que navegadors i sistemes operatius utilitzen i, si s'escau, fer us de les claus moltes vegades hostatjades en dispositius criptogràfics. La solució a aquesta problemàtica ha passat històricament per l'ús d'applets java, que donen accés a aquestes funcionalitats i que eren accessibles des de la majoria dels navegadors que els usuaris empraven. L'ús d'applets de java requereix que els usuaris tinguin instal·lada una màquina virtual java i que aquesta sigui accessible des dels navegadors que empren els usuaris.

Durant els darrers dos anys, l'evolució de la tecnologia emprada pels navegadors a l'hora de desenvolupar eines de client, cada cop més basada en javascript, així com els creixents requisits de seguretat que l'ús de d'una màquina virtual java presenta a l'hora de treballar amb certificats digitals ha dificultat i molt l'ús d'aquesta tecnologia. Aquesta tendència va arribar al punt de la insostenibilitat el darrer 16 d'abril del 2015, amb la desactivació per defecte de la màquina virtual java al navegador Google Chrome i l'anunci de la impossibilitat de la seva execució des d'aquest navegador a partir del mes de setembre.

L'ús d'applets java està deixant de ser una opció.

3 Alternatives

Durant aquests darrers dos anys, el sector relacionat amb la signatura electrònica ha estat buscant alternatives a l'ús dels applets java. En aquest apartat es descriuen les principals solucions que s'estan plantejant.

3.1 Signatura des de javascript.

El grup de criptografia web del World Wide Web Consortium (W3C) està treballant en una especificació, que hauria de ser implementada per tots els navegadors, anomenada Web Cryptography API, que hauria de permetre la generació de signatures electròniques des del propi navegador amb javascript. Aquesta especificació està, des del 11 de Desembre del 2014, en estat *Candidate Recommendation*, i per tant encara no està disponible des per la majoria de navegadors.

Des del Consorci AOC s'han estat fent proves de signatura amb la implementació que ha fet Google d'aquesta especificació al seu navegador Chrome. Tot i que els resultats han estat positius, les proves han posat de manifest la mancança a la pròpia especificació d'un mecanisme per accedir al magatzem de claus que empra el navegador.

En definitiva, l'especificació que permetrà produir signatures electròniques des de javascript encara està en vies d'estandardització i no preveu totes les funcionalitats que es necessiten per permetre la signatura efectiva de documents. És una via que, per tant, actualment és insuficient.

3.2 Signatura amb aplicació d'escriptori.

Al ser la solució de signatura via javascript inviable actualment, alguns actors del sector de la signatura electrònica han desenvolupat aplicacions client natives d'escriptori que són invocades via protocol per les aplicacions web quan és necessari que l'usuari signi. Aquest és el cas de l'aplicació "Firma Fácil" desenvolupada per la *Dirección de Tecnologías de la Información y las Comunicacions* del Ministeri d'Hisenda i Administracions Públiques.

Tot i que l'aplicació desenvolupada acaba amb la necessitat d'executar applets de java des del navegador, obliga als signataris a haver instal·lat una aplicació al seu ordinador. Aquesta necessitat, tot i ser acceptable en alguns àmbits, por resultar ser massa feixuga en d'altres com pot ser la tramitació del ciutadà, que acostuma a signar molt esporàdicament. Per altra banda, mentre que els applets de java eren multi plataforma, els desenvolupadors de la solució han de mantenir una versió de la solució per cada sistema operatiu.

A la forja del CTT, a l'àrea de descàrregues del projecte *Cliente @Firma*, s'ha publicat una versió Beta del Client @Firma que implementa aquesta solució.

3.3 Extensions per als navegadors.

Alguns fabricants estan estudiant el desenvolupament d'extensions per als diferents navegadors per permetre operacions de signatura. Aquesta opció no obligaria a l'usuari a tenir una aplicació dedicada a aquest tipus d'operacions, però si seria necessari disposar d'aquesta extensió per instal·lar en la combinació navegador / sistema operatiu, presentant com a mínim els mateixos inconvenients de la opció anterior. Actualment el problema el presenta només el navegador Chrome, però si la tendència es manté, i la resta de navegadors deixen de donar suport als applets java, mantenir versions d'extensions per a tots els navegadors i sistemes operatius, ni que sigui els més utilitzats, seria inviable.

3.4 Signatura centralitzada.

Des de fa ja alguns anys, alguns fabricants de serveis relacionats amb la signatura electrònica ofereixen plataformes que permeten la gestió centralitzada de certificats digitals tant de programari com d'usuari final des d'un magatzem únic, controlat i segur.

En estar les claus custodiades en un dispositiu centralitzat, aquests serveis permeten accedir a les funcionalitats de signatura sense necessitat de que siguin les pròpies aplicacions web les que es comuniquin directament amb dispositius criptogràfics ni amb els magatzems de certificats de navegadors i sistemes operatius. Aquesta tecnologia és la que està al darrera de serveis com el "*DNI en la Nube*". Per altra banda, des del Consorci AOC la signatura personal emprant el servei Signador Centralitzat amb certificats T-CAT-P està en fase de proves.

Amb l'aprovació del Reglament Europeu 910/2014 relatiu a la identificació i als serveis de confiança, així com de la normativa tècnica que la desenvolupa, les signatures personals produïdes emprant aquest tipus de dispositius tindran la consideració de signatura qualificada, sent equiparables a les manuscrites en l'àmbit europeu.

3.5 Dispositius mòbils.

El creixement constant del mercat de la telefonia mòbil, així com de les prestacions que els terminals ofereixen, permet que siguin tinguts en compte com a mecanismes d'identificació i

magatzem de credencials. Alguns països com Estònia, Noruega i Finlàndia estan oferint, en estreta col·laboració amb les operadores de telefonia mòbil, sistemes d'identificació i signatura electrònica emprant claus emmagatzemades al SIM dels telèfons mòbils, que moltes vegades són utilitzades amb l'ajuda d'una app.

En aquesta línia, des del Consorci AOC, durant l'any 2014, es va fer un pilot anomenat idCAT Mòbil, que consistia en una app que emmagatzemava un certificat idCAT que es podia emprar en processos d'autenticació i signatura executats des d'un ordinador de sobretaula. Per altra banda, el projecte idCAT-SMS , que ofereix al conjunt de les Administracions Públiques Catalanes un sistema d'identificació de cara al ciutadà basat en l'enviament de codis d'un sol ús al mòbil, permet produir signatures electròniques ordinàries, vinculant la identitat dels signataris amb l'ajut d'un segell electrònic.

4 Proposta d'aplicació

Totes les alternatives presentades tenen la necessitat d'entomar algun tipus de desenvolupament per la banda de les aplicacions de negoci que les vulguin emprar, i no són per tant solucions aplicables de manera immediata. En molts casos, fins i tot impliquen canvis de paradigma i de model que requereixen temps, i que idealment caldria portar a terme després de haver fet una certa reenginyeria dels processos. És per això que, des del Consorci AOC es proposa seguir la següent estratègia.

4.1 Curt termini

Tal i com vàrem avançar al nostre article del 17 d'abril, a curt termini l'única cosa que es pot fer sense obligar als usuaris de l'applet a portar a terme cap desenvolupament és recomanar no emprar el navegador Google Chrome per fer servir aplicacions web que impliquin signatura electrònica. Naturalment, aquesta no és una solució a llarg, ni tant sols a mig termini. És només la recomanació que es fa als usuaris mentre s'implanten les solucions anteriorment descrites.

D'aquestes, a curt termini l'única que es podria implantar sense canviar el model de negoci de les aplicacions web usuàries passaria per implantar l'aplicació client desenvolupada pel Ministeri d'Hisenda i Administracions Públiques "Firma Fácil", però caldria estudiar en quins casos es pot implantar, i valorar si realment val la pena fer-ho tenint en compte les seves característiques.

4.2 Mig termini

Amb l'aprovació l'any 2010 del Real Decret 3/2010 que regula l'Esquema Nacional de Seguretat, i més recentment amb el nou Reglament Europeu 910/2014 relatiu a la identificació i als serveis de confiança, les Administracions públiques disposen d'un cert marge de maniobra a l'hora de seleccionar els mecanismes d'identificació i signatura electrònica per cada tipus d'actuació. En aquesta línia, el passat dia 8 de maig el Govern de l'Estat va aprovar la remissió a les Corts Generals el Projecte de Llei de Procediment Administratiu Comú de les Administracions Públiques que, entre d'altres, descriu els sistemes d'identificació i signatura electrònica que empraran les administracions al seu Capítol II. Els sistemes que es contemplen són (Article 9 i 10):

- Sistemes basats en certificats reconeguts o qualificats
- Sistemes basats en l'ús de segells electrònics

- Sistemes basats en claus concertades i qualsevol altre sistema que les administracions considerin vàlid en els termes i condicions que s'estableixin.

Val a dir que l'Article 10.3 obre la porta a l'acceptació dels mecanismes d'identificació com a mecanismes de signatura electrònica quan així ho disposi la normativa reguladora aplicable. Per altra banda, i per si això fos poc, l'Article 11 especifica que les Administracions Públiques només demanaran la signatura per formular sol·licituds, presentar declaracions responsables, interposar recursos, desistir d'accions i renunciar a drets.

Per tant, tenint en compte el marc jurídic i normatiu actual, així com els canvis que estan per venir, a mig termini els ciutadans i ciutadanes hauran de produir signatures electròniques basades en certificats digitals en molt poques ocasions, sent acceptables d'altres sistemes d'identificació i signatura més usables i que no requereixen d'una gran complexitat tecnològica.

Des del Consorci AOC estem impulsant l'ús d'aquests sistemes no criptogràfics, com és el ja esmentat idCAT-SMS, com a mecanisme d'identificació i signatura electrònica dels ciutadans i ciutadanes.

4.3 Mig/Llarg termini

Pel que fa a la signatura electrònica de treballadors públics i funcionaris, des del Consorci AOC entenem que la gestió de les credencials i el seu ús passarà a estar centralitzada. Tot i que la tecnologia ja està disponible, la implantació de projectes amb canvis que afecten a nivell tècnic, procedimental i de gestió és complexa i no soluciona la problemàtica presentada de manera immediata. En qualsevol cas, el reconeixement de la qualificació per part del ReIdAS de les signatures produïdes emprant serveis de signatura centralitzada fan que aquestes es del màxim nivell de garanties tècniques i jurídiques. Les millores que aporten aquests tipus de solucions a nivell d'usabilitat i gestió, i la possibilitat de accedir-hi des de diferents tipus de terminals sense que això impliqui l'ús d'un applet de signatura, fan que els serveis de signatura centralitzada s'estiguin implantant satisfactòriament en entorns tancats (organitzacions i col·lectius) i que fins i tot s'estigui plantejant el seu us en obert, com és el cas del DNI al Núvol.

5 Altres consideracions

El món de la identificació i signatura electrònica està en constant evolució. Les solucions proposades són les que estan en funcionament actualment, però n'hi ha d'altres que s'estan estudiant com les basades en claus custodiades en dispositius mòbils. Haurem d'estar pendents sobre aquesta evolució per veure de quina manera les noves propostes ajuden a millorar l'accessibilitat i usabilitat de les solucions d'administració electrònica. Avui dia els nous mecanismes de signatura electrònica es proposen amb aquesta voluntat, mantenint uns nivells de seguretat acceptables. La tecnologia que la sustentava basada en certificat digital en targeta, i que feia servir applets de java per produir signatures en entorns web, comença a presentar símptomes d'estancament, i entre tots hem de començar a pensar en emprar les noves propostes que la complementen.