Consorci
Administració Oberta
de Catalunya

# Procediment de Manteniment de Signatures Electròniques

Generalitat de Catalunya

LOCALRET

Versió: 0.2
Data: 18/10/2012
Arxiu: Procediment de Manteniment de Signatures v0.2 20120314.docx

## Index

# 1 Objectius

L'objectiu d'aquest document és el de proposar una solució a la problemàtica plantejada per sistemes que disposen de documents signats electrònicament, però que es sospita que les seves signatures han caducat i han deixat de ser validables. La casuística que es planteja inclou la caducitat del certificat del signatari en signatures sense segell de temps així com la del propi certificat que produeix el segell de temps.

# 2 Les signatures electròniques i el procés de verificació tècnica

Tal i com es defineix a la Llei 59/2003, una signatura electrònica és un conjunt de dades en format electrònic, consignats amb altres o associats amb ells, poden ser utilitzats en la identificació del signatari. La solució tècnica a aquests requeriments la dona la signatura digital basada en l'ús de certificats segons el model descrit per la "RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

Tal i com estableix aquest estàndard, per tal de garantir la validesa dels algorismes de criptografia utilitzats, els certificats són emesos amb una temps de vida limitat, que no sol superar els quatre anys, i que per altra banda pot ser terminat prematurament utilitzant el procediment de la revocació. Quan un certificat caduca o és revocat, la identitat del signatari deixa de poder ser assegurada tècnicament per si sola.

La "RFC 3126 - Electronic Signature Formats for long term electronic signatures" estableix els mecanismes que cal utilitzar a l'hora de garantir tècnicament la validesa de les signatures al llarg del temps, utilitzant el segellat de temps com a mecanisme per provar fefaentment la existència de la signatura electrònica en un moment determinat, en el qual es sap que el certificat estava vigent. Al estar basat en l'ús de certificats digitals, el segell de temps també s'ha de mantenir.

La mateixa RFC descriu un procediment, anomenat Validació, segons el qual es verifica si tècnicament, i tenint en compte la casuística descrita, es pot garantir la identitat del signatari d'un document. Com a resultat, el procediment estableix que les signatures poden ser vàlides o invàlides, segons si es pot assegurar la identitat del signatari o no.

Quan una signatura és invàlida, el que es vol dir es que la identitat del signatari no es pot garantir de manera automàtica amb la informació disponible. La signatura podria ser vàlida jurídicament, però no es pot demostrar tècnicament.

En aquest document es pretén donar una solució organitzativa a aquesta situació, mitjançant un procediment de manteniment de les signatures que incorpora element de confiança en el sistema de gestió documental.

# 3 Fonaments de dret

La Llei de Signatura Electrònica (Llei 59/2003, de 19 de desembre), en el seu article 8. A), estableix que la primera causa d'extinció de la vigència d'un certificat electrònic és l'expiració del període de validesa que figura en el certificat. Es tracta de la pèrdua definitiva d'eficàcia d'un certificat i les seves causes, tant previstes com imprevistes, davant de la suspensió temporal de l'eficàcia regulada en l'article 9 de la mateixa llei. Podem parlar

d'invalidesa del certificat per finalització del termini de vigència previst i invalidesa anticipada per causes no previstes (bàsicament la revocació del certificat).

El problema de fons és, doncs, la temporalització o qüestió de la determinació de l'instant en què es va utilitzar la clau, qüestió que condueix a la necessitat de l'ús del segell de temps en tots els documents signats digitalment si es vol demostrar que la signatura digital es va realitzar durant el període de validesa del certificat utilitzat per a la seva verificació.

# 4 Procediment

Així, l'objectiu del procediment descrit al present document és el de portar a terme un manteniment de les signatures electròniques allotjades en un sistema d'informació, detectant aquelles que no són verificables de manera automàtica i proposar la signatura d'un document com evidència probatòria de la vigència dels certificats en el moment escollit del temps.
El procediment és el que segueix:

1. Enviar a validar les signatures a mantenir en la data actual. El Consorci AOC ofereix dues eines que es poden utilitzar.

   - **PSIS**. S'ofereix en forma de *Webservice* i pot ser integrat per aplicacions de tercers permetent l'enviament massiu de fitxers de manera automàtica.
   - **S-Perdura**. Ofereix una interfície a través d'EACAT i permet el manteniment manual de signatures. Les signatures a mantenir cal que siguin enviades una a una.

2. El resultat de la validació pot ser:

   a. Signatura vàlida.
   b. Signatura invàlida. Certificat caducat o revocat sense segell de temps
   c. Signatura invàlida. Segell de temps caducat.
   d. Error durant el procés de validació.

3. Si la signatura és vàlida.

   a. Si la plataforma de validació utilitzada és capaç de completar la signatura incloent un nou segell de temps, guardarà aquesta nova versió de la signatura. La plataforma informarà sobre la seva nova data de caducitat que es guardarà per tal de poder programar una nova renovació.
   b. Si la plataforma de validació informa que la signatura és tècnicament vàlida però el seu format no permetés la seva actualització, es podrà guardar el tiquet signat emès per PSIS com a evidència que en el moment de la validació la signatura era bona.

c. En qualsevol cas, es considera una bona pràctica guardar els tiquets signats de PSIS.

4. Si la plataforma de validació retorna un error en el procés de validació, es notificarà aquest fet al Servei de Suport del Consorci AOC per tal que es pugui estudiar el cas.
5. Si la signatura digital és tècnicament invàlida al haver caducat el certificat del signatari i no disposar d'un segell de temps vàlid caldrà:

- enviar-la a validar en la data al·legada de signatura o en la data de signatura que consti en el document o en aquella data que el responsable de l'aplicació cregui que el mateix ja estava allotjat al sistema. Amb el conjunt de les noves validacions de les signatures que estiguin en aquesta condició es construirà un Índex de Signatures de Documents que llisti els documents i les signatures validades i les relacioni amb les respostes de la plataforma de validació.
- que una persona responsable del sistema de gestió documental, o bé de la plataforma de tramitació, signi un document, que contindrà l'Índex de Signatures de Documents esmentats fent constar que aquells estaven signats, i les seves signatures eren tècnicament vàlides, en el moment d'ingrés al sistema, aportant com a prova els tiquets de validació. Cada entitat haurà de determinar quina és la persona adequada per signar aquest document.

# 5 Contingut de l'índex de signatures de documents

L'objectiu d'elaborar aquest índex de signatures és el d'identificar inequívocament els documents que contenen les signatures generades amb certificat ha caducat ( o altres supòsits) i, addicionalment, dóna informació que pot ser pertinent a l'hora de demostrar que no ha estat compromesa la seva fiabilitat..

Una proposta de contingut per aquest índex consistiria en que cada entrada, corresponent a una signatura, contindrà:

1. *Subject* del certificat del signatari.
2. Data al·legada de signatura
1. Nom del document signat
2. Resum criptogràfic del document signat
3. Resum criptogràfic signat
4. En cas de signatures XMLDSig o XAdES, identificació de l'objecte signat
5. Referència al tiquet de validació de la signatura en la data al·legada

En qualsevol cas, cal identificar el document, la signatura i lligar-la amb l'evidència que assegura que el document i al seva signatura existien en el moment al·legat.

Addicionalment, es poden incloure garanties sobre la integritat dels documents i els objectes signats, com son els resums criptogràfics dels documents i les signatures.

# 6 Identitat i signatura del responsable

Finalment, tal i com ja s'ha dit, caldrà que la persona responsable designada signi un document per garantir l'existència de les signatures en la data de validació.

La signatura s'haurà de portar a terme obligatòriament amb un certificat personal de treballador públic de manera que es garanteixi la seva identitat, la seva pertinença a l'organització i, si s'escau, el seu càrrec.

La responsabilitat de la persona designada es limitaria a garantir l'autenticitat i la integritat dels documents que contenen els expedients electrònics; no certificaria la validesa legal o competencial ni del contingut dels actes que d'aquests se'n deriven. I així es podria fer constar a la propi document.

Es recomana produir una signatura avançada (BES), que en temps de validació haurà de ser completada a AdES-C pel seu posterior manteniment i preservació.

# 7 Sobre el manteniment de signatures

Els sistemes de gestió documental que tractin amb documents signats haurien de tenir en compte que els certificats amb els que es generen les signatures caduquen, i programar tasques de manteniment per tal d'incorporar elements de prova que garanteixin que aquelles signatures es van generar vàlidament.

En general, sobre tot quan s'han de signar documents que s'han de guardar durant un temps, es recomana:

1. Produir formats de signatura avançats, ja siguin XAdES,CAdES o PAdES, ja que són els únics que es poden anar completant en el temps. El format de les signatures a produir podrà ser fixat per política de signatura.

   Val a dir que els formats avançats en la seva forma més simple (BES/EPES), i que són els que s'acostumen a aconsellar produir en temps de signatura, són els que contenen:

   - El certificat del signatari
   - Una data de signatura al·legada
   - Opcionalment, Identificador de la política de signatura utilitzada.

2. Els sistemes de gestió documental haurien de tenir en compte el temps que s'ha de preservar un document dintre del sistema. Seria convenient disposar d'un catàleg que especifiqués els requisits pel que fa a la preservació de cada document, tenint en compte la legislació aplicable al mateix i el procediment al qual forma part.
3. El sistema hauria d'enviar a validar tots els documents signats electrònicament a PSIS abans de ser allotjades, guardant la seva versió completada amb un format AdES-C que retorna la pròpia operació de validació.

Aquest format, que també podrà ser fixat per política de signatura, afegeix a la signatura la següent informació:

- Un Segell de Temps
- Referències a tots els certificats arrel utilitzats durant el procés de validació
- Referència a les llistes de revocació utilitzades durant el procés de validació

Caldrà que el sistema guardi:

- La signatura completada a AdES-C
- La data de caducitat de la signatura
- Opcionalment, el tiquet de PSIS

4. El sistema de gestió documental haurà d'assegurar el manteniment de les signatures durant la fase activa dels documents. Per això aquests sistemes hauran de disposar de funcionalitats de manteniment periòdic de les evidències de les signatures, enviant-les a validar a PSIS abans que arribi la data de caducitat obtinguda durant la validació anterior. Serà doncs necessari disposar d'un procés en *batch* que agafi les signatures que estiguin apunt de caducar, i que calgui mantenir, les enviï a PSIS, i guardi la nova versió tant de la signatura, la nova data de caducitat i, si s'escau, el tiquet.

   Es recomana, demanar a PSIS el completat de les signatures a AdES-X durant la primera execució del sistema de manteniment. Només per aquelles signatures que s'hagin de mantenir una segona vegada (estant el document en fase activa més de 8 anys) es demanarà AdES-A, ja que aquest ocupa un espai molt més gran, i mantenir totes les signatures en aquest format pot tenir un cost important i innecessari.

   A l'Annex I d'aquest document conté un quadre resum dels formats avançats de signatura i les seves característiques. Per altra banda, al document 'S-Perdura: especificacions integració serveis web' es poden trobar exemples sobre com obtenir la data de caducitat de les signatures i demanar el seu completat.

5. Quan un expedient es tanca, cal fer un índex dels document que conté. Aquest índex s'ha de signar electrònicament i, mantenint aquesta signatura, no caldria mantenir totes les dels documents que conté l'expedient. Es recomana que, un cop tancats els expedients, aquests siguin enviats a la plataforma d'arxiu electrònic iArxiu que ofereix el consorci AOC i que ja ofereix aquestes funcionalitats.

# 8 Proposta de document de l'índex de signatures de documents

Amb l'objectiu de garantir l'autenticitat i la integritat dels documents que contenen els expedients electrònics, enumerats a l'Annex adjunt manifesto que aquests existien i es trobaven al gestor documental del sistema [Nom del sistema de gestió documental i entitat a la que pertany] en la data de validació que s'indica a tal efecte.

La signatura d'aquest document no implica la certificació de la validesa legal o competencial ni del contingut dels actes que d'aquests se'n deriven i es limita a garantir la dates en que els documents es trobaven allotjats al sistema.

Com a garantia de les evidències incorporades a les signatures, s'adjunten els fitxers signats de resposta del Servei de Validació de Certificats i Signatures del Consorci AOC, i que demostren que les signatures, en les dates garantides per aquest document, eren vàlides.

# 9 Referències

Ley 59/2003, de 19 de diciembre, de firma electrónica.

RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

RFC 3126 - Electronic Signature Formats for long term electronic signatures.

XML Advanced Electronic Signatures (XAdES) W3C Note 20 February 2003.

ETSI TS 101 733 CMS Advanced Electronic Signatures (CAdES).

ETSI TS 102 734 Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES).

ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES).

ETSI TS 102 904 Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES).

ETSI TS 102 778-1 PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES.

ETSI TS 102 778-2 PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1.

ETSI TS 102 778-3 PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles.

Consorci AOC. S-Perdura: especificacions integració serveis web. Localització: http://www.aoc.cat/Inici/SERVEIS/Gestio-interna/S-PERDURA/Com-utilitzar-ho

# Annex I: Quadre resum de formats de signatura avançats

| FORMAT | DESCRIPCIÓ | CARACTERÍSTIQUES |
|---|---|---|
| AdES - BES | Conté data de signatura al·legada i el certificat del signatari. | És el format de signatura avançada més simple i es pot completar per fer possible la seva preservació |
| AdES – EPES | Igual que BES amb identificador de política. | La política imposa regles i restriccions a l'hora de generar i validar les signatures |
| AdES-T | BES/EPES amb segell de temps. | Permet a les signatures sobreviure a la revocació del certificat del signatari |
| AdES-C | BES/EPES amb segell de temps i referències a:<br>• certificats de la cadena de certificació que ha emès el certificat del signatari<br>• llistes de revocació emprades durant la validació | És el format completat que retorna PSIS per defecte. Permet a la signatura sobreviure fins que caduca el certificat del segell de temps |
| AdES-X | Protegeix amb un segell de temps les referències afegides al format AdES-C. | Protegeix contra la possibilitat de compromís de les claus dels certificats de la cadena de certificació. |
| AdES-XL | Afegeix a AdES-X els valors de la cadena de certificació i informació de revocació. | Format que disposa de tota la informació necessària per la validació de manera autocontiguda. |
| AdES-A | Protegeix AdES-XL amb una seqüència de segells de temps | Format d'arxiu que disposa de tota la informació de validació de manera autocontinguda i que es manté per mitjà de successius segells de temps. |

- Formats produïts en fase durant la signatura
- Format retornat durant la primera validació
- Es recomana demanar aquest format durant la segona validació
- Format utilitzat per les plataformes d'arxiu i que es recomana utilitzar si són necessàries més de dues validacions durant la fase activa del document