Consejería de Hacienda y Administración Pública

Plataforma @firma

Adaptación de aplicaciones para utilización del formato CAdES

Versión: v01r00

Fecha: 26/03/2012

HOJA DE CONTROL

Título	Adaptación de aplicaciones para utilización del formato CAdES		
Entregable	Adaptación de aplicaciones para utilización del formato CAdES		
Nombre del Fichero	Adaptación de aplicaciones para utilización del formato CADES v01r00.pdf		
Autor	DGTHAE		
Versión/Edición	v01r00	**Fecha Versión**	26/03/12
		Nº Total Páginas	7

REGISTRO DE CAMBIOS

Versión	Causa	Responsable	Área	Fecha
v01r00	Primera versión del documento para publicación	DGTHAE	SCAE	26/03/12

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área
Manuel Perera Domínguez	Jefe de Servicio de Coordinación de Administración Electrónica	DGTHAE / SCAE
José Ignacio Cortés Santos	Gabinete de Administración Electrónica	DGTHAE / SCAE
Antonio Heredia Rizo	Oficina Soporte	UTE
Pablo Pizarro Armendariz	Oficina Soporte	UTE
Ernesto Salgado Suárez	Oficina Soporte	UTE

ÍNDICE

1 Introducción

Este documento tiene por objeto documentar el procedimiento a seguir por las aplicaciones y servicios integradas con la plataforma @firma v5 (servicios web nativos) que actualmente utilizan formatos de firma electrónica no avanzados (CMS) para que utilicen formatos de firma avanzados (CAdES).

El propósito de este documento es facilitar y contribuir al cumplimiento de lo dispuesto en la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración, aprobada por Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, en lo relativo a la aplicación de la firma electrónica basada en certificados con el propósito de "firma de contenido" como herramienta para garantizar la autenticidad, integridad y no repudio de aquel, en el marco sustantivo de la prestación de servicios de la plataforma @firma definido en el artículo 20 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

La primera versión de la plataforma @firma implantada en la Junta de Andalucía utilizaba de forma invariable y predefinida el formato de firma PKCS#7, un estándar de firma en formato binario ASN.1 recogido en RFC 2315. Este estándar fue evolucionado por IETF al estándar criptográfico CMS (Cryptographic Message Syntax) cuya especificación se recoge en RFC 5652 y que define un marco de propósito general. Sobre la especificación CMS se definió posteriiormente un nuevo formato denominado CAdES (CMS Advanced Electronic Signatures) basado en perfiles para la firma electrónica avanzada y recogido en la especificación ETSI TS 101 733.

El desarrollo en el año 2006 de la versión 5 de la plataforma @firma supuso la utilización del formato CMS de firma electrónica en detrimento del anterior formato PKCS#7. La versión actual de la plataforma permite el uso de formatos avanzados de firma electrónica.

Es objeto de este documento definir las tareas a realizar por los integradores de las aplicaciones afectadas (aplicaciones con funciones de firma electrónica integradas de forma nativa con @firma v5) para adaptarlas, en su caso, a la utilización del formato avanzado CAdES de firma electrónica.

Este documento no resulta aplicable a las aplicaciones integradas mediante el componente opcional de la plataforma denominado “extensión de compatibilidad” que únicamente contempla firma CMS, del cual forma parte asimismo la denominada "fachada de firma web", que posibilita la utilización de aplicaciones desarrolladas para versiones anteriores de la plataforma y que no debe ser utilizado en el desarrollo de nuevas aplicaciones y servicios de administración electrónica, debiéndose considerar como obsoleto y procederse a su eliminación.

2 Adaptación del cliente de firma electrónica

Para modificar el formato de firma utilizado en firmas de usuario es necesario modificar la interacción con el cliente de firma electrónica. El cambio consiste en modificar el fichero "***constantes.js***" que se distribuye con el cliente y modificar un parámetro del método "***setSignatureFormat***" del cliente.

Modificación del fichero "*constantes.js*"

El único cambio consiste en modificar el valor de la variable "*signatureFormat*" que debe quedar de la siguiente manera:

var signatureFormat = 'CADES'

Modificación en el javascript de la aplicación

En caso de utilizar la aplicación el método del cliente "*setSignatureFormat*", asegurarse que el parámetro utilizado es "CADES":

clienteFirma.setSignatureFormat("CADES");

3 Adaptación de la integración con @firma (servicios web)

Además de los cambios en cliente descritos en el apartado anterior, es necesario asegurar que en la llamada que se realiza a los servicios web de firma electrónica se establece el parámetro "*formatoFirma*" con el valor "*CADES*". Los servicios web afectados son:

- FirmaServidor.
- FirmaServidorCoSign
- FirmaServidorCounterSign
- FirmaUsuario2FasesF2
- FirmaUsuario3FasesF3
- FirmaUsuario3FasesF1CounterSign
- FirmaUsuario3FasesF1CoSign
- FirmaUsuarioBloquesF3

También de cara a la validación de las firmas, se requiere que no se establezca ningún valor al parámetro "*formatoFirma*" de los siguientes servicios web:

- ValidarFirma.
- ValidarFirmaBloquesCompleto.
- ValidarFirmaBloquesDocumento.
- ObtenerFirmaTransaccion.

4 Referencias

Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.
http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-13171

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. .
http://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-1331