
Plataforma @firma

# Novedades de la versión 3.1 del cliente de firma electrónica

Versión: v01r01

Fecha: 18/11/2010

# HOJA DE CONTROL

| | | | |
|---|---|---|---|
| **Título** | Novedades de la versión 3.1 del cliente de firma electrónica | | |
| **Entregable** | Novedades de la versión 3.1 del cliente de firma electrónica | | |
| **Nombre del Fichero** | Novedades_cliente 3_1_v01r01 | | |
| **Autor** | José Ignacio Cortés Santos <josei.cortes@juntadeandalucia.es><br>(Servicio de Coordinación de Administración Electrónica) | | |
| **Versión/Edición** | v01r01 | **Fecha Versión** | 18/11/2010 |
| **Aprobado por** | | **Fecha Aprobación** | 18/11/210 |

## REGISTRO DE CAMBIOS

| Versión | Causa del Cambio | Responsable del Cambio | Área | Fecha del Cambio |
|---|---|---|---|---|
| v01r00 | Versión inicial | SCAE | - | 15/11/2010 |
| v01r01 | Revisión del documento | SCAE | - | 18/11/2010 |
| | | | | |
| | | | | |

## CONTROL DE DISTRIBUCIÓN

| Nombre y Apellidos | Cargo | Área | Nº Copias |
|---|---|---|---|
| Manuel Perera Domínguez | Jefe de Servicio | SCAE | 1 |
| Juan José López Portillo | - | TELVENT | 1 |

Este documento se publicará en la web de soporte de administración electrónica de la Junta de Andalucía, en la dirección *https://ws024.juntadeandalucia.es*

## 1. ALCANCE Y RESUMEN

El objetivo de este documento es establecer a modo de resumen, las nuevas características y problemas resueltos respecto a la versión anterior 3.0.2 del cliente.

El nuevo cliente 3.1 resuelve la problemática detectada en las contrafirmas con sello de tiempo en formatos XML y las contrafirmas CAdES.

También se ha optimizado el código para Firefox y las librerías NSS, así como se ha mejorado la compatibilidad con las tarjetas criptográficas, característica más limitada de la versión anterior del cliente.

En cuanto a las nuevas funcionalidades cabe destacar:

– Incorporación de un nuevo modo de despliegue del cliente basado en JNLP con el que ya no es necesario cargar un applet instalador e instalar el cliente en el equipo del usuario. Para utilizar este método se requiere el uso de una versión de Java 6_10 o superior.

– Nuevos formatos de firma OOXML compatibles con Microsoft Office 2007, 2008 y 2010.

– Nuevo formato de firma PDF compatible con PAdES.

– Adaptación de los formatos de firma XAdES conforme a la versión 1.4.1.

– Adaptación de los formatos de firma CAdES conforme a la versión 1.8.1.

– Incorporación de filtros de certificados conforme a RFC 2254.

– Posibilidad de selección del almacén de certificados (incluidos certificados en disco).

En cuanto a compatibilidad, como puede comprobarse en los documentos pertinentes, se ha aumentado la compatibilidad en entornos Linux, así como se ha incorporado el navegador Chrome/Chromium en varias configuraciones. No obstante, se ha comprobado que existen incompatibilidades con la próxima versión de Firefox 4 (en fase beta en el momento de escribir este documento) y con el navegador Opera.

A continuación se detallan las características añadidas a esta versión y los errores más importantes que se han corregido.

## 2. NUEVAS CARACTERÍSTICAS

– Traducción de los mensajes del cliente de @firma a idioma inglés y autodetección del entorno del usuario (español por defecto).

– Optimización del tamaño al empaquetarse los ficheros jar con PACK2000.

– Nuevo método de despliegue del cliente basado en JNLP (sólo disponible para Java 6_10 o superior). Con este método no se requiere el uso del applet instalador.

– Soporte para los formatos de firma OOXML compatible con Microsoft Office 2007, 2008 y 2010.

– Generación de firmas PDF compatibles con el estándar PAdES manteniendo compatibilidad con Adobe Reader y el estándar ISO 32000-1.

– Generación de firmas XML conforme al estándar XAdES 1.4.1.

– Generación de firmas binarias conforme al estándar CAdES 1.8.1.

– Posibilidad de firmar subestructuras XML mediante transformaciones.

– Posibilidad de firmar hojas de estilo XML.

– Recuperación de certificados en base 64 desde servidores LDAP.

– Incorporación de un almacén de claves de cifrado de usuario para el cliente de @firma.

– Se incorporan mejoras para mejorar la detección de errores y diagnosticar problemas de ejecución.

– Se habilita el uso de filtros de certificados acordes a RFC 2254.

– Eliminación del algoritmo de firma MD2withRSA.

– Posibilidad de selección del almacén de certificados (incluidos certificados en disco).

## 3. ERRORES CORREGIDOS

– Errores varios en la generación de firmas XML (XMLDSig y XAdES).

– Modificaciones en la visibilidad de algunos métodos.

– Se soluciona el problema de acceso al almacen interno de Mozilla (“No se pudo cargar el módulo softokn3.dll”).

– Mejoras en la ejecución del cliente bajo el navegador Mozilla/Firefox.

– Solucionado el problema de contrafirmas con sello de tiempo.

– Corregido problema por el que se podía instanciar múltiples veces los almacenes PKCS#11.

– Mejoras en el proceso de carga del cliente de afirma.

– Corregidos errores con la firma mediante DNIe.

– Aumento de la compatibilidad con firmas XML realizadas con aplicaciones de terceros.

– Corregidos problemas con contrafirmas CAdES.

– Optimización del proceso de carga de NSS en entornos Windows /Firefox.

– Utilización de los certificados del perfil activo en Mozilla Firefox.

## 4. REFERENCIAS

| | |
|---|---|
| @firma | Plataforma de identificación, validación y firma electrónica<br>*https://ws024.juntadeandalucia.es/pluton/adminelec/ArTec/afirma.jsp?zona=9* |
| CAdES | CMS Advanced Electronic Signature<br>*http://en.wikipedia.org/wiki/CAdES_(computing)* |
| DNIe | DNI electrónico<br>*http://www.dnielectronico.es* |
| JNLP | Java Networking Launching Protocol<br>*http://es.wikipedia.org/wiki/JNLP* |
| NSS | Network Security Services<br>*http://en.wikipedia.org/wiki/Network_Security_Services* |
| OOXML | Office Open XML<br>*http://es.wikipedia.org/wiki/OOXML* |
| PAdES | PDF Advanced Electronic Signatures<br>*http://en.wikipedia.org/wiki/PAdES* |
| RFC 2254 | The String Representation of LDAP Search Filters<br>*http://www.faqs.org/rfcs/rfc2254.html* |
| XAdES | *XML Advanced Electronic Signatures*<br>*http://es.wikipedia.org/wiki/Xades* |