

# ¿Qué ofrece Autentia Real Business Solutions S.L?

Somos su empresa de **Soporte a Desarrollo Informático**.  
 Ese apoyo que siempre quiso tener...

## 1. Desarrollo de componentes y proyectos a medida



## 2. Auditoría de código y recomendaciones de mejora

## 3. Arranque de proyectos basados en nuevas tecnologías

1. Definición de frameworks corporativos.
2. Transferencia de conocimiento de nuevas arquitecturas.
3. Soporte al arranque de proyectos.
4. Auditoría preventiva periódica de calidad.
5. Revisión previa a la certificación de proyectos.
6. Extensión de capacidad de equipos de calidad.
7. Identificación de problemas en producción.



## 4. Cursos de formación (impartidos por desarrolladores en activo)

Spring MVC, JSF-PrimeFaces /RichFaces,  
 HTML5, CSS3, JavaScript-jQuery

Gestor portales (Liferay)  
 Gestor de contenidos (Alfresco)  
 Aplicaciones híbridas

Tareas programadas (Quartz)  
 Gestor documental (Alfresco)  
 Inversión de control (Spring)

Control de autenticación y  
 acceso (Spring Security)  
 UDDI  
 Web Services  
 Rest Services  
 Social SSO  
 SSO (Cas)

JPA-Hibernate, MyBatis  
 Motor de búsqueda empresarial (Solr)  
 ETL (Talend)

Dirección de Proyectos Informáticos.  
 Metodologías ágiles  
 Patrones de diseño  
 TDD

BPM (jBPM o Bonita)  
 Generación de informes (JasperReport)  
 ESB (Open ESB)



Powered by 

Hosting Patrocinado por  
**enREDados.com**



[Home](#) | [Quienes Somos](#) | [Empleo](#) | [Tutoriales](#) | [Contacte](#)



**CoNceptT**

Lanzado

## TNTConcept versión 0.4.1 (04/06/2007)

Desde [Autentia](#) ponemos a vuestra disposición el software que hemos construido (100% gratuito y sin restricciones funcionales) para nuestra gestión interna, llamado TNTConcept (auTeNTia).

Construida con las últimas tecnologías de desarrollo Java/J2EE (Spring, JSF, Acegi, Hibernate, Maven, Subversion, etc.) y disponible en licencia GPL, seguro que a muchos profesionales independientes y PYMES os ayudará a organizar mejor vuestra operativa.

**Las cosas grandes empiezan siendo algo pequeño** ..... Saber más en: <http://tntconcept.sourceforge.net/>

	<p><b>Tutorial desarrollado por: <a href="#">Javier Antoniucci</a></b></p> <p><b>Puedes encontrarme en <a href="#">Autentia</a></b>  <b>Somos expertos en Java/J2EE</b>  <b>Contacta en <a href="mailto:javier.antoniucci@autentia.com">javier.antoniucci@autentia.com</a></b></p>	 <p><b>NUEVO CATÁLOGO DE SERVICIOS DE AUTENTIA (PDF 6,2MB)</b></p> <p><a href="http://www.adictosaltrabajo.com">www.adictosaltrabajo.com</a> es el Web de difusión de conocimiento de <a href="http://www.autentia.com">www.autentia.com</a></p>  <p><b>real business solutions</b></p> <p><a href="#">Catálogo de cursos</a></p>
---	--	---

Descargar este documento en formato PDF [FirmasFirefox.pdf](#)

[Firma en nuestro libro de Visitas](#) <-----> [Asociarme al grupo AdictosAlTrabajo en eConozco](#)

### Java Reporting ReportMill

Great Java Report Tool - Free Eval! PDF, HTML, Excel, XML, Swing & more  
[www.reportmill.com](http://www.reportmill.com)

### Portal + BPM + ECM

Gestión unificada de personas, procesos y contenidos

Anuncios Google

**Fecha de creación del tutorial: 2007-06-27**

## Firmas Digitales muy Fácil con Firefox

### Introducción

Los certificados digitales son cada vez más populares y su utilidad no se limita sólo a identificar al usuario sino que también permite que éste "firme" electrónicamente datos con garantías de no repudio y reconocimiento legal en muchos países. Particularmente útil para que el usuario firme contratos u ordene productos/servicios, de consentimiento con validez legal, etc.

Para implementar certificados digitales en el navegador Microsoft Internet Explorer contamos con cuantiosa documentación y tutoriales sobre el tema, pero en el caso de Firefox estamos más escasos así que aquí va nuestro humilde aporte.

### En la página web

Firefox implementa el objeto JavaScript 1.2 "window.crypto" que encapsula el operador de firma y simplifica notablemente la etapa en cliente. Una vez en servidor, veremos cómo validar la firma y extraer información de la misma.

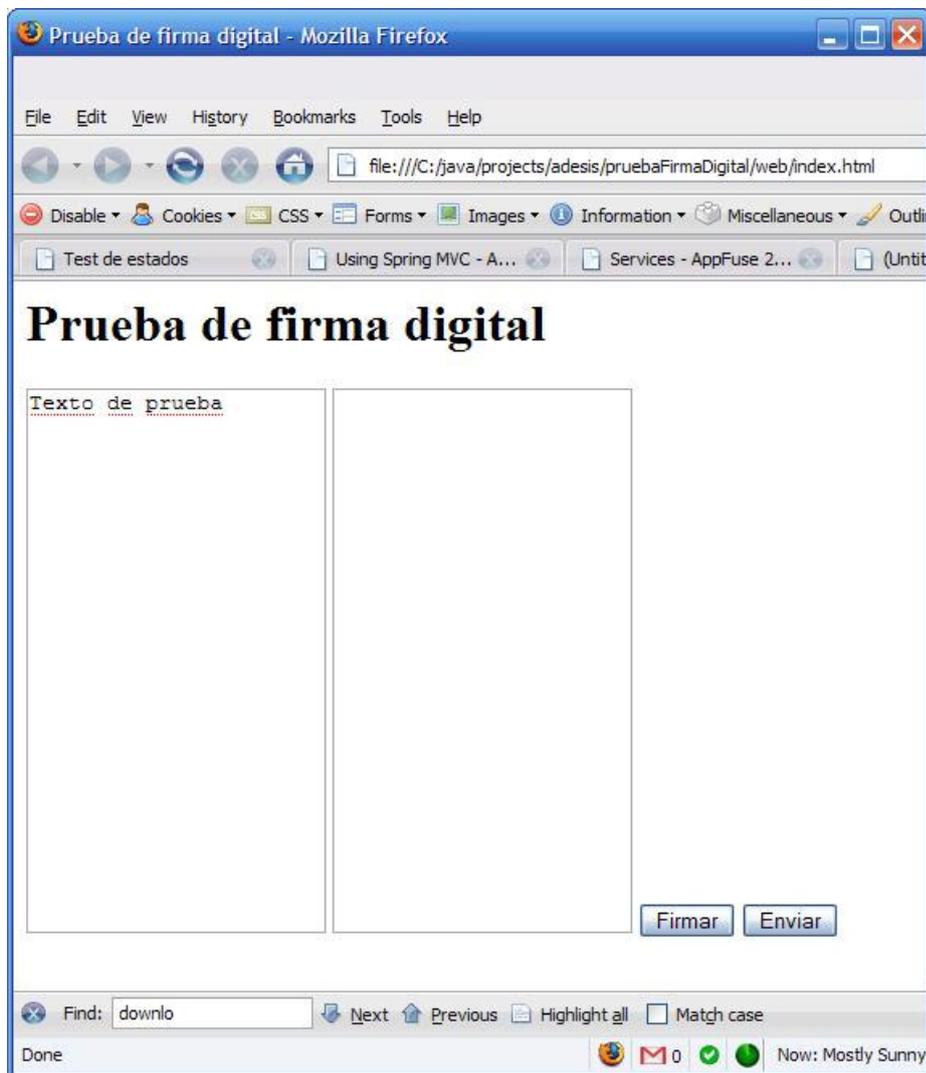
A fines de simplificar el ejemplo, copiamos una página muy breve con el JavaScript incrustado:

```
<html>
<head>
<title>Prueba de firma digital</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<script>
function firmar(original) {
if (navigator.appName=="Microsoft Internet Explorer"){
// Implementar la firma digital con MS IE con CAPICOM
} else {
return firmarFirefox(original);
}
}
function firmarFirefox(original) {
var firmado = window.crypto.signText(original, "ask");
if (firmado.substring(0,5) == "error") {
alert("Su navegador no ha generado una firma valida");
}
}
}

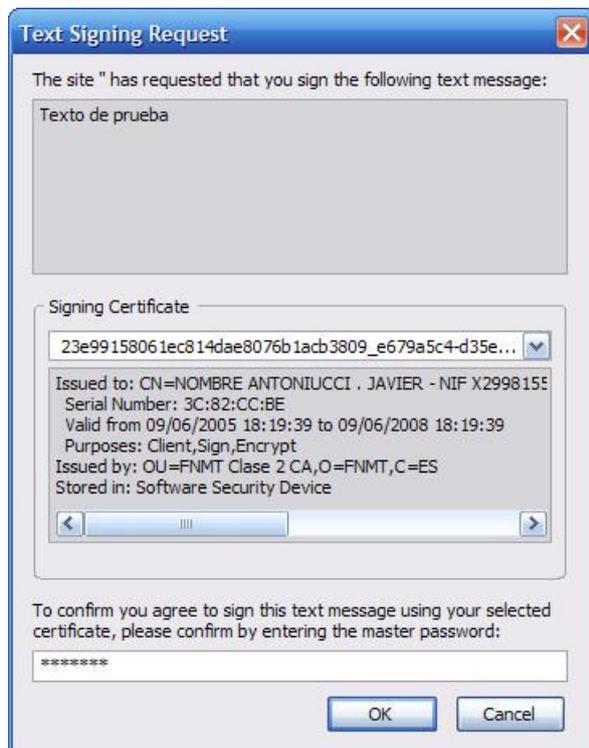
```

```
return "";  
}  
else if (firmado == "no generada") {  
alert("No ha generado la firma.");  
return "";  
}  
else {  
return firmado ;  
alert("Firma generada correctamente. Pulse enviar para comprobarlos en servidor.");  
}  
}  
</script>  
</head>  
<body>  
<h1>Prueba de firma digital</h1>  
<form action="CompruebaFirmaDigital" method="post">  
<textarea name="original" cols="20" rows="20">Texto de prueba</textarea>  
<textarea name="firmado" cols="20" rows="20"></textarea>  
<input type="button" value="Firmar" onclick="document.forms[0].firmado.value = firmar(document.forms[0].original.value)"/>  
<input type="submit" value="Enviar" />  
</form>  
</body>  
</html>
```

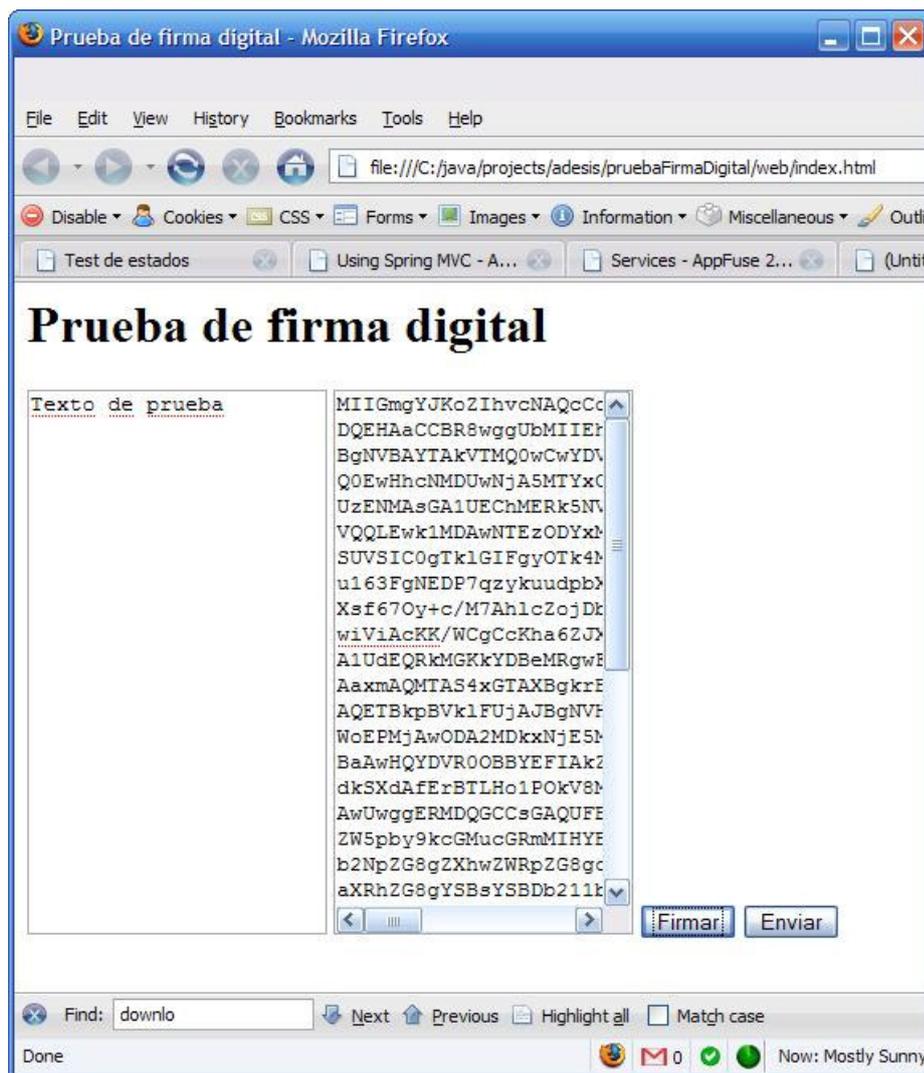
Como vemos, el formulario CompruebaFirmaDigital tiene un campo original donde pondremos el contenido a firmar.



Luego presionaremos el botón Firmar y Firefox nos mostrará un pop-up donde seleccionamos el certificado a utilizar:

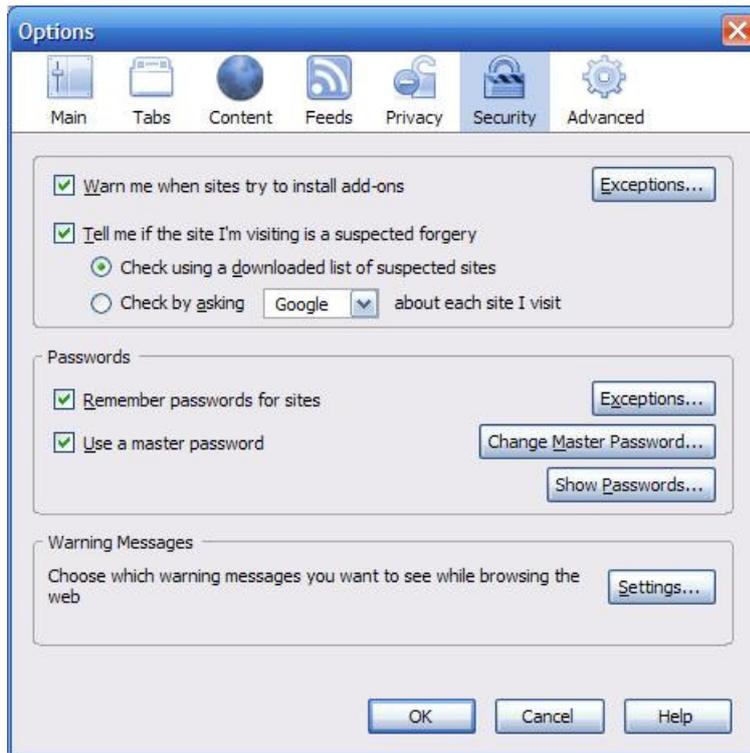


En esta ventana podemos comprobar el texto a firmar, seleccionar el certificado (podríamos tener varios instalados) e introducir la clave del repositorio\*. Al presionar OK, se generará en firmado la firma correspondiente.



El botón Enviar realizará el post al servlet que veremos en la siguiente sección.

\*Si no hemos definido ninguna clave de repositorio o "master password", deberíamos ir a Tools / Options / Security (o Herramientas / Opciones / Seguridad):



Y entonces seleccionar "Use a master password" y establecer la nueva clave pinchando en el botón "Change Master Password":



Es interesante observar la barra "Password quality meter" que calcula la dificultad de nuestra password en base a reglas como: contener letras en mayúsculas y minúsculas, números, caracteres de puntuación, etc.

## En el servidor

Vamos a crear un servlet donde:

1. Obtendremos el contenido original y el contenido firmado
2. Verificaremos que el firmado coincida con el original
3. Obtendremos más información desde el certificado

Y vamos directamente al código:

```
package com.autentia.tutorial.firmaDigital.firefox.servlet;

import java.io.IOException;
import java.io.PrintWriter;
import java.security.cert.X509Certificate;

import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
```

```

import javax.servlet.http.HttpServletResponse;

import com.sun.org.apache.xerces.internal.impl.dv.util.Base64;

import sun.security.pkcs.PKCS7;
import sun.security.pkcs.SignerInfo;

public class CompruebaFirmaDigital extends HttpServlet {

private static final long serialVersionUID = -1691697973877536487L;

@Override
protected void doPost(HttpServletRequest request, HttpServletResponse response) throws ServletException,
IOException {
    PrintWriter out = response.getWriter();
    String original = request.getParameter("original");
    String firmado = request.getParameter("firmado");

    try {
        PKCS7 p7 = new PKCS7(Base64.decode(firmado));
        SignerInfo[] si = null;

        // check if data is "attached" to this P7 blob
        if (p7.getContentInfo().getContentBytes() == null) {
            // do the verification on the data provided
            si = p7.verify(original.getBytes());
        }
        else {
            // original data is embedded or "attached" to this P7,implicit verification will do...
            si = p7.verify();
        }

        out.println("[VERIFY OK]");

        // printout the p7 contents
        out.println("[P7 CONTENES]");
        out.println(p7.toString());

        out.println("[EXTRACTING DATA]");
        // check if data is "attached" to this P7 blob
        if (p7.getContentInfo().getContentBytes() == null) {
            out.println("No data found");
        }
        else {
            out.println(p7.getContentInfo().getContentBytes());
        }
    }
    catch (Exception e) {
        out.print("[ERROR VALIDATING SIGNATURE]");
        e.printStackTrace();
    }
}
}

```

Al enviar un mensaje firmado, se ejecutará el servlet y obtendremos una página como la que copio a continuación:

```

[VERIFY OK]
[P7 CONTENES]
Content Info Sequence
  Content type: 1.2.840.113549.1.7.1
  Content: null
PKCS7 :: version: 01
PKCS7 :: digest AlgorithmIds:
  SHA
PKCS7 :: certificates:
  0. [
[
  Version: V3
  Subject: CN=NOMBRE ANTONIUCCI . JAVIER - NIF X2998155J, OU=500051386, OU=FNMT Clase 2 CA,
  O=FNMT, C=ES
  Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

  Key: Sun RSA public key, 1024 bits
  modulus: 131575675323991855481882695090604255354283802995994130325140287343442527550523287
  735330662450495312300738878218939717859247210783036875426139715204374930718984052460866831
  380022824796002705409063853029223667641707 5659210682004122052836707771024886312323336689
  83461209287086466595754860589074641524008749629753
  public exponent: 65537
  Validity: [From: Thu Jun 09 18:19:39 CEST 2005,
  To: Mon Jun 09 18:19:39 CEST 2008]
  Issuer: OU=FNMT Clase 2 CA, O=FNMT, C=ES
  SerialNumber: [ 3c82ccbe]

Certificate Extensions: 11
[1]: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
[OID.1.3.6.1.4.1.5734.1.1=JAVIER, OID.1.3.6.1.4.1.5734.1.2=ANTONIUCCI,
OID.1.3.6.1.4.1.5734.1.3=., OID.1.3.6.1.4.1.5734.1.4=X2998155J]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 40 9A 76 44 97 74 07 C4 AC 14 CB 1E 8D 4F 3A 45 @.vD.t.....O:E
0010: 7C 30 D7 61 .0.a
]
]

```

```

]
[3]: ObjectID: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 80 24 65 E9 F7 0E 54 3C 1A AD 49 69 CD 21 10 58 .$.e...T<..Ii!!X
0010: 0C 4D 04 17 .M..
]
]
[4]: ObjectID: 1.3.6.1.5.5.7.1.3 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 23 30 21 30 08 06 06 04 00 8E 46 01 01 30 15 .#0!0.....F..0.
0010: 06 06 04 00 8E 46 01 02 30 0B 13 03 45 55 52 02 .....F..0...EUR.
0020: 01 64 02 01 00 .d...
]
[5]: ObjectID: 1.3.6.1.4.1.5734.1.33 Criticality=false
Extension unknown: DER encoded OCTET string =
0000: 04 10 16 0E 50 45 52 53 4F 4E 41 20 46 49 53 49 ...PERSONA FISI
0010: 43 41 CA
]
[6]: ObjectID: 2.5.29.16 Criticality=false
PrivateKeyUsage: [
From: Thu Jun 09 18:19:39 CEST 2005, To: Mon Jun 09 18:19:39 CEST 2008]
]
[7]: ObjectID: 2.5.29.32 Criticality=false
CertificatePolicies [
[CertificatePolicyId: [1.3.6.1.4.1.5734.3.5]
[PolicyQualifierInfo: [
qualifierID: 1.3.6.1.5.5.7.2.1
qualifier: 0000: 16 28 68 74 74 70 3A 2F 2F 77 77 77 2E 63 65 72 .(http://www.cer
0010: 74 2E 66 6E 6D 74 2E 65 73 2F 63 6F 6E 76 65 6E t.fnmt.es/conven
0020: 69 6F 2F 64 70 63 2E 70 64 66 io/dpc.pdf
]
], PolicyQualifierInfo: [
qualifierID: 1.3.6.1.5.5.7.2.2
qualifier: 0000: 30 81 CB 1A 81 C8 43 65 72 74 69 66 69 63 61 64 0....Certificad
0010: 6F 20 52 65 63 6F 6E 6F 63 69 64 6F 20 65 78 70 o Reconocido exp
0020: 65 64 69 64 6F 20 73 65 67 FA 6E 20 6C 65 67 69 edido seg.n legi
0030: 73 6C 61 63 69 F3 6E 20 76 69 67 65 6E 74 65 2E slaci.n vigente.
0040: 55 73 6F 20 6C 69 6D 69 74 61 64 6F 20 61 20 6C Uso limitado a l
0050: 61 20 43 6F 6D 75 6E 69 64 61 64 20 45 6C 65 63 a Comunidad Elec
0060: 74 72 F3 6E 69 63 61 20 70 6F 72 20 76 61 6C 6F tr.nica por valo
0070: 72 20 6D E1 78 69 6D 6F 20 64 65 20 31 30 30 20 r m.ximo de 100
0080: 65 20 73 61 6C 76 6F 20 65 78 63 65 70 63 69 6F e salvo excepcio
0090: 6E 65 73 20 65 6E 20 44 50 43 2E 43 6F 6E 74 61 nes en DPC.Conta
00A0: 63 74 6F 20 46 4E 4D 54 3A 43 2F 4A 6F 72 67 65 cto FNMT:C/Jorge
00B0: 20 4A 75 61 6E 20 31 30 36 2D 32 38 30 30 39 2D Juan 106-28009-
00C0: 4D 61 64 72 69 64 2D 45 73 70 61 F1 61 2E Madrid-Espaa.
]] ]
]
[8]: ObjectID: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
SSL client
S/MIME
]
]
[9]: ObjectID: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:false
PathLen: undefined
]
]
[10]: ObjectID: 2.5.29.31 Criticality=false
CRLDistributionPoints [
[DistributionPoint:
[CN=CRL2049, OU=FNMT Clase 2 CA, O=FNMT, C=ES]
]]
]
[11]: ObjectID: 2.5.29.15 Criticality=false
KeyUsage [
DigitalSignature
Key_Encipherment
]
]
Algorithm: [SHA1withRSA]
Signature:
0000: 7F F2 DF B5 7B 2E 36 12 89 AD 3E FB C6 48 A6 63 .....6...>..H.c
0010: 5E CC E6 92 C6 14 86 93 AD 5D 09 F3 3D 04 CC 37 ^.....]!..=..7
0020: 29 DE 97 22 32 EA FE 23 B1 1C 46 B3 60 A4 23 9C )..*2...#.F.`.#.
0030: 08 CB 6F B8 8A 74 92 FF 9A C5 5A 8F 87 8D 17 6C .o.o.t...Z...l
0040: 2E 93 9A 3F 47 C1 77 38 24 00 0B 51 6F 26 29 3C ...?G.w8$.Qo&<
0050: B0 CF EE 72 AE CE F9 45 72 BA 3D A6 57 ED DF C8 ...r...Er.=.W..
0060: 79 4F 1D B8 EF 4F 5B 98 95 3E 49 D3 7A FD 2D 9B yO...O[.>I.z.-.
0070: 85 F6 95 9F 0F A5 D8 FE EA 48 D3 A3 E7 0F FB 76 .....H.....v
]
PKCS7 :: signer infos:
0. Signer Info for (issuer): OU=FNMT Clase 2 CA, O=FNMT, C=ES
version: 01
certificateSerialNumber: 3c82ccbe
digestAlgorithmId: SHA
authenticatedAttributes: PKCS9 Attributes: [
[ContentType: 1.2.840.113549.1.7.1];
[MessageDigest: 0000: 63 94 C1 CE 6B 7D AD 3A 34 04 68 01 53 A5 96 BF c...k...:4.h.S...
0010: 1E F3 96 12 ....
]

```

```

];
    [SigningTime: Wed Jun 20 12:17:33 CEST 2007]
  ] (end PKCS9 Attributes)
  digestEncryptionAlgorithmId: RSA
  encryptedDigest:
0000: 1A FD 86 01 B6 B6 85 27 87 FB AE 6C C0 78 FE 3C .....'.l.x.<
0010: 04 74 38 F2 F6 9B D2 29 46 47 EA 9F 36 E7 64 8D .t8....)FG..6.d.
0020: BB A2 A3 B5 0C A5 01 60 19 1C 30 09 3D EA BC 0C .....`.0.=...
0030: 63 4A 8A 2E BC C8 42 35 E1 3A D7 06 18 EB 38 3A cJ....B5.:...8:
0040: 89 B8 F8 BC 1E AC 0A 46 CE B5 1A 3D 6B F5 2C 2C .....F...=k,,
0050: 8A FD B8 05 9D 8B 79 64 73 00 26 CE 65 38 97 01 .....yds.&.e8..
0060: F9 3B 01 A4 11 58 FC B7 0E 27 7A D5 F6 7A 4F 69 ;...X...'z..zOi
0070: ED B2 20 3F 40 8A CA C1 CE FF 55 67 4E 3E F8 6B .. ?@.....UgN>.k

[EXTRACTING DATA]
No data found

```

## Consideraciones

Recordemos que lo que firma el usuario es un texto, así que si lo que queremos que firme es, por ejemplo, una solicitud de compra de productos deberemos traducir el formulario o "carrito de la compra" a un texto tipo "Don Juan Perez, con DNI XXX se compromete a comprar el 30 de Junio de 2007 los siguientes productos: 2 Cartuchos de Tinta HP6546 y 1 Papel 500x90g por un valor total de 67 euros (IVA incluido) pagaderos en efectivo y que serán enviados a C/Castellana, 1 Bajo C. En Madrid, a los 20 días del mes de junio de 2007."

## ¿Dónde encuentro más info?

Mozilla Development Center: JavaScript crypto [http://developer.mozilla.org/en/docs/JavaScript\\_crypto](http://developer.mozilla.org/en/docs/JavaScript_crypto)

Introducing MS CAPICOM <http://msdn2.microsoft.com/en-us/library/ms995332.aspx>

## Conclusiones

Con la popularización de los certificados digitales (más con llegada de los DNI electrónicos en España)

Muy buena herramienta, muy útil, muy estable y en constante evolución.

En [Autentia](#) tenemos mucha experiencia en desarrollo Web y podemos ayudarte a construir u optimizar tus portales o aplicaciones web. No dudes en ponerte en contacto con nosotros.



This work is licensed under a [Creative Commons Attribution-NonCommercial-No Derivative Works 2.5 License](#).  
[Puedes opinar sobre este tutorial aquí](#)



## Recuerda

que el personal de [Autentia](#) te regala la mayoría del conocimiento aquí compartido ([Ver todos los tutoriales](#))

¿Nos vas a tener en cuenta cuando necesites consultoría o formación en tu empresa?

**¿Vas a ser tan generoso con nosotros como lo tratamos de ser con vosotros?**

[info@autentia.com](mailto:info@autentia.com)

Somos pocos, somos buenos, estamos motivados y nos gusta lo que hacemos .....

**Autentia = Soporte a Desarrollo & Formación**

J2EE, EJBs, Struts...

[Autentia S.L.](#) Somos expertos en:  
**J2EE, Struts, JSF, C++, OOP, UML, UP, Patrones de diseño ..**  
 y muchas otras cosas

## Nuevo servicio de notificaciones

Si deseas que te enviemos un correo electrónico cuando introduzcamos nuevos tutoriales, inserta tu dirección de correo en el siguiente formulario.

<b>Subscribirse a Novedades</b>	
<b>e-mail</b>	<input type="text"/>
	<input type="button" value="Enviar"/>

## Otros Tutoriales Recomendados ([También ver todos](#))

Nombre Corto	Descripción
<a href="#">Creación y configuración de firmas y plantillas de fondos para Microsoft Office - Outlook</a>	En el siguiente tutorial, se explicará como crear y configurar archivos HTML para utilizarlos como firmas y fondos para Microsoft Outlook.
<a href="#">Certificados en IIS para activación SSL</a>	En este tutorial vamos a habilitar el soporte SSL (Secure Socket Layer, comunicación segura por https) en un servidor IIS (Internet Information Server de Microsoft).
<a href="#">Firmar Applets Java para MS Internet Explorer</a>	Cristhian Herrera nos enseña a firmar un Applets Java, para adquirir privilegios, en Internet Explorer, usando herramientas Microsoft
<a href="#">Firmar applets usando keytool y jarsigner</a>	En este tutorial os mostramos como firmar un applet con las herramientas incluidas en el JDK estándar
<a href="#">Desarrollando portales para móviles con FireFox</a>	En este tutorial, se va a presentar User Agent Switcher una extensión para el navegador Web FireFox que nos permite de una forma sencilla emular y probar aplicaciones Web sobre cualquier teléfono móvil a través del propio navegador.
<a href="#">Navegador Mozilla FireFox</a>	En esta ocasión probamos el estado de evolución del navegador gratuito Mozilla FireFox, una verdadera alternativa en el mercado.
<a href="#">Manejo de certificados digitales con keytool</a>	En este tutorial vamos a presentar un monográfico sobre la herramienta keytool y el manejo de certificados para habilitar el SSL (Secure Socket Layer, comunicación segura por https) en un servidor.

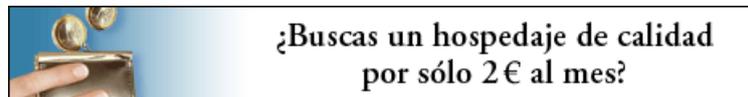
Nota: Los tutoriales mostrados en este Web tienen como objetivo la difusión del conocimiento.

Los contenidos y comentarios de los tutoriales son responsabilidad de sus respectivos autores.

En algún caso se puede hacer referencia a marcas o nombres cuya propiedad y derechos es de sus respectivos dueños. Si algún afectado desea que incorporemos alguna reseña específica, no tiene más que solicitarlo.

Si alguien encuentra algún problema con la información publicada en este Web, rogamos que informe al administrador rcanales@adictosaltrabajo.com para su resolución.

[Patrocinados por enredados.com .... Hosting en Castellano con soporte Java/J2EE](#)



www.AdictosAlTrabajo.com Optimizado 800X600