

GUÍA PRÁCTICA

Generación de Certificado de Servidor

Sevilla, Octubre de 2004

Versión 1.0

Andalucía en la Red

24

Y con Paco, Carmen, Pedro,
Rocio, Manolo, María, Peppe,
Luisa, Antonio, Concha, Juan,
Reyes, Fernando, Lucía, Alicia,
Cristina, Diego, Rogelio, Rafael, Isabel,
David, Macarena, Miguel, Sandra, Jorge,
Cristina, Aguilera, Susana, Estefanía, Iñargacilla,
Braldo, Louisa, Stanón, Inma, Carlos,
Julia, Roberto, Celso, Paloma, Estrella ...

Hoja de control

Fecha	Autor	Descripción
09/10/2004	Samuel Muñoz Rodríguez Cristóbal Ramírez Fernández	Versión inicial
08/02/2005	Leopoldo Pérez Ortiz	Actualización

Índice

<i>Índice</i>	3
<i>1. Generar la clave privada</i>	4
<i>2. Crear el fichero PKCS#10</i>	5
<i>3. Enviar el fichero PKCS#10</i>	6
<i>4. Generar el fichero PKCS#12</i>	7
<i>5. Instalar el certificado en el servidor</i>	9

Los pasos a seguir para la generación del certificado de servidor son los siguientes:

1. Generar la clave privada

Lo primero es **generar la clave privada** del certificado, que va a ser de 1024 bits, y la vamos a cifrar usando 3DES. Se nos va a pedir una palabra de paso cuando la estemos creando.

```
openssl genrsa -des3 -out nombreServidor.pem 1024
```

```
Ej : openssl genrsa -des3 -out afirma0.pem 1024
```

```
root@pluton:/usr/local/ssl
[root@pluton ssl]# dir
afirma0  certs  curso  include  man  openssl.cnf  private
bin      crt.pem demoCA  lib      misc  openssl.cnf.ori  scint3
[root@pluton ssl]# openssl genrsa -des3 -out afirma0.pem 1024
Generating RSA private key, 1024 bit long modulus
....+++++
.....+++++
e is 65537 (0x10001)
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
[root@pluton ssl]# dir
afirma0  bin  crt.pem  demoCA  lib  misc  openssl.cnf.ori  scint3
afirma0.pem  certs  curso  include  man  openssl.cnf  private
[root@pluton ssl]#
```

NOTA: Está clave es muy importante que se guarde en lugar seguro, y se recuerde la palabra de paso con la que se creó.

2. Crear el fichero PKCS#10

Creamos el **fichero de petición de firmado**, PKCS#10, para la CA (Autoridad Certificadora) que en nuestro caso es la FNMT-RCM. Dicha petición de firmado es el fichero de extensión *.csr:

```
openssl req -new -key nombreServidor.pem -out nombreServidor.csr
```

```
Ej: openssl req -new -key afirma0.pem -out afirma0.csr
```

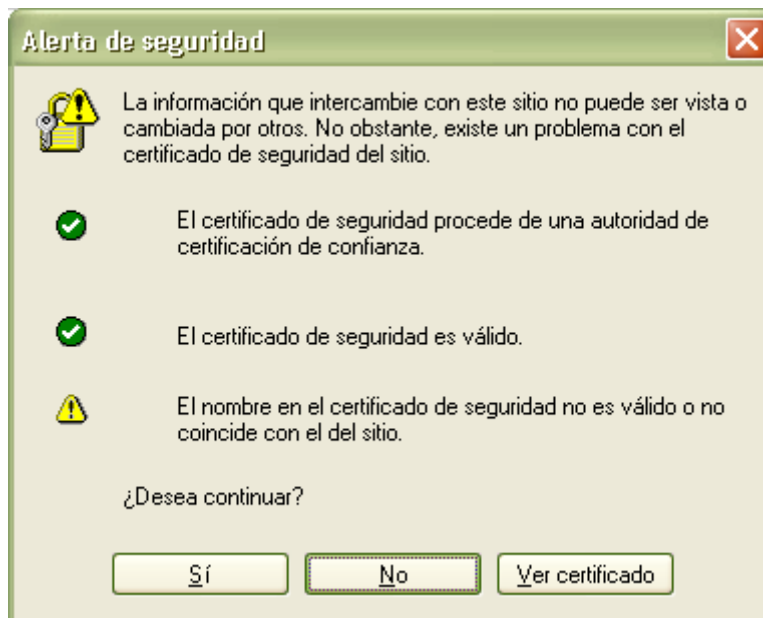
En este paso, se nos pedirá que introduzcamos la información referente al servidor en el certificado, pero en primer lugar, se nos requerirá la palabra de paso de la clave privada:

```
root@pluton:/usr/local/ssl
[root@pluton ssl]# ls -la afirma0.pem
-rw-r--r--  1 root  root   963 Nov 12 13:03 afirma0.pem
[root@pluton ssl]# openssl req -new -key afirma0.pem -out afirma0.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Nombre del pais (Código de 2 letras[ES]) [ES]:ES
Estado o Nombre de la Provincia [Andalucía]:Andalucía
Nombre de la ciudad [Sevilla]:Sevilla
Nombre de la Organización [Junta de Andalucía]:Junta de Andalucía
Nombre de la sección []:SCI - CJ&P
Nombre (p ej.: su nombre o el del servidor) []:ws005.juntadeandalucia.es
Email Address []:administrador@juntadeandalucia.es

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@pluton ssl]#
```

El dato más importante es el nombre del servidor, que debe coincidir con el nombre de DNS de este, sino cuando se establezca una comunicación segura https, saltará una ventana de alerta

de seguridad en el navegador diciendo que el nombre del servidor no coincide con el del sitio web:

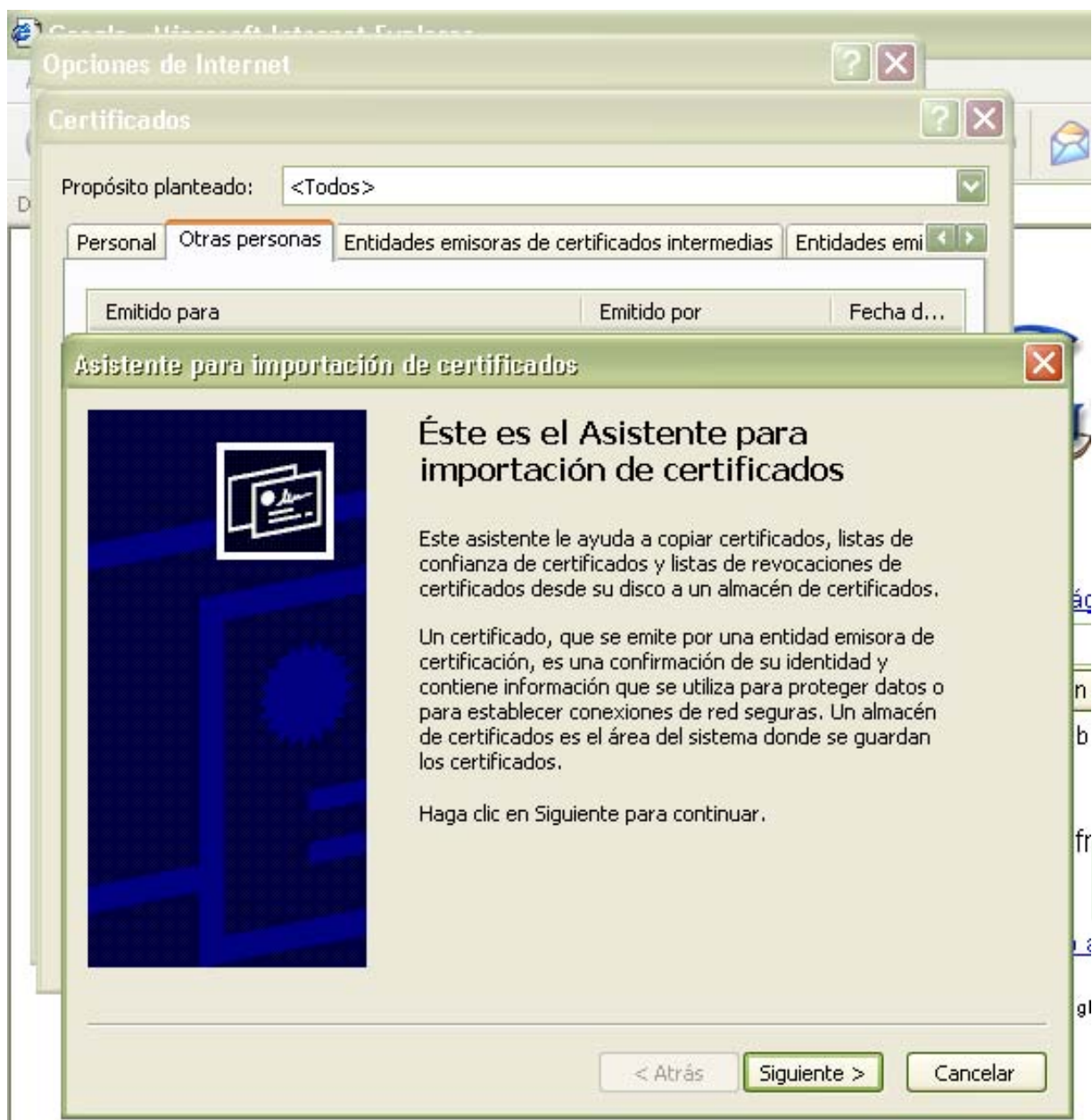


3. Enviar el fichero PKCS#10

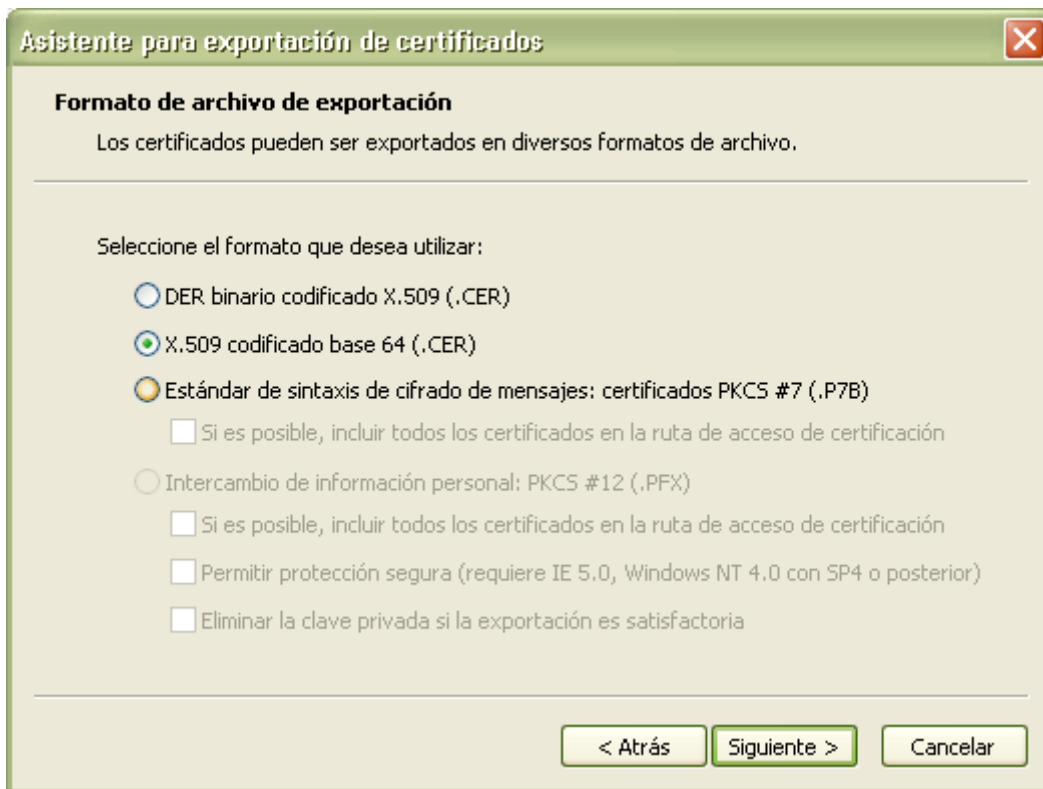
El fichero de petición de firmado, PKCS#10, debe ser enviado a la dirección de correo info.admonelectronica@juntadeandalucia.es junto con el Modelo 003, el formulario de solicitud y la documentación adicional exigida, tal y como se detalla en el **Procedimiento, Solicitud de Certificado de Componente**. Toda la documentación necesaria está disponible en la Web de Administración Electrónica de Plutón, <http://ws024.juntadeandalucia.es>.

4. Generar el fichero PKCS#12

Una vez que la FNMT-RCM remita nuestro certificado firmado, nos devolverá un fichero con extensión *.cer, lo que tenemos que hacer primero es importarlo a un navegador, por ejemplo a Internet Explorer, y meterlo en la sección de certificados de otras personas:



Una vez importado al navegador, es importante que lo exportemos a *.cer, eligiendo el formato "X.509 codificado base 64".



Para finalizar, hay que generar el fichero PKCS#12, esto es, unirlo a la clave privada que generamos en el apartado 1. Para ello:

```
openssl pkcs12 -export -in nombreServidor.cer -inkey  
nombreServidor.pem -out nombreServidor.p12
```

```
Ej: openssl pkcs12 -export -in  
www.juntadeandalucia.es_justiciayadministracionpublica.cer -inkey  
afirma0.pem -out afirma0.p12
```


5. Instalar el certificado en el servidor

Una vez concluidos todos los pasos anteriores , ya tenemos listo el certificado de servidor para instalarlo en el servidor web.

Para ello hay que recurrir a la documentación que facilita el fabricante del software del servidor web.