GUÍA PRÁCTICA

Generación de Certificado de Servidor

Sevilla, Octubre de 2004

Versión 1.0

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

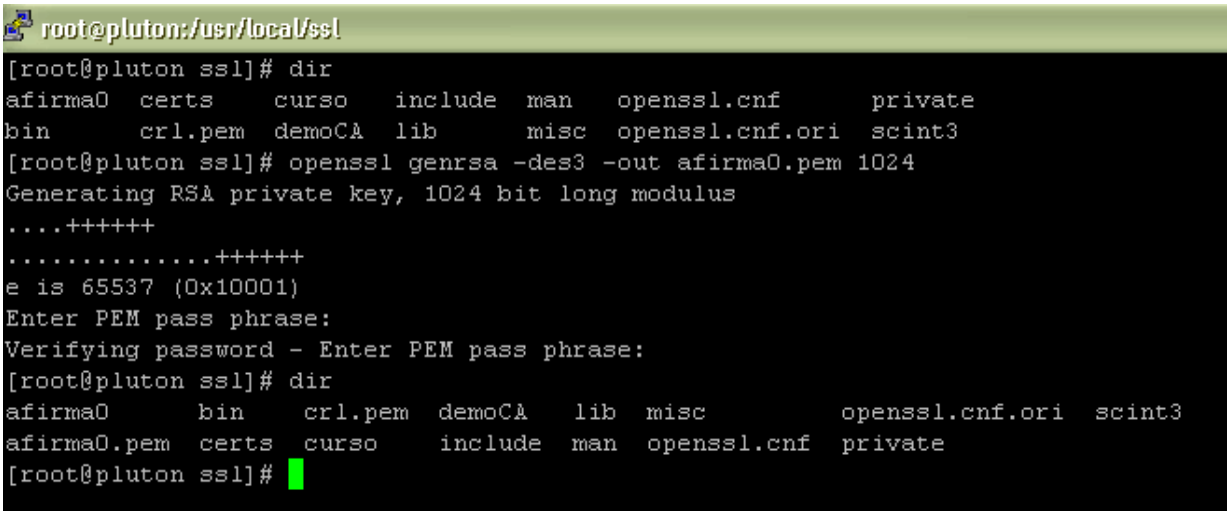
Índice

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***



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

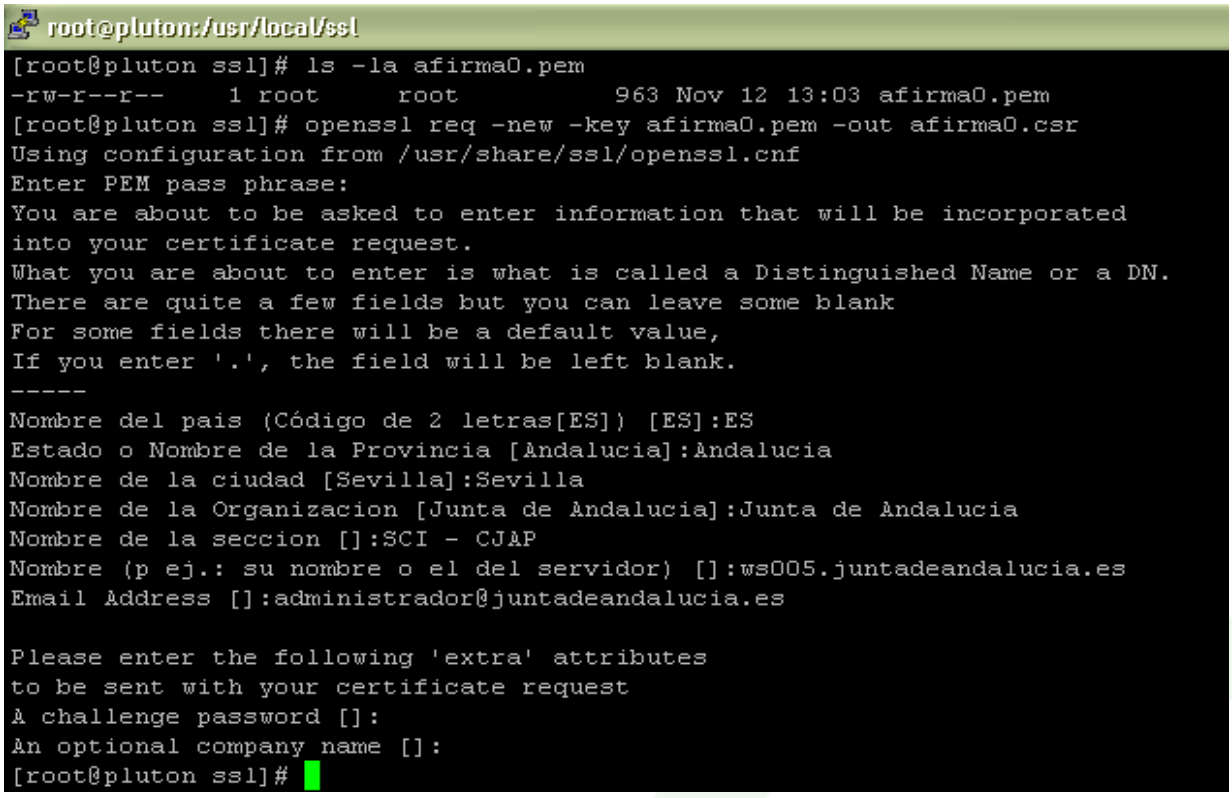
2. Crear el fichero PKCS#10

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

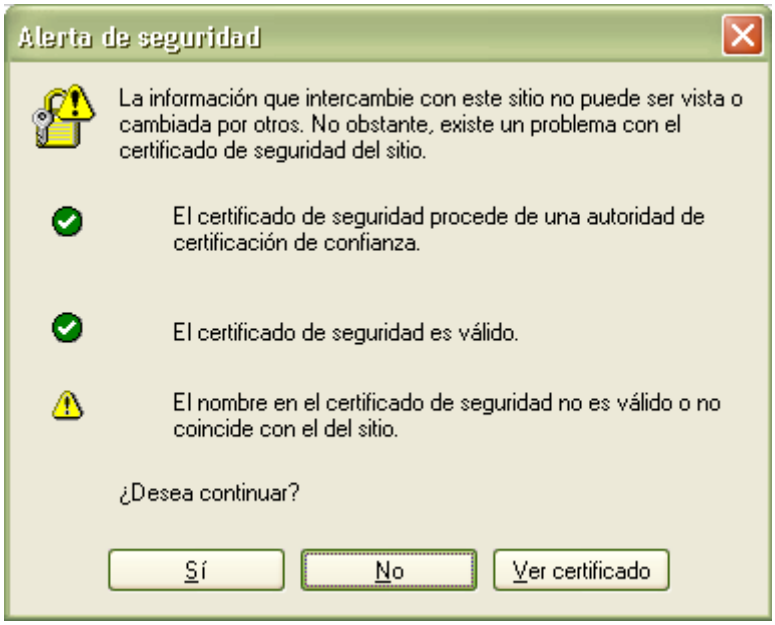
Ej: openssl req –new –key afirma0.pem –out afirma0.csr

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:



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:

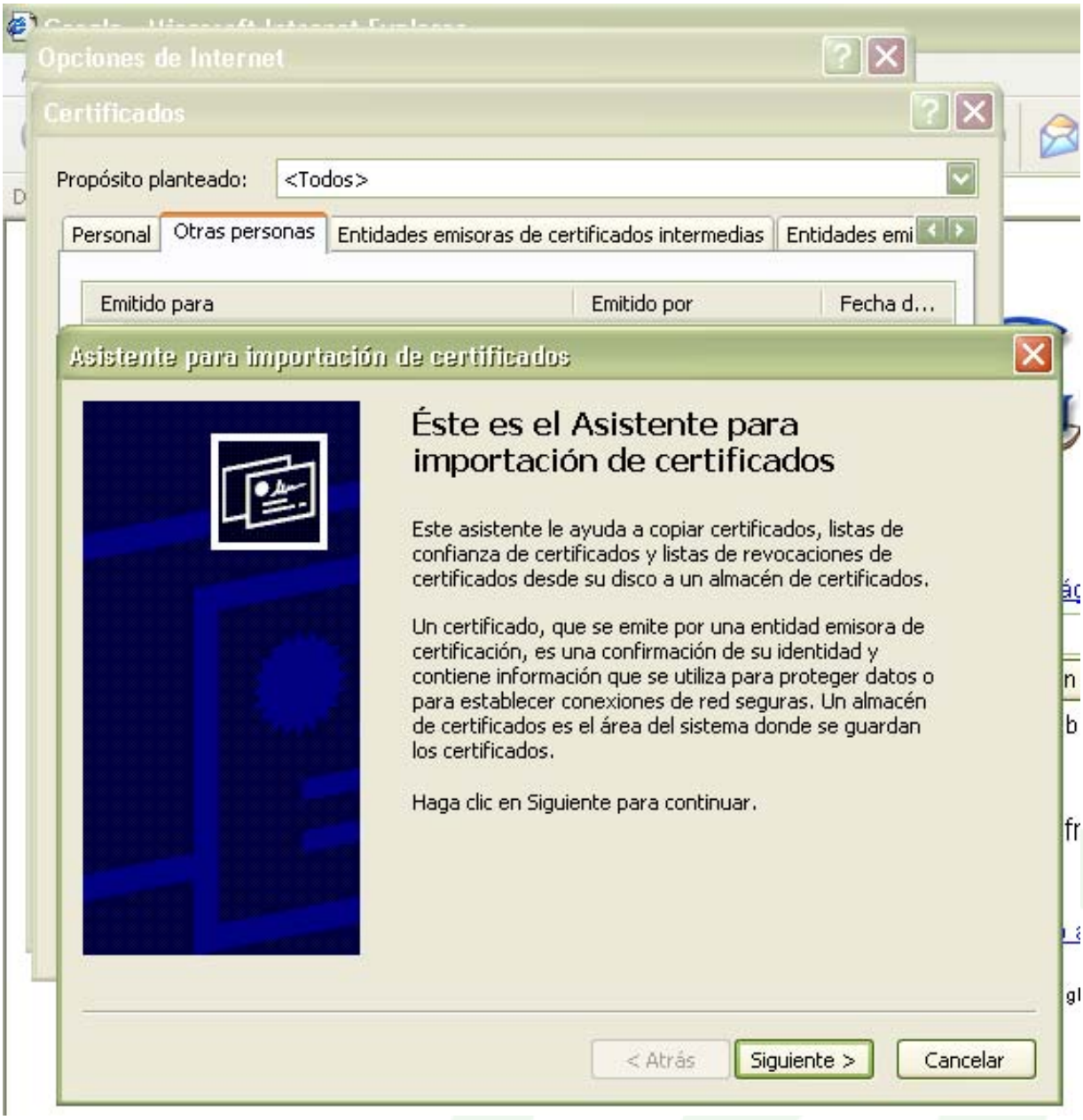


3. Enviar el fichero PKCS#10

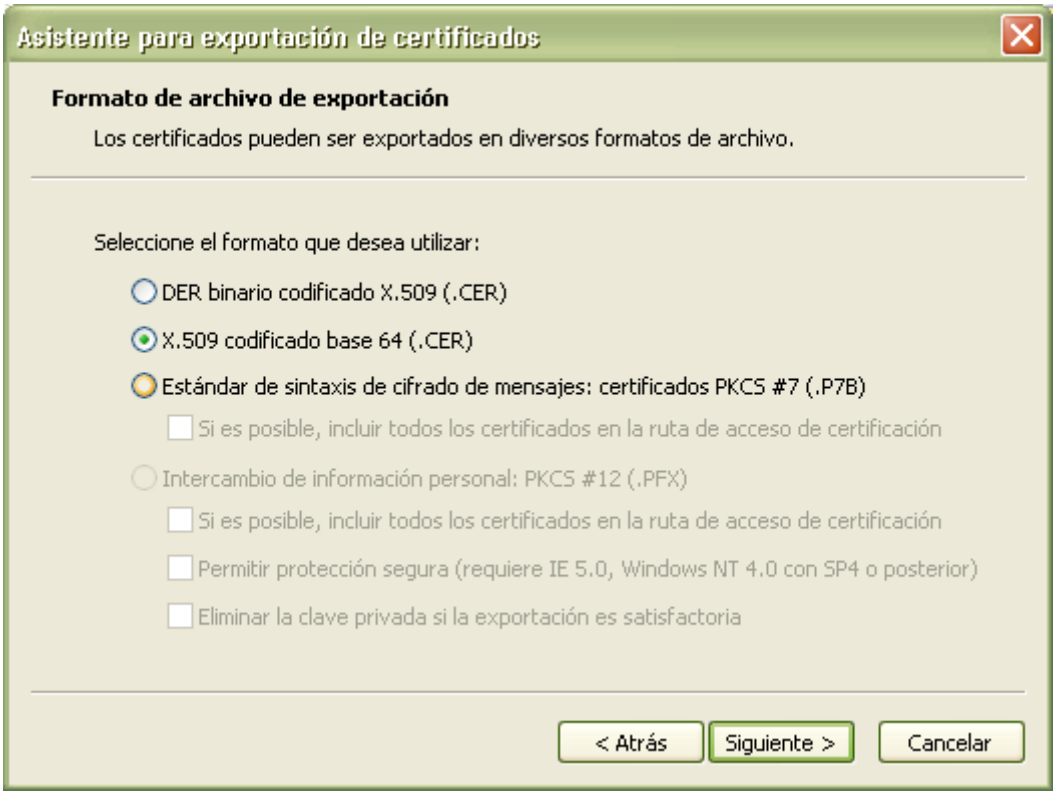
El fichero de petición de firmado, PKCS#10, debe ser enviado a la dirección de correo info.admonelectronica@juntadeandalucia.es junto con el Modelo 003, el formulario de solicitud y la documentación adicional exigida, tal y como se detalla en el **Procedimiento, Solicitud de Certificado de Componente**. 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.