



Agencia de Tecnología y Certificación Electrónica

Petición de certificados de sede y sello con Openssl

Fecha: 15/03/2010	Versión: 1.0
Estado: BORRADOR	Nº de páginas: 7
OID: No asignado	Clasificación: PUBLICO
Archivo: Petición de certificados de sede y sello con Openssl.doc	
Preparado por: José Antonio Amador	

Tabla de Contenido

1. INTRODUCCIÓN.....	3
1.1. OBJETO.....	3
1.2. ÁMBITO Y DEBER DE LECTURA.....	3
1.3. CLASIFICACIÓN.....	3
2. DESARROLLO.....	4
2.1. DESCRIPCIÓN GENERAL.....	4
2.2. GENERACIÓN DE LA PETICIÓN.....	4
3. APÉNDICES.....	7

Cif.: PUBLICO	Ref.: Petición de certificados de sede y sello con Openssl.doc	Versión: 1.0
Est.: APROBADO	OID: No asignado	Pág. 2 de 7

1. Introducción

1.1. Objeto

Descripción de los pasos a seguir para la generación de una petición de certificado de sede y sello con el paquete criptográfico Openssl.

1.2. Ámbito y deber de lectura

El ámbito de este documento es la generación de una petición de certificado de sede y sello con el paquete criptográfico Openssl.

Todos los administradores que deseen obtener un certificado de sede y sello acorde a las Políticas para Certificados Reconocidos de Sede Electrónica y para Certificados Reconocidos de Sello de Órgano , disponible en <http://www.accv.es/administracion-publica/certificados/>.

1.3. Clasificación

La información contenida en este documento se ha clasificado como: **PUBLICO**

2. Desarrollo

2.1. Descripción General

A continuación se detallan los pasos necesarios para la generación de una petición de certificado a partir del paquete criptográfico Openssl.

Se considera que el administrador tiene conocimientos básicos de criptografía así como del manejo de la aplicación Openssl.

El ejecutable openssl debe encontrarse en la ruta del sistema, de lo contrario en los pasos siguientes habría que colocar la ruta completa al ejecutable.

El sistema operativo sobre el que se va a trabajar es Win32, pero todos los comandos y operaciones son inmediatamente trasladables a cualquier sistema soportado por los diversos componentes (Linux, Solaris, Mac OS, etc.), mientras se cumplan los requisitos anteriormente expuestos.

En el caso de utilizar un HSM para la generación de la claves los comandos pueden variar dependiendo del fabricante y de las opciones que proporcione para el ENGINE de OpenSSL.

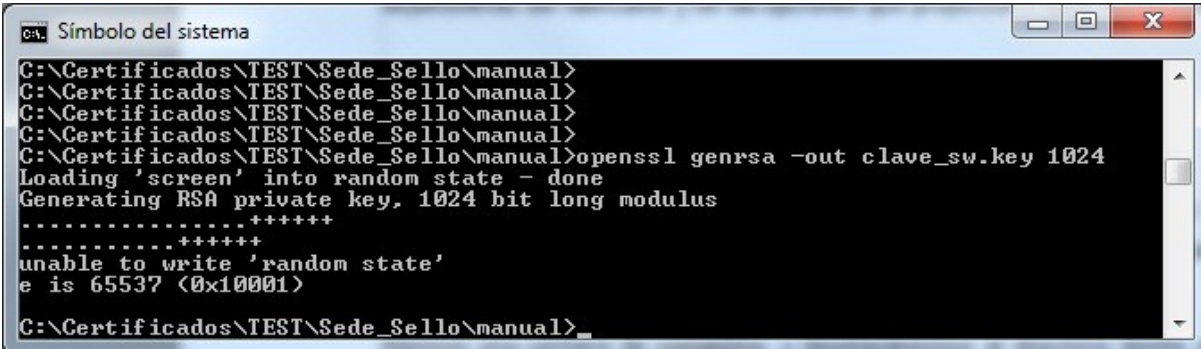
2.2. Generación de la petición

PASO 1: Generación de la clave

El primer paso es la generación de las claves necesarias para el resto de procesos. La única diferencia entre los distintos tipos de certificados es que el tamaño de la clave es de 1024 bits en el caso de certificados software y de 2048 bits en el caso de HSM.

Abrimos una ventana de comandos, y desplazándonos al directorio donde queremos almacenar los distintos elementos y tecleamos:

```
openssl genrsa -out clave_sw.key 1024
```



```
Símbolo del sistema
C:\Certificados\TEST\Sede_Sello>manual>
C:\Certificados\TEST\Sede_Sello>manual>
C:\Certificados\TEST\Sede_Sello>manual>
C:\Certificados\TEST\Sede_Sello>manual>
C:\Certificados\TEST\Sede_Sello>manual>openssl genrsa -out clave_sw.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
unable to write 'random state'
e is 65537 (0x10001)
C:\Certificados\TEST\Sede_Sello>manual>
```

Ilustración 1

Con esta orden, generamos las claves RSA de tamaño 1024 bits, sin encriptación, en el fichero clave_sw.key.

PASO2: Creación de la petición de certificado

En este paso vamos a utilizar los ficheros de configuración de OpenSSL disponibles en la pagina web de la ACCV. Tenemos cuatro ficheros de configuración, uno por tipo de certificado

openssl_sello_hw.cnf

openssl_sello_sw.cnf

openssl_sede_hw.cnf

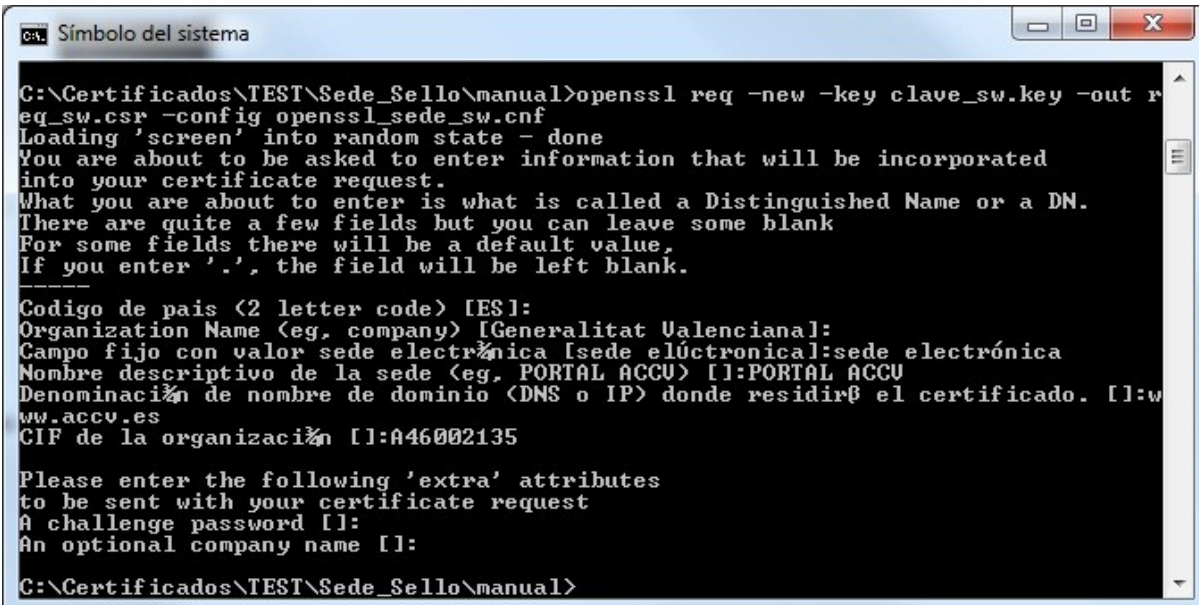
openssl_sede_sw.cnf

Estos ficheros determinan los parámetros que se solicitan en la generación de la petición y se encuentran explicados con mas detalle en los documentos de políticas de certificación correspondientes.

Desde el mismo directorio donde generamos la clave privada, tecleamos:

```
openssl req -new -key clave_sw.key -out req_sw.csr -config <path_a_openssl.cnf>
```

Una vez ejecutada, nos pedirá los datos necesarios para realizar la petición



```
ca. Símbolo del sistema
C:\Certificados\TEST\Sede_Sello>manual>openssl req -new -key clave_sw.key -out req_sw.csr -config openssl_sede_sw.cnf
Loading 'screen' into random state - done
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.
-----
Codigo de pais (2 letter code) [ES]:
Organization Name (eg, company) [Generalitat Valenciana]:
Campo fijo con valor sede electrónica [sede electrónica:sede electrónica
Nombre descriptivo de la sede (eg, PORTAL ACCU) []:PORTAL ACCU
Denominación de nombre de dominio (DNS o IP) donde residirá el certificado. []:ww
ww.accv.es
CIP de la organización []:A46002135

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

C:\Certificados\TEST\Sede_Sello>manual>
```

Ilustración 2

El contenido de ese fichero es el que debemos pegar en el campo "Petición generada (PKCS10)" del NPSC (<https://npsc.accv.es:8450/npsc>).

-----BEGIN CERTIFICATE REQUEST-----

MIIByjCCATMCAQAwwYkxCzAJBgNVBAYTAKVTMR8wHQYDVQQKEExZHZW5lcmFsaXRh
dCBWYWxlbmNpYW5hMRkwFwYDVQLFBBzZWRIIGVsZWN0cGJuaWNhMRQwEgYDVQLL
EwtQT1JUQUwgQUINDVjEUMBIGA1UEAxMLd3d3LmFjY3YuZXMxEjAQBGNVBAUTCUE0
NjAwMjEzNTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAtpH+0DY9WCkYg1F
VI+twe8ojgPXEMI2NjZlZ+DI2sG56qW2vU2urfXPAavuMhioNbwVOeQSasp0OZ32
8FSn8geGdT3bNNBBkuzm+kkNyL7MwIEQ+ubm8nste5g+85wuGbe7NjLI6e/4CCsu
ImPLcUq3BeJi74ovA35iYM5qYsECAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBAJpY
yVgdhZ/nTFfwBR5LkQlgHJQdiagCqd8lbtXlvbaCZ/U5OJTMt2rNjx39FDREWCMQ
vsd277Pb4/WD8SmzH2IL5/2jU1gtNDQ4hjlamchXBYmLiwPIYvwwR7FEto/8v3et
m9OC9FjSSVq8JWPJ1QCKZRnCE4rwBJAo4/4+Eh+Q

-----END CERTIFICATE REQUEST-----

Una vez efectuada la petición y tal como se describe en la política de certificación correspondiente (<http://www.accv.es/quienes-somos/practicas-y-politicas-de-certificacion/>), obtendremos el certificado firmado por la Autoridad de Certificación correspondiente a la petición enviada. Para efectuar dicha petición es necesario disponer de un certificado personal emitido por la Agencia de Tecnología y Certificación Electrónica.

3. Apéndices

No aplicable.