Agencia de Tecnología y Certificación Electrónica

Petición de certificados de servidor con Apache y Openssl

Fecha: 22/03/2014	**Versión:** 2.0
Estado: APROBADO	**Nº de páginas:** 8
OID: 1.3.6.1.4.1.8149.1.1.8.2	**Clasificación: PUBLICO**
Archivo: Petición de certificados de servidor con Apache y Opensslv2.doc	
Preparado por: José Antonio Amador	

Tabla de Contenido

1. Introducción

1.1. Objeto

Descripción de los pasos a seguir para la generación de una petición de certificado de servidor web e instalación de la respuesta utilizando el servidor Apache y 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 servidor web e instalación de la respuesta utilizando el servidor web Apache y el paquete criptográfico Openssl.

Todos los administradores que deseen obtener un certificado de servidor acorde a la Política para Servidores con soporte SSL, disponible en http://www.accv.es/legislacion_c.htm.

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 servidor web Apache y el paquete criptográfico Openssl, así como a la posterior inserción de la respuesta firmada por la Autoridad de Certificación en el servidor.

Se considera que el administrador tiene conocimientos de Apache, y que el servidor tiene el servidor web configurado correctamente. Esto incluye los módulos necesarios de Apache y el paquete criptográfico 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 Win64, 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.

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.

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

openssl genrsa –out apachessl.key 2048

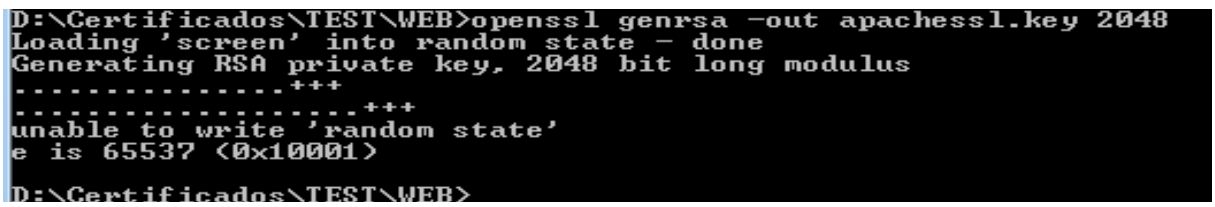


Ilustración 1

Con esta orden, generamos las claves RSA de tamaño 2048 bits, sin encriptación, en el fichero apachessl.key.

PASO2: Creación de la petición de certificado

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

openssl req –new –key apachessl.key –out apachessl.csr –config <path_a_openssl.cnf>

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

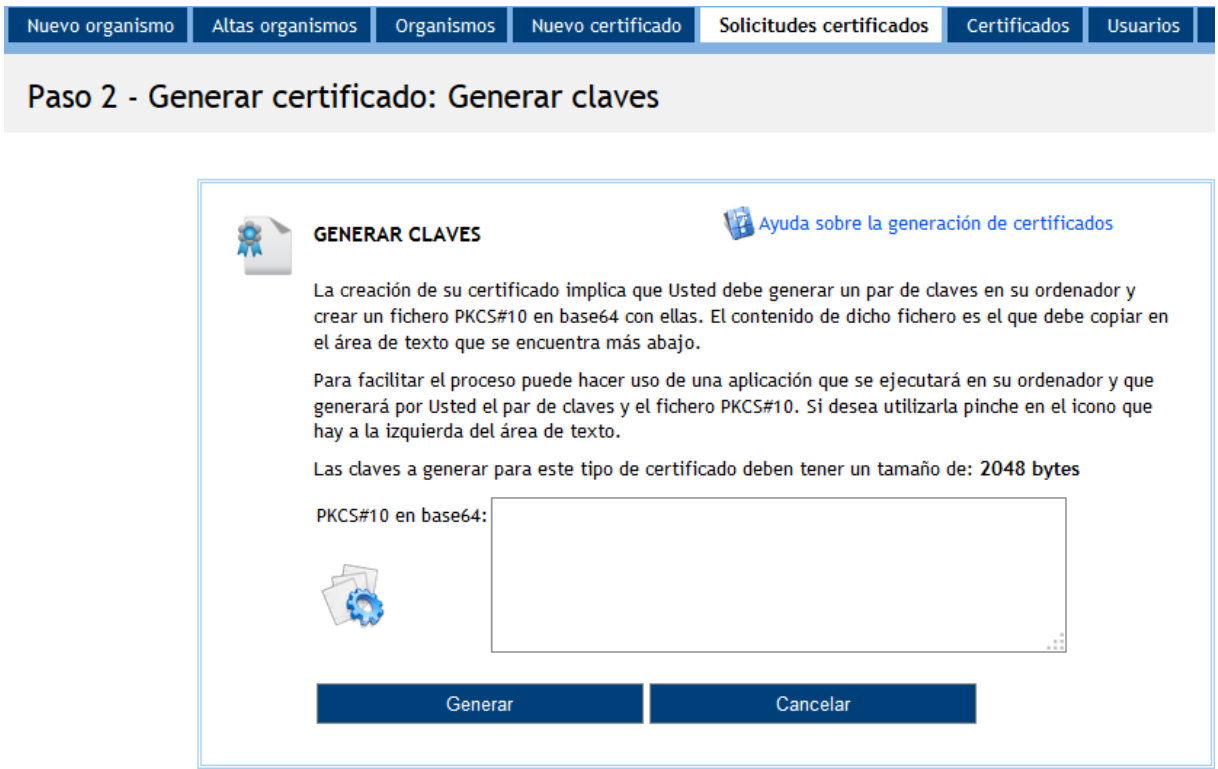
```
C:\certificados>openssl req -new -key apachessl.key -config "\Archivos de progra
ma\GnuWin32\bin\openssl.cnf" -out apachessl.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name 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.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Valencia
Locality Name (eg, city) []:Valencia
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Generalitat Valencian
a
Organizational Unit Name (eg, section) []:Servidores
Common Name (eg, YOUR name) []:www.pki.gva.es
Email Address []:soporte@pki.gva.es

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

C:\certificados>_
```

Ilustración 2

El contenido de ese fichero es el que debemos pegar en el campo “PKCS10 en base64” de la aplicación, en el Paso 2 – Generar certificado: Generar Claves (https://npsc.accv.es:8450/npsc).



Una vez efectuada la petición y tal como se describe en la política de certificación para Servidores con soporte SSL (http://www.accv.es/administracion-publica/certificados/servidor-con-soporte-ssl/), obtendremos el certificado firmado por la Autoridad de Certificación correspondiente a la petición enviada.

Con este certificado, p.ej apachessl.crt, que guardaremos en lugar seguro, debemos efectuar los pasos descritos en el paso 3 (configuración de apache).

ATENCION: Requisitos previos:

Para efectuar la petición es necesario disponer de un certificado de la ACCV (Agencia de Tecnología y Certificación Electrónica) o de un DNIe. Si el soporte del certificado es tarjeta inteligente (en el caso del DNIe siempre lo es) debe estar insertada en el lector y configurada en el equipo.

Para el caso de certificados de la ACCV deben estar instalados en el almacén del navegador los certificados de la CA tal y como se detalla en:

http://www.accv.es/ayuda/manuales-de-instalacion/

y ademas debe realizarse con éxito la comprobación de la firma electrónica en la pagina:

http://www.accv.es/ayuda/comprobacion-de-la-firma-electronica/

Ademas hay que confirmar que el puerto 8450 esta abierto de salida en nuestra organización. En caso contrario debe ponerse en contacto con el departamento responsable de la seguridad para solicitar la apertura del puerto.

PASO 3: Configuración de Apache

Editamos el fichero httpd.conf (o el fichero de configuración correspondiente a la configuración SSL de Apache en nuestro servidor). Nos posicionamos en la definición de "Virtual Host" de SSL (solo se han remarcado las entradas que tienen relación directa con los ficheros generados, el de claves y el de certificado).

```
##
## SSL Virtual Host Context
##

<VirtualHost _default_:443>

#   Server Certificate:
#   Point SSLCertificateFile at a PEM encoded certificate.  If
#   the certificate is encrypted, then you will be prompted for a
#   pass phrase.  Note that a kill -HUP will prompt again. A test
#   certificate can be generated with `make certificate' under
#   built time. Keep in mind that if you've both a RSA and a DSA
#   certificate you can configure both in parallel (to also allow
#   the use of DSA ciphers, etc.)
SSLCertificateFile <ruta_al_fichero_apachessl.crt>

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile <ruta_al_fichero_apachessl.key>
```

Para obtener más información acerca de la configuración de Apache con soporte SSL, se recomienda la lectura de http://www.modssl.org/docs/

Ademas de estas directivas, para un funcionamiento correcto es necesario establecer la directiva SSLCertificateChainFile, que lleva concatenada la cadena de certificación del certificado.

y si se quiere realizar autenticación de cliente, las directivas SSLCACertificateFile y SSLCACertificatePath

3. Apéndices

No aplicable.