



# Autoritat de Certificació de la Comunitat Valenciana

## Petición de certificados de servidor con Apache y Openssl

|                   |                  |
|-------------------|------------------|
| Fecha: 22/03/2006 | Versión: 1.2     |
|                   | Nº de páginas: 8 |



**Secretaria Autònoma de Telecomunicacions i  
Societat de la Informació**  
**Conselleria d'Infraestructures i Transport**



## Tabla de Contenido

|                                      |          |
|--------------------------------------|----------|
| <b>1. DESARROLLO .....</b>           | <b>3</b> |
| 1.1. DESCRIPCIÓN GENERAL .....       | 3        |
| 1.2. GENERACIÓN DE LA PETICIÓN ..... | 3        |
| DN Field .....                       | 5        |
| Explicación .....                    | 5        |
| Ejemplo.....                         | 5        |

|                      |   |              |
|----------------------|---|--------------|
| Clf.: <b>PUBLICO</b> | Ref.: Petición de certificados de servidor con Apache y Openssl.doc | Versión: 1.2 |
| Est.: APROBADO       | OID: 1.3.6.1.4.1.8149.1.1.8.2                                       | Pág. 2 de 8  |

## 1. Desarrollo

### 1.1. 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 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.

### 1.2. 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 1024
```

```
C:\certificados>openssl genrsa -out apachessl.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
C:\certificados>
```

#### Ilustración 1

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

|                      |   |              |
|----------------------|---|--------------|
| Clf.: <b>PUBLICO</b> | Ref.: Petición de certificados de servidor con Apache y Openssl.doc | Versión: 1.2 |
| Est.: APROBADO       | OID: 1.3.6.1.4.1.8149.1.1.8.2                                       | Pág. 3 de 8  |



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 programa\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 Valenciana
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

|                      |   |              |
|----------------------|---|--------------|
| Clf.: <b>PUBLICO</b> | Ref.: Petición de certificados de servidor con Apache y Openssl.doc | Versión: 1.2 |
| Est.: APROBADO       | OID: 1.3.6.1.4.1.8149.1.1.8.2                                       | Pág. 4 de 8  |



A continuación se muestra una explicación breve de los distintos campos:

| DN Field               | Explicación   | Ejemplo  |
|------------------------|---|--|
| Common Name            | El nombre con el que el servidor responde en Internet. Debe ser nombre más dominio. | Si la Web a certificar es https://www.accv.es, entonces el nombre común de la petición debe ser www.accv.es. |
| Organization Name      | El nombre de la organización. <b>Debe ser 'Generalitat Valenciana'</b>              | Generalitat Valenciana   |
| Organization Unit Name | El nombre de la unidad organizativa. <b>Debe ser 'Servidores'</b> .                 | Servidores   |
| City or Locality       | Ciudad. Como se considere (no nulo).  | Valencia   |
| State or Province      | El estado o la provincia. Como se considere (no nulo).                              | Valencia   |
| Country                | La abreviatura de ISO de dos letras para el país. <b>Debe ser 'ES'</b> .            | ES   |

Los atributos extra deben dejarse en blanco.

Esta orden nos genera el archivo apachessl.csr . El contenido de este fichero es el que hay que pegar en la caja de texto asociada de la página web de solicitud de certificado de servidor que se encuentra en:

[https://www.accv.es/html-gestion/solicitud/certservidor\\_c.htm](https://www.accv.es/html-gestion/solicitud/certservidor_c.htm)



\* **Petición generada por el servidor:**



**Ilustración 3**

|                      |   |              |
|----------------------|---|--------------|
| Cif.: <b>PUBLICO</b> | Ref.: Petición de certificados de servidor con Apache y Openssl.doc | Versión: 1.2 |
| Est.: APROBADO       | OID: 1.3.6.1.4.1.8149.1.1.8.2                                       | Pág. 6 de 8  |



Una vez efectuada la petición y tal como se describe en la política de certificación para Servidores con soporte SSL ([https://www.accv.es/legislacion\\_c.htm](https://www.accv.es/legislacion_c.htm)), 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 Autoridad de Certificación de la Generalitat Valenciana.

Con este certificado, p.ej apachessl.crt, que guardaremos en lugar seguro, debemos efectuar los pasos siguientes.

|                      |   |              |
|----------------------|---|--------------|
| Clf.: <b>PUBLICO</b> | Ref.: Petición de certificados de servidor con Apache y Openssl.doc | Versión: 1.2 |
| Est.: APROBADO       | OID: 1.3.6.1.4.1.8149.1.1.8.2                                       | Pág. 7 de 8  |



### 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/>

|                      |   |              |
|----------------------|---|--------------|
| Clf.: <b>PUBLICO</b> | Ref.: Petición de certificados de servidor con Apache y Openssl.doc | Versión: 1.2 |
| Est.: APROBADO       | OID: 1.3.6.1.4.1.8149.1.1.8.2                                       | Pág. 8 de 8  |