# SOLICITUD Y EMISIÓN DE CERTIFICADOS Y CONFIGURACIÓN DE APACHE COMO SERVIDOR SEGURO

## Descripción

En esta práctica aprenderemos a crear una autoridad certificadora, cómo crear solicitudes de certificados digitales de servidor y cliente, cómo firmar esos certificados y emitirlos, cómo configurar Apache como servidor seguro y la gestión de los certificados en los navegadores Web.

## 1. Creación de una solicitud de certificado digital

Para conseguir que nuestro servidor Web albergue un sitio seguro (HTTPS) se necesita obtener un certificado digital. Mediante OpenSSL nosotros podremos crear una solicitud de certificado digital.

Crearemos una nueva carpeta en /etc/apache2/ llamada SSL donde guardaremos todos los documentos de certificados y claves privadas generadas y desde donde ejecutaremos todos los comandos necesarios.

**Creación de la clave privada del certificado:**
/usr/local/ssl/install/bin/openssl genrsa -des3 -out clavecert.pem -passout pass:alfonso 2048

**Creación de la solicitud del certificado:**
/usr/local/ssl/install/bin/openssl req -new -key clavecert.pem -passin pass:alfonso -out SolicitudCertificado.pem

En el proceso de creación de la solicitud se pedirán datos de identificación de la empresa u organización que utilizará el certificado digital. Se debe prestar atención en la solicitud del *Common Name,* ya que en en este dato se almacenara el nombre del sitio seguro.

## 2. Creación de una Autoridad Certificadora y emisión del certificado

Para la generación del certificado digital es necesario que una autoridad certificadora firme nuestra solicitud de certificado verificando los datos de la empresa y emitiendo el certificado final.

**Creación de la autoridad certificadora**
/usr/local/ssl/install/bin/openssl req -x509 -newkey rsa:2048 -keyout ClavePrivadaCA.pem -days 3650 -out CertificadoCA.pem -passout pass:alfonsoca

**Firma y emisión de nuestra solicitud de certificado:**
Para la firma del certificado es necesario crear un archivo de configuración que llamaremos *CertServerConf* donde se especifican los siguientes parámetros de configuración:

```
basicConstraints = critical,CA:FALSE
extendedKeyUsage = serverAuth
```

/usr/local/ssl/install/bin/openssl x509 -CA CertificadoCA.pem -CAkey ClavePrivadaCA.pem -req -in SolicitudCertificado.pem -days 3650 -extfile CertServerConf -sha1 -CAcreateserial -out Certificado.pem

## 3. Configuración de Apache como servidor seguro

Para la configuración de Apache como servidor seguro debemos modificar el fichero de configuración ssl.conf situado en /etc/apache2/conf/

```
NameVirtualHost *:443
<VirtualHost *:443>
ServerAdmin webmaster@localhost
DocumentRoot /home/alfonso/mipagina
ServerName localhost
SSLCertificateFile ssl/certificados/cert/Certificado.pem
SSLCertificateKeyFile ssl/certificados/claves/clavecert.pem
```

**Con estas directivas configuraremos lo siguiente:**

El sitio seguro debe ser un servidor virtual, por lo tanto crearemos un servidor virtual que estará escuchando por el puerto 443 (Puerto por defecto de HTTPS) cuyo documento raíz estará definido en *DocumentRoot* y cuyo nombre del servidor estará definido en *ServerName.*

Para arrancar el sitio seguro, Apache debe saber donde se ubican el certificado del sitio y su clave privada, estas rutas las definiremos en *SSLCertificateFile* y *SSLCertificateKeyFile.*

Una vez configurado Apache, lo arrancamos con SSL en /etc/apache2/bin/ mediante:

*#:> ./apachectl startssl*

## 4. Creación de una solicitud de certificado digital de cliente

Para conseguir un nivel más de seguridad a la hora de acceder a nuestro sitio seguro, podemos obligar al cliente a que tenga un certificado digital para poder acceder a nuestro sitio seguro.

**Creación de la clave privada del certificado:**

```
/usr/local/ssl/install/bin/openssl genrsa -des3 -out clavecertCliente.pem -passout
pass:alfonsocli 2048
```

**Creación de la solicitud del certificado:**

```
/usr/local/ssl/install/bin/openssl req -new -key clavecertCliente.pem -passin pass:alfonsocli
-out SolicitudCertificadoCliente.pem
```

En el proceso de creación de la solicitud se pedirá datos de identificación del certificado de cliente.

## 5. Emisión del certificado y configurar apache para solicitar certificado de cliente

**Firma y emisión de nuestra solicitud de certificado de cliente:**

Para la firmar del certificado es necesario crear un archivo de configuración que llamaremos *CertClientConf* donde se especifican los siguientes parámetros de configuración:

```
basicConstraints = critical,CA:FALSE
extendedKeyUsage = clientAuth
```

/usr/local/ssl/install/bin/openssl x509 -CA CertificadoCA.pem -CAkey ClavePrivadaCA.pem -req -in SolicitudCertificadoCliente.pem -days 3650 -extfile CertClientConf -sha1 -CAcreateserial -out CertificadoCliente.pem

**Conversión a formato pkcs12**

Para que los navegadores clientes puedan importar el certificado de cliente y poder acceder al sitio seguro debemos de convertir el certificado a un formato pkcs12.

/usr/local/ssl/install/bin/openssl pkcs12 -export -in CertificadoCliente.pem -inkey / clavecertCliente.pem -certfile CertificadoCA.pem -out CertificadoCliente.p12 -passin pass:alfonsocli -passout pass:alfonsocli

**Configurar apache para requerir certificado cliente**

Debemos añadir estas dos lineas nuevas en nuestro servidor virtual, que indican la ruta donde se encuentra el certificado de la CA *SSLCACertificateFile* y que se requiere certificado por parte cliente *SSLVerifyClient require.*

```
SSLCACertificateFile ssl/CA/CertificadoCA.pem
SSLVerifyClient require
```

**Configuración del navegador Web**

Para acceder al sitio seguro es necesario que el navegador Web tenga el certificado de cliente, por lo tanto se deberá importar el paquete pkcs12 como certificado en la sección de certificados de cliente del navegador en cuestión.