SSL en Apache con certificado autofirmado (/despliegue-de-aplicaciones-web/81-administracion-de-servidores-web/292-ssl-en-apache-con-certificado-autofirmado)

Generación del certificado autofirmado

El conjunto de **herramientas *openssl* (http://www.openssl.org/)** ofrece todo un conjunto de funciones para el manejo de comunicaciones a través de SSL. Entre otros servicios ofrece la posibilidad de crear certificados SSL autofirmados. La utilidad openssl se instala junto con el servidor web Apache. Si la instalación se está realizando en Windows, se ha debido elegir la descarga del servidor web Apache que incluye openSSL (*Win32 Binary* ***including OpenSSL*** *0.9.8o*).

La **ejecución de *openssl*** se hace **desde el símbolo del sistema o el terminal**. En **Ubuntu**, se puede hacer **directamente la llamada** desde cualquier carpeta, pero en **Windows** hay que tener en cuenta que el ejecutable se encuentra en la **carpeta *bin*** en la ubicación donde se haya instalado el servidor web. Por tanto, para ejecutar *openssl* desde Windows, debes indicar delante la ruta donde se encuentra la utilidad, o bien, añadir la ruta a la carpeta *bin* en la variable PATH del sistema. En Windows además se debe indicar la **ruta al archivo de configuración *openssl.cnf***, lo cual puedes hacer indicando, durante la generación del certificado, la opción *-config* seguida de la ruta a dicho archivo, o bien establecer (usando el comando *SET*) la variable de sistema ***OPENSSL_CONF=C:\ruta\instalacion\Apache\conf\openssl.cnf***. El archivo openssl.cnf se encuentra en la carpeta de configuración donde se haya instalado el servidor web. Por ejemplo, en la versión 2.2 se encuentra en *C:\Program Files\Apache Software Foundation\Apache2.2\conf\openssl.cnf*.

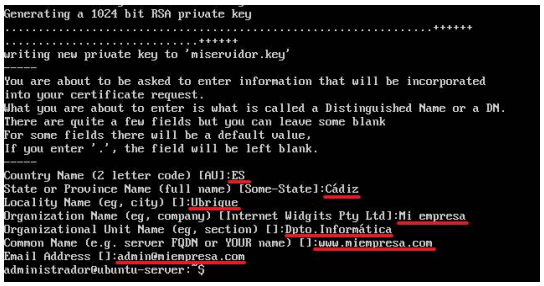
La generación de certificados se realiza mediante la **utilidad *req* (http://www.openssl.org/docs/apps/req.html)** que está incluida dentro de la herramienta *openssl*. En concreto, para generar un certificado autofirmado puedes usar los siguientes parámetros:

```
openssl req -new -x509 -nodes -days 365 -keyout archivoClavePrivada.key -out archivoCertificado.crt
```

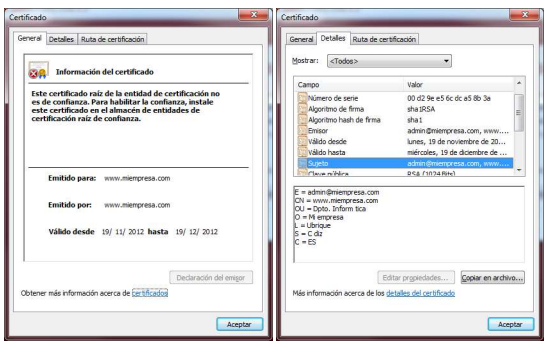
El significado de cada opción indicada en el siguiente:

- **-new**: genera una petición de certificado.
- **-x509**: indica que va a ser un certificado autofirmado.
- **-nodes**: evita que se solicite una contraseña al usuario para generar la clave privada. Si no se indica esta opción, hay que introducir una contraseña que se utiliza para encriptar la clave privada y hay que configurar el servidor web para que se le proporcione la misma contraseña de la clave privada.
- **-days n**: permite especificar el número de días (n) de vigencia del certificado. En el ejemplo se ha indicado que el certificado caducará dentro de 1 año. Si no se especifica esta opción se obtiene un certificado con 1 mes de validez.
- **-keyout *nombreArchivo***: permite especificar el nombre del archivo en el que se va a almacenar la clave privada. Si no se indica esta opción, se guarda en un archivo llamado *privkey.pem*.
- **-out *nombreArchivo***: permite indicar el nombre del archivo que va a almacenar el certificado. Si no se especifica, se mostrará en pantalla.

Al ejecutar la orden anterior, se solicitará una serie de **datos que se almacenarán en el certificado** y podrán ser consultados por las personas que visiten las páginas del servidor. El dato más importante es el ***Common Name***, donde conviene indicar el nombre de dominio de nuestro servidor.



Esos datos del certificado se verán de la siguiente manera en el navedor web *Chrome* al hacer clic en la zona *https* de la barra de direcciones:



Activación del módulo SSL

Para que el servidor web Apache pueda utilizar la capa SSL en sus comunicaciones, es necesario activar el módulo correspondiente.

En ***Ubuntu*** debes guardar enlaces simbólicos en la carpeta */etc/apache2/mods-enabled* que enlacen con los archivos *ssl.conf* y *ssl.load* que se encuentran en la carpeta */etc/apache2/mods-available/*. Puedes hacerlo con la siguiente instrucción:

```
sudo ln -s /etc/apache2/mods-available/ssl* /etc/apache2/mods-enabled
```

A partir de Apache 2.4 también hay que **activar el módulo *socache_shmcb***:

```
 ln -s /etc/apache2/mods-available/socache_shmcb.load /etc/apache2/mods-enabled/.
```

En caso de que se esté configurando el servidor en **Windows** debes descomentar la siguiente línea del archivo de configuración:

```
#LoadModule ssl_module modules/mod_ssl.so
```

Permitir escuchar por el puerto 443

El protocolo HTTPS que utiliza la capa SSL utiliza el puerto de comunicaciones 443 por defecto, por lo que hay que configurar el servidor web para que admita las comunicaciones por ese puerto.

En **Ubuntu**, el archivo *ports.conf*, contiene la línea necesaria para ello si se ha activado el módulo SSL, por lo que no hay que hacer nada más.

En **Windows**, la versión 2.2 de Apache incluye el archivo conf/extra/httpd-ssl.conf con la estructura básica para configurar este tipo de comunicación. Pero si deseas hacer una configuración más sencilla, puedes incluir la línea de escucha del puerto directamente en el archivo de configuración *httpd.conf*.

```
Listen 443
```

Servidor virtual seguro

Usando la directiva *VirtualHost* debes crear un servidor virtual que utilice el puerto 443. Dentro de la configuración de esta directiva debes indicar las líneas necesarias para **activar SSL** e indicar las **rutas a los archivos** que contienen la **clave privada y el certificado**.

```
<VirtualHost *:443>
    DocumentRoot /ruta/a/sitio-seguro

    SSLEngine on
    SSLCertificateFile /ruta/a/archivoCertificado.crt
    SSLCertificateKeyFile /ruta/a/archivoClavePrivada.key

    <Directory /ruta/a/sitio-seguro>
        Order allow,deny
        allow from all
    </Directory>

</VirtualHost>
```

Acceso al sitio web seguro

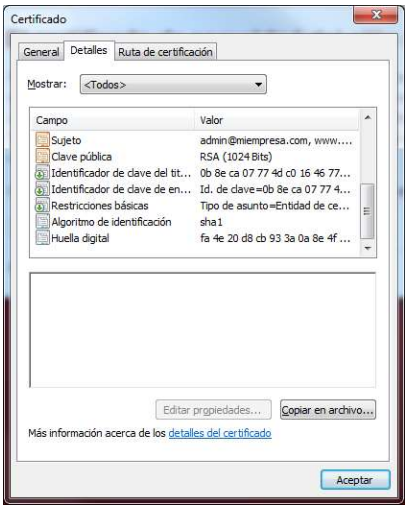
Una vez finalizada la configuración y reiniciado el servidor web, puedes acceder al sitio web seguro que has configurado indicando en la barra de direcciones del navegador web el protocolo HTTPS antes de la dirección del servidor (***https://****mi.servidor.com*).

Ya que estamos usando un certificado autofirmado, el navegador mostrará un **aviso** indicando que el sitio al que estamos accediendo **no ha sido registrado por ninguna autoridad como un sitio de confianza**. Para terminar de acceder a la web, puedes usar el botón *Continuar de todos modos* o el botón equivalente según el navegador web que utilices.

Si deseas que no vuelva a aparecer en ningún momento este aviso, debes añadir tu certificado a la **lista de entidades de certificación de confianza** del navegador.

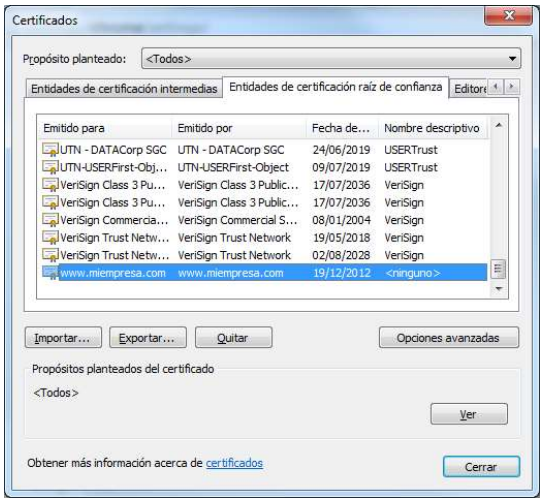
Desde el mismo navegador que están intentando cargar la web puedes guardar el archivo que contiene el certificado, usando el enlace de *Datos del certificado*.

En la **pestaña *Detalles*** puedes encontrar el botón *Copiar en archivo* que abrirá un asistente donde indicarás el nombre que deseas darle al archivo.



Una vez que tengas almacenado el certificado debes **importarlo al navegador**. En Chrome puedes hacerlo desde su **configuración**, mostrando la sección ***Mostrar opciones avanzadas***, donde encontrarás el botón ***Administrar certificados***.

En la pestaña ***Entidades de certificación de raíz de confianza***, utiliza el botón ***Importar*** para que aparezca el asistente que te pedirá el archivo que contiene el certificado. Tras añadirlo, comprueba que aparece en la lista el certificado correspondiente al dominio que estás utilizando.



Recuerda que para que no aparezca el aviso de que el sitio no es de confianza, debes **acceder a él usando el mismo nombre de dominio** que has registrado en el certificado. Si usas la dirección IP continuarás viendo el mismo mensaje. Ten en cuenta además que puede ser necesario **reiniciar el navegador** para que tenga efecto.

Detalles

Categoría: Administración de servidores web (/despliegue-de-aplicaciones-web/81-administracion-de-servidores-web)
Publicado: 19 Noviembre 2012
Última actualización: 16 Febrero 2017
Visto: 14226