SSL es… una manera de crear un *tunel* entre el servidor web y tu ordenador. Mediante un certificado de encriptación que debe estar firmado por el servidor alguien en quien TU confías

**fuente:** http://en.juantxu.net/doku.php/ssl

(debemos tener instalado el paquete openssl instalado, disculpad la ortografía, el artículo ha sido copiado integramente de la fuente)

Vamos a empezar. Lo primero es general la LLAVE PRIVADA del servidor. Esto se hace mediante la generacion aleatoria de una cadena de texto. El modo simple es este:

```
openssl genrsa -des3 -out server.key 1024
```

O si eres un loco con manía persecutoria puedes indicarle el nombre de tantos archivos como quieras para que genere la secuencia aleatoria en base a esos archivos. Pueden ser archivos de texto, archivos comprimidos y creo que tambien gráficos, pero esto último no estoy muy seguro.

```
openssl genrsa -des3 -rand file1:file2:file3:file4:file5 -out server.key 1024
```

donde file1:file5 son esos archivos

El sistema te pedirá una contraseña…. **¡RECUERDALA!** Pos ala! ya tenemos nuestra llave privada. El caso es que el sistema te la pedriá siempre. Pero… que pasa cuando actualizas apache
y se reinicia? pues que te pide la clave y si se reinicia automaticamente… pues no arranca hasta que algun pringao va y mete la contraseña. No es aconsejable a nivel de seguridad. pero si a nivel de practicidad. Puedes deshabilitar el hecho de que te pida simpre la clave con este comando:

```
openssl rsa -in server.key -out server.pem
```

Por último vamos a generar el archivo csr.

```
openssl req -new -key server.key -out server.csr
```

Aqui te hará una serie de preguntas..

Enter pass phrase for server.key: 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]:Catalunya Locality Name (eg, city) []:Barcelona Organization Name (eg, company) [Internet Widgits Pty Ltd]:juantxu.net Organizational Unit Name (eg, section) []:juantxu.net Common Name (eg, YOUR name) []:juantxu.net Email Address []:juantxu@juantxu.net Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []: una cualquiera... An optional company name []:juantxu.net

De este modo la clave no requiere de la contraseña.

Una vez que ya tenemos esto hecho… ya podemos emitir certificados para nuestro sitio. Vamos a generar un certificado auto-firmado. Se puede hacer un certificado que será firmado por una entidad de confianza. Osea, como un notario de internet. Y que cobra como un notario real.

openssl x509 -req -days 60 -in server.csr -signkey server.key -out server.crt

Te pedirá la clave… la general…

Signature ok
subject=/C=ES/ST=Catalunya/L=Barcelona/O=juantxu.net/OU=juantxu.net/CN=juantxu.net/emailAddress=juantxu@juantxu.net Getting Private key Enter pass phrase for server.key:

pues ya tenemos nuestra certificado. ahora vamos a usarlo!!!

NameVirtualHost *:443 ServerAdmin webmaster@localhost DocumentRoot /var/local/mipagina SSLEngine on SSLCertificateFile /etc/apache2/ssl/server.crt SSLCertificateKeyFile /etc/apache2/
ssl
/server.pem ServerName mipagina.midominio.com Options Indexes FollowSymLinks MultiViews AllowOverride None Order allow,deny allow from all