

# certificados de seguridad

## conceptos

- .key → fichero conteniendo clave privada de un certificado
- .csr → fichero de petición para certificar por una entidad certificadora → Certificate Signing Request
- .crt → fichero firmado por la entidad certificadora, para instalar en el webserver

## creacion

1. generar la clave privada:

```
openssl genrsa -des3 -out fichero.key 2048
```

- quitar la opción -des3 para generarla sin contraseña

2. generar el .csr:

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

- country: ES
- State: Madrid
- Locality: Madrid
- Organization: Mate, SL
- Organization Unit: ITs
- Common Name: host.dominio.com
- Email Address: email
- VIGILAR QUE LOS DATOS DE DOMINIO Y CERTIFICADO COINCIDAN Y QUE TENGAMOS ACCESO AL CORREO Y TELÉFONO QUE CONSTAN

3. autofirmar el .csr para obtener el .crt (o enviar a un agente certificador reconocido) :

```
openssl x509 -req -days 365 -in fichero.csr -signkey fichero.key -out fichero.crt
```

- en este caso, es para 1 año (365 days)

4. Ejemplo de configuración apache:

```
<VirtualHost xxx.xxx.xxx.xxx:443>
    ServerAdmin hostmaster@domain.none
    ServerName secure.domain.none

    SSLEngine on
    SSLProtocol all -SSLv2
    SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW
    SSLCertificateFile /etc/httpd/certs/x.cer
    SSLCertificateKeyFile /etc/httpd/certs/x.key
    SSLCACertificateFile /etc/httpd/certs/xAuth.cer

    DocumentRoot /home/www/secure.domain.none/
    <Directory /home/www/secure.domain.none/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
```

```
    allow from all
</Directory>

ErrorLog /var/log/httpd/secure.domain.none.errors.log
CustomLog /var/log/httpd/secure.domain.none.access.log combined

# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
LogLevel debug

ServerSignature Off
</VirtualHost>
```

<http://www.thegeekstuff.com/2009/07/linux-apache-mod-ssl-generate-key-csr-crt-file/>

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/linux:certificados:start?rev=1323124360>

Last update: **05/12/2011 14:32**

