

# 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
```

1. quitar la opción -des3 para generarla sin contraseña
2. generar el .csr:

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

1. country: ES
  2. State: Madrid
  3. Locality: Madrid
  4. Organization: Mate, SL
  5. Organization Unit: ITs
  6. Common Name: host.dominio.com
  7. Email Address: email
3. autofirmar el .csr:

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

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

```
<VirtualHost 62.97.72.24:443>
    ServerAdmin mailerdaemon@eone.es
    ServerName www.spain.volvo-online.net

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

    DocumentRoot /home/www/bree.eurorscg.es/
    <Directory /home/www/bree.eurorscg.es/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>
```

```
ErrorLog /var/log/httpd/x.errors.log
CustomLog /var/log/httpd/x.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=1322392175>

Last update: **27/11/2011 03:09**

