

# Crear certificado privado SSL + root CA

Crear certificado autofirmado con openssl para servidores de pruebas con HTTPS, certificados para tablets, etc.

## domain.ext

```
authorityKeyIdentifier=keyid,issuer  
basicConstraints=CA:FALSE  
subjectAltName = @alt_names  
[alt_names]  
DNS.1 = domain  
DNS.2 = *.domain
```

## Create Private Key and Signing Request (csr)

```
openssl req -newkey rsa:2048 -nodes -keyout domain.key -out domain.csr
```

## Certificate

```
openssl x509 -req -CA rootCA.crt -CAkey rootCA.key -in domain.csr -out  
domain.crt -days 365 -CAcreateserial -extfile domain.ext
```

## Crear nuevo root CA

```
openssl req -x509 -sha256 -days 1825 -newkey rsa:2048 -keyout rootCA.key -out  
rootCA.crt
```