# 1 Autoridade certificadora

Se os servizos da rede non requiren un número considerable de certificados, o mellor é crear unha *autoridade certificadora* (CA) propia para uso interno da nosa organización.

O uso de certificados asinados pola propia CA, permite que varios servizos que usan certificados confien en certificados emitidos pola CA.

O proceso para ter unha CA é o seguinte:

1. Creamos o directorio onde se garda o certificado da CA e ficheiros relacionados:
```
mkdir /etc/ssl/CA
mkdir /etc/ssl/newcerts
```

2. A CA necesita uns ficheiros adicionais: Un deles para gardar o último numero de serie utilizado pola CA, xa que cada certificado debe ter un número de serie único, e outro ficheiro para rexistrar os certificados emitidos:
```
sh -c "echo '01' > /etc/ssl/CA/serial"
touch /etc/ssl/CA/index.txt
```

3. Editamos o ficheiro de configuración da CA. Edita o ficheiro */etc/ssl/openssl.cnf*, e na sección *[ CA_default ]* cambia:
```
dir             = /etc/ssl/             # Onde se garda o certificado
database        = $dir/CA/index.txt     # Ficheiro da base de datos da relación certificados.
certificate     = $dir/certs/cacert.pem # O certificado da CA
serial          = $dir/CA/serial        # O numero de serie actual
private_key     = $dir/private/cakey.pem# A chave privada
```

4. Creamos o certificado raíz da CA autoasinado:
```
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650
```

   Haberá que responder aos detalles da creación do certificado. Os datos que introduzamos en pais, localidade, organización deben ser os mesmos que os dos certificados que vai asinar. Non se poden asinar certificados con datos diferentes.
5. Instalación do certificado raíz e da chave:
```
mv cakey.pem /etc/ssl/private/
mv cacert.pem /etc/ssl/certs/
```

Se queremos comprobar os datos do certificado, tecleamos:

```
openssl x509 -in /etc/ssl/certs/cacert.pem -text -noout
```

Desde este momento xa se poderían emitir certificados dixitais por parte da CA. Os pasos para emitilos son os seguintes:

1. Primeiro creamos unha chave privada no equipo onde se vai a empregar:
```
openssl genrsa -des3 -out server.key 2048
#Se queremos que non nos pregunte o contrasinal, podemos introducilo coa opción -passout
#openssl genrsa -des3 -out server.key  -passout pass:abc123. 2048
```

2. Agora creamos unha chave insegura:
```
openssl rsa -in server.key -out server.key.insecure
#Se queremos que non nos pregunte o contrasinal, introducímolo coa opción -passin
#openssl rsa -in server.key -out server.key.insecure -passin pass:abc123.
mv server.key server.key.secure
mv server.key.insecure server.key
```

3. A chave insegura, agora chámase *server.key* e usaremola para crear a solicitide (ficheiro .csr) que logo asinará a CA:
```
openssl req -new -key server.key -out server.csr
```

   Preguntará tamén por nome da organización, nome do sitio, .... Estes mesmos datos volveran a ser preguntados a hora de emitir o certificado. Tamén hai a opción de empregar o modo batch, para introducir os datos de organización, nome do sitio, etc.

```
openssl req -new -key server.key -out server.csr -batch -subj "/C=ES/ST=Galicia/L=Santiago/O=IES San Clemente/CN=www.sitio.
```

Os datos de organización, estado, país, localidade deben ser os mesmos, que se introduciron cando se creou a autoridade certificadora.

4. Agora xa se pode asinar o certificado. Levamos o ficheiro .csr ao equipo que é autoridade certificadora, e asinamos o certificado.:

```
openssl ca -in server.csr -config /etc/ssl/openssl.cnf
```

Se os datos de pais, localidade, organización son os mesmos, permitiranos asinar o certificado, senón non.

Tamén hai a opción de empregar o modo batch, para non ter que introducir de cada vez a palabra de paso.

```
openssl ca -in server.csr -batch -notext -out server.crt -config /etc/ssl/openssl.cnf -passin pass:abc123.
```

5. O comando anterior producirá unha saída por pantalla, que coincidirá co contido do ficheiro */etc/ssl/newcerts/01.pem* (Os seguintes certificados serán 02, 03, ...) Deberáse gardar o contido dese ficheiro entre `-----BEGIN CERTIFICATE-----` e `----END CERTIFICATE-----` **incluídas ámbalas dúas**. O nome dese ficheiro de texto pode ser www.sitio.lan.crt

Unha vez rematado, temos dous ficheiros, o *server.key* contendo a chave privada e o ficheiro *.crt* contendo o certificado asinado pola CA

Para verificar que un certificado foi asinado, por unha autoridade, executamos

```
openssl verify -verbose -CAfile cacert.pem  server.crt
```