Certificação Digital

1 – Configurando o arquivo openssl.cnf

Altere o conteúdo do arquivo `openssl.conf` (localização pode variar dependendo da distribuição):

CentOS:
```
$ vim /etc/pki/tls/openssl.cnf
-----------------------------------------------------------
```

Ubuntu/Mint:
```
$ vim /etc/ssl/openssl.conf
-----------------------------------------------------------
```

Conda:
```
$ vim ~/miniconda3/ssl/openssl.conf
-----------------------------------------------------------
```

```
...
HOME = $ENV::HOME
...
[ CA_default ]
dir = $HOME/CA
...
```

2 - Criando um cartório digital - CA

Preparar o ambiente para criação das chaves e dos certificados:

```
$ mkdir -p ~/CA/private
$ mkdir ~/CA/newcerts
$ touch ~/CA/index.txt
$ echo 01 > ~/CA/serial
$ cd ~/CA
```

Criando a chave privada e o certificado da CA:

```
$ openssl req -nodes -new -x509 -keyout ./private/cakey.pem -out cacert.pem -days 365
```

Criando a chave pública a partir da chave privada gerada anteriormente:

```
$ openssl rsa -in ./private/cakey.pem -pubout -out cakeypub.pem
```

3 – Certificado auto-assinado

Criando e assinando o próprio certificado:

```
$ openssl req -x509 -nodes -new -addext "subjectAltName = DNS:localhost"
-keyout priv-minhachave.pem -out cert-meucertificado.pem -days 365
```

> **obs.:** `-addext "subjectAltName = DNS:localhost"` é necessário caso esteja programando para sockets com criptografia.

4 – Assinando um certificado de terceiros

Criando uma requisição:

```
$ openssl req -nodes -new -addext "subjectAltName = DNS:localhost"
-keyout priv-minhachave.pem -out req-minharequisicao.csr -days 365
```

> **obs.:** `-addext "subjectAltName = DNS:localhost"` é necessário caso esteja programando para sockets com criptografia.

Assinando uma requisição/certificado de terceiros:

```
$ openssl x509 -req -extfile <(echo "subjectAltName=DNS:localhost") -in
req-minharequisicao.csr -CA ./cacert.pem -CAkey ./private/cakey.pem
-CAserial ./serial -out cert-meucertificado.pem -days 365
```

> **obs.:** devido a um bug no Openssl ainda não resolvido (31/03/2020 - https://www.openssl.org/docs/man1.1.1/man1/x509.html#BUGS), "*Extensões em certificados não são transferidas para requisições de certificado e vice-versa.*" O termo sublinhado é um paliativo para contornar esse problema.
>
> **obs.:** `-extfile <(echo "subjectAltName=DNS:localhost")` é necessário caso esteja programando para sockets com criptografia.

Assinando sua própria requisição:

> **obs.:** os nomes do país, estado, cidade e organização deste certificado deverão ser os mesmos da organização do certificado da CA.

```
$ openssl ca -out cert-meucertificado.pem -in req-minharequisicao.csr
-days 365
```