Certificação Digital

1 – Configurando o arquivo openssl.cnf

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

Red Hat/Rocky:

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

Ubuntu/Mint/Zorin:

```
$ vim /etc/ssl/openssl.conf
------------------------------------------------------------
```

Conda:

```
$ vim ~/miniconda3/envs/aulasocket/ssl/openssl.conf
------------------------------------------------------------
...
HOME = $ENV::HOME
...
[ CA_default ]
dir = $HOME/CA
...
new_certs_dir = $dir
```

2 - Criando um cartório digital - CA

Preparar o ambiente para criação das chaves e dos certificados:

```
$ mkdir -p ~/CA/private
$ 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 – Criando um certificado auto-assinado

Criando e assinando o próprio certificado:

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

4 – Criando e/ou Assinando um certificado para terceiros

Criando uma requisição:

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

Assinando uma requisição/certificado de terceiros:

```
$ openssl x509 -req -in req-minharequisicao.csr -copy_extensions=copy
-CA ./cacert.pem -CAkey ./private/cakey.pem -CAserial ./serial
-out cert-meucertificado.pem -days 365
```

5 – Consultando informações de um certificado ou requisição

Exibindo todas as informações de uma requisição:

```
$ openssl req -inform PEM -in req-minharequisicao.csr -text | more
```

Exibindo todas as informações de um certificado:

```
$ openssl x509 -in cert-meucertificado.pem -text | more
```