GUIDA OPERATIVA OPENSSL

1) GENERAZIONE DELLA CHIAVE PRIVATA E PUBBLICA

1.1 Chiave privata RSA 4096 bit

openssl genrsa -out private.key 4096

1.2 Estrazione chiave pubblica dalla chiave privata

openssl rsa -in private.key -pubout -out public.key

2) CREAZIONE DELLA CSR (CERTIFICATE SIGNING REQUEST)

2.1 CSR interattivo

openssl req -new -key private.key -out request.csr

2.2 CSR non interattivo

```
openssl req -new \
-key private.key \
-out request.csr \
-subj "/C=IT/ST=Lazio/L=Roma/O=CyberMagister/OU=Training/CN=www.esempio.com"
```

3) CREAZIONE CERTIFICATO SELF-SIGNED

3.1 Certificato self-signed diretto

```
openssl req -x509 -new \
-key private.key \
-sha256 \
-days 365 \
-out cert_selfsigned.pem \
-subj "/C=IT/ST=Lazio/L=Roma/O=CyberMagister/OU=Training/CN=www.esempio.com"
```

3.2 Certificato self-signed da CSR

```
openssl x509 -req \
-in request.csr \
-signkey private.key \
-sha256 \
-days 365 \
-out cert_selfsigned_from_csr.pem
```

4) VERIFICA CERTIFICATO

4.1 Visualizzare il contenuto

```
openssl x509 -in cert_selfsigned.pem -text -noout
```

4.2 Verifica firma con CA

```
openssl verify -CAfile ca.pem server.crt
```

4.3 Verifica certificato self-signed

```
openssl verify -CAfile cert_selfsigned.pem cert_selfsigned.pem
```