THAM KHẢO NHANH OPENSSL

Chứng chỉ, khóa, mã hóa và gỡ lỗi

Chứng Chỉ

Xem Chi Tiết Chứng Chỉ

```
openssl x509 -in cert.pem -text -noout
openssl x509 -in cert.pem -subject -noout
openssl x509 -in cert.pem -dates -noout
openssl x509 -in cert.pem -issuer -noout
```

Chuyển Đổi Định Dạng

```
# PEM to DER
openssl x509 -in cert.pem -outform DER \
    -out cert.der
# DER to PEM
openssl x509 -in cert.der -inform DER \
    -out cert.pem
```

Định Dạng Phổ Biến

`PEM`	Mã hoá Base64, `-----BEGIN CERTIFICATE-----`
`DER`	Định dạng nhị phân, nhỏ gọn
`PFX / P12`	Gói PKCS#12 (chứng chỉ + khóa + chuỗi)
`CRT / CER`	File chứng chỉ (thường là PEM hoặc DER)

Tạo Khóa

Khóa RSA

```
openssl genrsa -out key.pem 4096
openssl rsa -in key.pem -pubout \
    -out pubkey.pem
openssl rsa -in key.pem -text -noout
```

Khóa EC

```
openssl ecparam -genkey -name prime256v1 \
    -out ec_key.pem
openssl ec -in ec_key.pem -pubout \
    -out ec_pub.pem
```

Khóa Ed25519

```
openssl genpkey -algorithm Ed25519 \
    -out ed25519_key.pem
openssl pkey -in ed25519_key.pem -pubout \
    -out ed25519_pub.pem
```

So Sánh Thuật Toán Khóa

`RSA 2048/4096`	Được hỗ trợ rộng rãi, khóa lớn hơn
`ECDSA (P-256)`	Khóa nhỏ hơn, nhanh hơn, dành cho TLS hiện đại
`Ed25519`	Nhanh nhất, nhỏ nhất, không có trên tất cả hệ thống

CSR

Tạo CSR

```
openssl req -new -key key.pem \
    -out request.csr
# Non-interactive
openssl req -new -key key.pem -out req.csr \
    -subj "/CN=example.com/O=MyOrg/C=US"
```

Tạo Khóa + CSR Cùng Lúc

```
openssl req -new -newkey rsa:4096 \
    -nodes -keyout key.pem -out req.csr \
    -subj "/CN=example.com"
```

Kiểm Tra CSR

```
openssl req -in request.csr -text -noout
openssl req -in request.csr -verify -noout
```

Các Trường CSR Phổ Biến

`CN`	Common Name (domain hoặc hostname)
`O`	Tên tổ chức
`OU`	Đơn vị tổ chức
`C`	Quốc gia (mã 2 chữ cái)
`ST`	Tỉnh/bang
`L`	Địa phương / thành phố

Tự Ký

Chứng Chỉ Tự Ký Nhanh

```
openssl req -x509 -newkey rsa:4096 -nodes \
    -keyout key.pem -out cert.pem -days 365 \
    -subj "/CN=localhost"
```

Có SAN (Subject Alternative Name)

```
openssl req -x509 -newkey rsa:4096 -nodes \
    -keyout key.pem -out cert.pem -days 365 \
    -subj "/CN=myapp.local" \
    -addext "subjectAltName=\
DNS:myapp.local,DNS:*.myapp.local,IP:127.0.0.1"
```

Từ Khóa Có Sẵn

```
openssl req -x509 -key key.pem \
    -out cert.pem -days 365 \
    -subj "/CN=example.com"
```

Xác Minh

Xác Minh Chứng Chỉ

```
openssl verify -CAfile ca.pem cert.pem
openssl verify -CAfile ca.pem \
    -untrusted intermediate.pem cert.pem
```

Kiểm Tra Khóa / Chứng Chỉ Khớp

```
# Modulus must match for key and cert
openssl x509 -in cert.pem -modulus -noout
openssl rsa -in key.pem -modulus -noout
openssl req -in req.csr -modulus -noout
```

Kiểm Tra Hết Hạn

```
openssl x509 -in cert.pem -checkend 86400
# Returns 0 if valid for 86400s (24h)
openssl x509 -in cert.pem -enddate -noout
```

Chứng Chỉ Server Từ Xa

```
openssl s_client -connect example.com:443 \
    < /dev/null 2>/dev/null \
    | openssl x509 -text -noout
```

Mã Hóa

Mã Hóa Đối Xứng

```
openssl enc -aes-256-cbc -salt -pbkdf2 \
    -in plain.txt -out encrypted.bin
openssl enc -aes-256-cbc -d -pbkdf2 \
    -in encrypted.bin -out plain.txt
```

Mã Hóa Bất Đối Xứng

```
# Encrypt with public key
openssl pkeyutl -encrypt \
    -pubin -inkey pub.pem \
    -in secret.txt -out secret.enc
# Decrypt with private key
openssl pkeyutl -decrypt \
    -inkey key.pem \
    -in secret.enc -out secret.txt
```

Ciphers Phổ Biến

`aes-256-cbc`	AES 256-bit, chế độ CBC (mặc định phổ biến)
`aes-256-gcm`	AES 256-bit, chế độ GCM (có xác thực)
`chacha20-poly1305`	Stream cipher hiện đại (nhanh trên ARM)

Liệt kê tất cả: `openssl enc -list`

Hashing

Hash File

```
openssl dgst -sha256 file.txt
openssl dgst -sha512 file.txt
openssl dgst -md5 file.txt  # legacy only
```

HMAC

```
openssl dgst -sha256 -hmac "secret" file.txt
echo -n "message" | openssl dgst \
    -sha256 -hmac "mykey"
```

Thuật Toán Hash

`SHA-256`	Lựa chọn chuẩn cho kiểm tra tính toàn vẹn
`SHA-384 / SHA-512`	Biến thể SHA-2 mạnh hơn
`SHA3-256`	Tiêu chuẩn mới nhất (dựa trên Keccak)
`MD5`	Đã bị phá, chỉ dùng kế thừa — không dùng cho bảo mật
`BLAKE2`	Thay thế nhanh và an toàn (nếu được hỗ trợ)

S/MIME

Ký Email

```
openssl smime -sign -in msg.txt \
    -signer cert.pem -inkey key.pem \
    -out signed.msg
```

Xác Minh Email Đã Ký

```
openssl smime -verify -in signed.msg \
    -CAfile ca.pem -out original.txt
```

Mã Hóa / Giải Mã Email

```
# Encrypt for recipient
openssl smime -encrypt -aes256 \
    -in msg.txt -out encrypted.msg \
    recipient_cert.pem
# Decrypt
openssl smime -decrypt -in encrypted.msg \
    -recip cert.pem -inkey key.pem
```

Gỡ Lỗi

Kiểm Tra Kết Nối TLS

```
openssl s_client -connect host:443
openssl s_client -connect host:443 \
    -servername example.com  # SNI
openssl s_client -connect host:443 \
    -tls1_3  # force TLS 1.3
```

Hiển Thị Chuỗi Chứng Chỉ

```
openssl s_client -connect host:443 \
    -showcerts < /dev/null
```

Kiểm Tra TLS Ciphers

```
openssl ciphers -v 'HIGH:!aNULL'
openssl s_client -connect host:443 \
    -cipher 'ECDHE-RSA-AES256-GCM-SHA384'
```

Thao Tác PKCS#12

```
# Create PFX bundle
openssl pkcs12 -export -out bundle.pfx \
    -inkey key.pem -in cert.pem -certfile ca.pem
# Extract from PFX
openssl pkcs12 -in bundle.pfx -nodes \
    -out all.pem
```

Mẫu Phổ Biến

Tạo Số Ngẫu Nhiên An Toàn

```
openssl rand -hex 32    # 32 random bytes, hex
openssl rand -base64 24 # 24 random bytes, b64
```

Mã Hoá / Giải Mã Base64

```
openssl base64 -in file.bin -out file.b64
openssl base64 -d -in file.b64 -out file.bin
```

Hash Mật Khẩu

```
openssl passwd -6 -salt xyz "password"
# -6 = SHA-512, -5 = SHA-256, -1 = MD5
```

Cheat Nhanh: Khóa + Chứng Chỉ + Xác Minh

```
openssl req -x509 -newkey rsa:4096 -nodes \
    -keyout k.pem -out c.pem -days 365 \
    -subj "/CN=test"
openssl x509 -in c.pem -text -noout
```