Referensi Cepat OpenSSL

Sertifikat, key, enkripsi, dan debugging

Sertifikat

Lihat Detail Sertifikat

```
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
```

Konversi Format

```
# 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
```

Format Umum

PEM	Base64-encoded, **-----BEGIN CERTIFICATE-----**
DER	Format biner, ringkas
PFX / P12	Bundle PKCS#12 (cert + key + chain)
CRT / CER	File sertifikat (biasanya PEM atau DER)

Pembuatan Key

Key RSA

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

Key EC

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

Key Ed25519

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

Perbandingan Algoritma Key

RSA 2048/4096	Dukungan luas, key lebih besar
ECDSA (P-256)	Key lebih kecil, lebih cepat, TLS modern
Ed25519	Tercepat, terkecil, belum didukung semua sistem

CSR

Buat CSR

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

Buat Key + CSR Sekaligus

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

Periksa CSR

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

Field CSR Umum

CN	Common Name (domain atau hostname)
O	Nama organisasi
OU	Unit organisasi
C	Negara (kode 2 huruf)
ST	Provinsi atau negara bagian
L	Lokasi / kota

Self-Signed

Sertifikat Self-Signed Cepat

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

Dengan 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"
```

Dari Key yang Ada

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

Verifikasi

Verifikasi Sertifikat

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

Periksa Kecocokan Key / Cert

```
# Modulus harus sama untuk key dan cert
openssl x509 -in cert.pem -modulus -noout
openssl rsa -in key.pem -modulus -noout
openssl req -in req.csr -modulus -noout
```

Periksa Kedaluwarsa

```
openssl x509 -in cert.pem -checkend 86400
# Mengembalikan 0 jika valid selama 86400 detik (24 jam)
openssl x509 -in cert.pem -enddate -noout
```

Sertifikat Server Remote

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

Enkripsi

Enkripsi Simetris

```
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
```

Enkripsi Asimetris

```
# Enkripsi dengan public key
openssl pkeyutl -encrypt \
    -pubin -inkey pub.pem \
    -in secret.txt -out secret.enc
# Dekripsi dengan private key
openssl pkeyutl -decrypt \
    -inkey key.pem \
    -in secret.enc -out secret.txt
```

Cipher Umum

aes-256-cbc	AES 256-bit, mode CBC (default umum)
aes-256-gcm	AES 256-bit, mode GCM (terautentikasi)
chacha20-poly1305	Stream cipher modern (cepat di ARM)

Daftar semua: `openssl enc -list`

Hashing

Hash File

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

HMAC

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

Algoritma Hash

SHA-256	Pilihan standar untuk pemeriksaan integritas
SHA-384 / SHA-512	Varian SHA-2 yang lebih kuat
SHA3-256	Standar terbaru (berbasis Keccak)
MD5	Sudah usang, hanya legacy — jangan digunakan untuk keamanan
BLAKE2	Alternatif cepat dan aman (jika didukung)

S/MIME

Tanda Tangani Email

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

Verifikasi Email Bertanda Tangan

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

Enkripsi / Dekripsi Email

```
# Enkripsi untuk penerima
openssl smime -encrypt -aes256 \
    -in msg.txt -out encrypted.msg \
    recipient_cert.pem
# Dekripsi
openssl smime -decrypt -in encrypted.msg \
    -recip cert.pem -inkey key.pem
```

Debugging

Uji Koneksi 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  # paksa TLS 1.3
```

Referensi Cepat OpenSSL

Tampilkan Certificate Chain

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

Periksa TLS Cipher

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

Operasi PKCS#12

```
# Buat bundle PFX
openssl pkcs12 -export -out bundle.pfx \
    -inkey key.pem -in cert.pem -certfile ca.pem
# Ekstrak dari PFX
openssl pkcs12 -in bundle.pfx -nodes \
    -out all.pem
```

Pola Umum

Buat Random Aman

```
openssl rand -hex 32    # 32 byte acak, hex
openssl rand -base64 24 # 24 byte acak, b64
```

Encode / Decode Base64

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

Hashing Password

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

Cepat: Key + Cert + Verifikasi

```
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
```