Comandi OpenSSL

Verifica certificati, debug delle catene, conversione formati – i comandi openssl di tutti i giorni, cercabili e copiabili con un clic.

daniele.michelin // cheat sheet

Test di connessione

Connessione TLS con SNI e dettagli dell'handshake

```
openssl s_client -connect example.com:443 -servername example.com </dev/null
```

Mostra l'intera catena di certificati servita

```
openssl s_client -connect example.com:443 -servername example.com -showcerts </dev/null
```

Periodo di validità del certificato del server

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

Subject, emittente e SAN del certificato

```
openssl s_client -connect example.com:443 -servername example.com </dev/null 2>/dev/null | openssl x509 -noout -subject -issuer -ext subjectAltName
```

Verifica l'OCSP stapling

```
openssl s_client -connect example.com:443 -servername example.com -status </dev/null 2>/dev/null | grep -A 3 'OCSP Response'
```

Testa STARTTLS su SMTP submission

```
openssl s_client -starttls smtp -connect mail.example.com:587 -servername mail.example.com </dev/null
```

Testa STARTTLS su IMAP

```
openssl s_client -starttls imap -connect mail.example.com:143 </dev/null
```

Testa IMAPS (TLS implicito)

```
openssl s_client -connect mail.example.com:993 -servername mail.example.com </dev/null
```

Versioni TLS e cipher

Verifica se TLS 1.3 è supportato

```
openssl s_client -connect example.com:443 -servername example.com -tls1_3 </dev/null
```

Verifica se TLS 1.2 è supportato

```
openssl s_client -connect example.com:443 -servername example.com -tls1_2 </dev/null
```

Testa il vecchio TLS 1.1 (deve fallire)

```
openssl s_client -connect example.com:443 -servername example.com -tls1_1 </dev/null
```

Forza una specifica cipher suite

```
openssl s_client -connect example.com:443 -servername example.com -tls1_2 -cipher 'ECDHE-RSA-AES256-GCM-SHA384' </dev/null
```

Elenca i cipher di una cipher string

```
openssl ciphers -v 'HIGH:!aNULL:!MD5'
```

Analizzare certificati

Mostra il certificato completo in chiaro

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

Mostra la data di scadenza

```
openssl x509 -in cert.pem -noout -enddate
```

Scade entro 30 giorni? (exit code 1 = sì)

```
openssl x509 -in cert.pem -noout -checkend 2592000
```

Mostra l'impronta SHA-256

```
openssl x509 -in cert.pem -noout -fingerprint -sha256
```

Verifica la catena con root e intermedio

```
openssl verify -CAfile root.pem -untrusted intermediate.pem cert.pem
```

Chiavi e CSR

Crea chiave e CSR con SAN in un solo passo

```
openssl req -new -newkey rsa:4096 -nodes -keyout example.key -out example.csr -subj "/CN=example.com" -addext "subjectAltName=DNS:example.com,DNS:www.example.com"
```

Genera una chiave ECDSA (P-256)

```
openssl genpkey -algorithm EC -pkeyopt ec_paramgen_curve:P-256 -out example.key
```

Mostra una CSR e ne verifica la firma

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

Crea un certificato autofirmato di test

```
openssl req -x509 -newkey rsa:2048 -nodes -days 365 -keyout test.key -out test.crt -subj "/CN=test.local"
```

Chiave e certificato corrispondono? Hash uguali

```
openssl x509 -in cert.pem -noout -pubkey | openssl sha256; openssl pkey -in key.pem -pubout | openssl sha256
```

Confronto RSA tramite modulus (metodo classico)

```
openssl x509 -in cert.pem -noout -modulus | openssl md5; openssl rsa -in key.pem -noout -modulus | openssl md5
```

Convertire formati

Converte PEM in DER

```
openssl x509 -in cert.pem -outform der -out cert.der
```

Converte DER in PEM

```
openssl x509 -in cert.der -inform der -out cert.pem
```

Crea un PFX/P12 da chiave, certificato e catena (Windows/IIS)

```
openssl pkcs12 -export -out cert.pfx -inkey key.pem -in cert.pem -certfile chain.pem
```

! Estrae un PFX – la chiave risulta non cifrata

```
openssl pkcs12 -in cert.pfx -nodes -out all.pem
```

! Rimuove la passphrase da una chiave

```
openssl pkey -in encrypted.key -out plain.key
```

Utilità

Genera una password casuale (32 caratteri)

```
openssl rand -base64 24
```

Secret casuale in esadecimale (es. per token)

```
openssl rand -hex 32
```

Checksum SHA-256 di un file

```
openssl dgst -sha256 file.iso
```

Mostra versione e opzioni di build di OpenSSL

```
openssl version -a
```