

SSL/TLS & OpenSSL CLI Diagnostics Cheat Sheet

Essential OpenSSL terminal commands, certificate inspection flags, file formats, and TLS handshakes.

Live Interactive SSL Certificate Checker: <https://lotsofnetwork.com/ssl-checker>

OpenSSL CLI Command Syntax	Diagnostic Purpose & Action
<code>openssl s_client -connect host:443 -servername host</code>	Connects to remote server with SNI and displays full TLS certificate chain
<code>openssl x509 -enddate -noout -in cert.crt</code>	Prints exact certificate expiration date without opening full file
<code>openssl x509 -text -noout -in cert.crt</code>	Prints complete certificate details: Subject, Issuer, SANs, and algorithm
<code>openssl x509 -noout -modulus -in cert.crt openssl md5</code>	Computes cert modulus MD5 hash (must match private key hash exactly)
<code>openssl rsa -noout -modulus -in server.key openssl md5</code>	Computes private key modulus hash to verify certificate pair match
<code>openssl req -text -noout -verify -in request.csr</code>	Verifies and displays Certificate Signing Request details before submission
<code>openssl req -new -newkey rsa:2048 -nodes -keyout k.key -out r.csr</code>	Generates a fresh 2048-bit RSA private key and matching CSR in one step
<code>openssl pkcs12 -export -out b.pfx -inkey k.key -in c.crt</code>	Bundles certificate and private key into PKCS#12 (.pfx/.p12) archive

Certificate File Formats & Extensions Reference

Extension	Encoding Format	Usage & Server Environment
<code>.pem, .crt</code>	Base64 ASCII	Begins with '-----BEGIN CERTIFICATE-----'. Standard for Nginx, Apache, Linux
<code>.key</code>	Private Key	Confidential private key matching certificate. Store with chmod 600 permissions
<code>.csr</code>	Signing Request	Public key and domain identity submitted to Certificate Authority for issuance
<code>.pfx, .p12</code>	PKCS#12 Archive	Password-protected binary container containing cert, CA chain, and private key
<code>.der</code>	Binary ASN.1	Binary certificate representation common in Java keystores and Windows servers