OpenSSL s_client Options Cheat Sheet

-connect host:port	Host and port to connect to. Default: localhost:4433. IPv6 addresses must be in brackets.
host:port	Positional alternative to -connect .
-bind host:port	Local address/port to bind as the connection source.
-proxy_user userid	Username for proxy basic authentication.
-proxy_pass arg	Password source for proxy authentication.
-unix path	Connect over a Unix-domain socket.
-4	Use IPv4 only.
-6	Use IPv6 only.
-reconnect	Reconnect 5 times using the same session ID to test session caching.
-servername name	Set TLS SNI extension value. Defaults to the hostname from -connect or 'localhost'.
-noservername	Suppress sending the SNI extension.
-cert filename	Client certificate to present if requested by the server.
-certform DER|PEM|P12	Format of the client certificate file.
-cert_chain	FIle/URI of the untrusted certs for building the client certificate chain.
-key filename|uri	Client private key. Defaults to the certificate file if not specified.
-keyform DER|PEM|P12|ENGINE	Format of the private key.
-pass arg	Password source for the private key and certificate.
-verify depth	Enable server certificate verification up to the given chain depth. Continues on error unless -verify_return_error is set.
-verify_return_error	Abort the handshake on certificate verification failure.
-verify_quiet	Show only verification errors, not all verify output.
-verifyCAfile filename	PEM file of trusted CAs for verifying the server certificate.
-verifyCApath dir	Directory of trusted CAs (hash format) for server verification.
-verifyCAstore uri	URI of a certificate store for server verification.
-chainCAfile file	PEM file of trusted certs for building the client certificate chain.
-chainCApath dir	Directory of trusted certs (hash format) for building the client chain.
-chainCAstore uri	URI of a store used to build the client certificate chain.
-CRL filename	CRL file for checking the server's certificate.
-crl_download	Download CRL from distribution points in the server certificate. Requires -crl_check.
-CAfile / -CApath / -CAstore	Trusted CA sources for certificate verification.
-status	Request OCSP stapling from the server and print the response.
-ct	Request and report signed certificate timestamps (SCTs). Also enables OCSP stapling.
-noct	Disable Certificate Transparency.
-dane_tlsa_domain domain	Enable DANE TLSA authentication and set the base domain. Requires -dane_tlsa_rrdata.
-dane_tlsa_rrdata rrdata	DANE TLSA RRDATA in presentation form. Can be specified multiple times.
-showcerts	Display the full certificate chain sent by the server (not verified).
-ssl_config section	Use named config file section to configure SSL_CTX.
-no_ssl3 / -no_tls1 / -no_tls1_1 / -no_tls1_2 / -no_tls1_3	Disable a specific protocol version.
-ssl3 / -tls1 / -tls1_1 / -tls1_2 / -tls1_3	Force a specific protocol version.
-dtls / -dtls1 / -dtls1_2	Use DTLS instead of TLS.
-cipher cipherlist	TLS 1.2 and below cipher list to advertise.
-ciphersuites val	TLS 1.3 cipher suite list (colon-separated names).
-sigalgs sigalglist	Signature algorithms to advertise in the ClientHello.
-curves curvelist	Supported elliptic curves/groups to advertise.
-starttls protocol	Send protocol-specific STARTTLS negotiation: smtp, pop3, imap, ftp, xmpp, irc, postgres, mysql, lmtp, nntp, sieve, ldap.
-name hostname	Hostname for STARTTLS protocols (XMPP stream 'to'; SMTP/LMTP EHLO/LHLO name).
-alpn protocols	Advertise ALPN with a comma-separated protocol list.
-no_ticket	Disable session ticket support.
-sess_out filename	Save the SSL session to a file.
-sess_in filename	Load and attempt to resume a session from a file.
-early_data file	Send file contents as TLS 1.3 early data (requires a resumed session).
-enable_pha	Send Post-Handshake Authentication extension (TLS 1.3 only).
-fallback_scsv	Send TLS_FALLBACK_SCSV in the ClientHello.
-no_etm	Disable Encrypt-then-MAC negotiation.
-bugs	Enable workarounds for known SSL/TLS implementation bugs.
-ignore_unexpected_eof	Treat a connection closed without close_notify as a clean shutdown.
-maxfraglen len	Enable Maximum Fragment Length Negotiation (512, 1024, 2048, or 4096).
-keymatexport label	Export keying material using the given label.
-keymatexportlen len	Number of bytes to export (default: 20).
-psk_identity identity	PSK identity for PSK cipher suites. Default: 'Client_identity'.
-psk key	PSK key in hex. Required for PSK cipher suites.
-psk_session file	PEM-encoded SSL_SESSION for PSK (TLS 1.3 only).
-keylogfile file	Append TLS secrets to a file for decryption in Wireshark.
-msg	Show protocol messages.
-trace	Verbose trace of protocol messages.
-msgfile filename	Write -msg or -trace output to a file instead of stdout.
-debug	Verbose debug output with hex dump of all traffic.
-tlsextdebug	Hex dump of TLS extensions received from the server.
-state	Print SSL session state transitions.
-prexit	Print session info on exit, even if the connection failed.
-quiet	Suppress session and certificate output. Implies -ign_eof and -nocommands.
-brief	Print a short connection summary instead of full verbose output.
-crlf	Translate LF to CR+LF (required by some servers).