

1. Client hello: client gửi message tới server, chứa thông tin về SSL/TLS version hổ trợ, thuật toán mã hóa, ...
2. Server hello: server gửi message tới client, chứ thông tin về SSL/TLS version sẽ được dùng, thuật toán mã hóa được chọn, về digital certificate của server (nếu có).
3. Server certificate: chứa public key được cung cấp bởi trusted Certificat Authority (CA), client sẽ kiểm tra certificate. Nếu còn giá trị sử dụng sẽ tạo kết nối.
4. Key exchange: client và server trao đổi khóa để tạo ra một khóa bí mật, sẽ được dùng để mã hóa và giải mã trong suốt quá trình trao đổi thông tin.
5. Session key: trong khi chia sẻ khóa bí mật, cả client và server sẽ nhận được session key. Session key dùng để mã hóa và giải mã trong suốt quá trình. Mỗi session sẽ có một session key riêng.
6. Cipher suite selection: Client và server cùng thỏa thuận về bộ giải mã, bao gồm thuật toán giải mã, thuật toán hàm băm và các thuật toán khác trong suốt quá trình trao đổi.
7. Finish handshake: sau khi thỏa thuận xong bộ giải mã và các keys, client và server cùng gửi FINISH message để kết thúc quá trình bắt tay. Từ thời điểm này, SSL/TLS đảm bảo bảo mật và mã hóa.
8. Secure data exchange: sau bước bắt tay, dữ liệu có thể được trao đổi thông qua các giao thức bảo mật.
9. Session resumption: SSL/TLS cho phép nối lại phiên, nhằm cải thiện hiệu suất bằng cách sử dụng lại các phiên đã sử dụng mà không cần qua bước bắt tay.