



Client

Server

1. ClientHello

Parameter negotiation  
Key exchange

Key exchange  
Handshake finished  
Send server certificate \*  
Request client certificate \*

2. ServerHello

*Secure channel*

3. Application data

Protected application data  
Handshake finished  
Verify server certificate \*  
Send client certificate \*

Protected application data

4. Application data