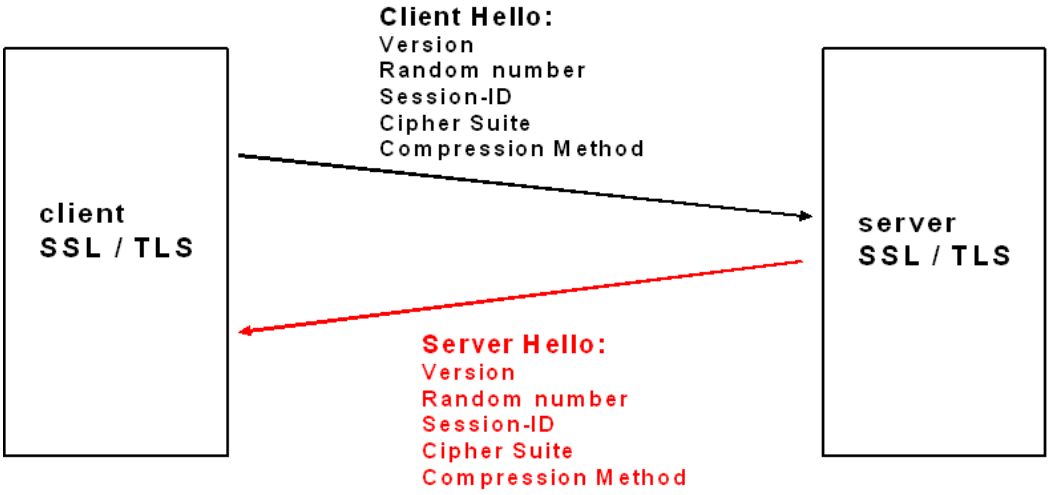
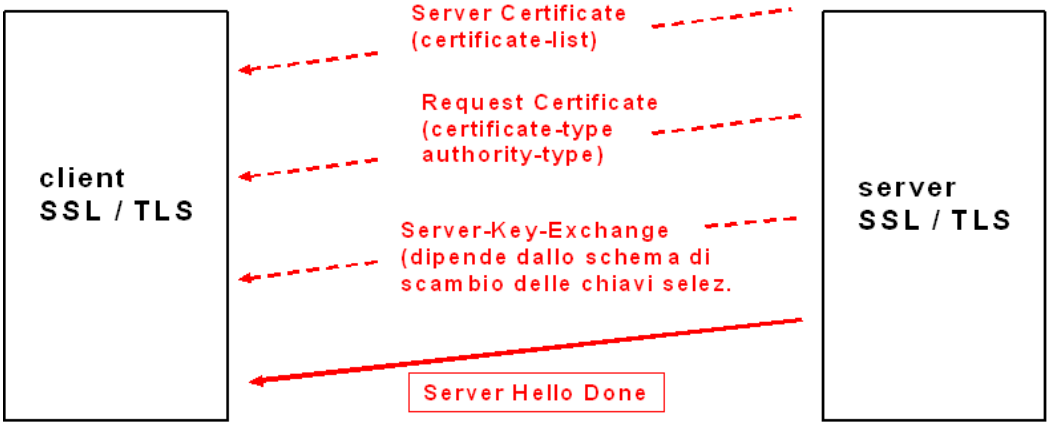
SSL TLS handshake

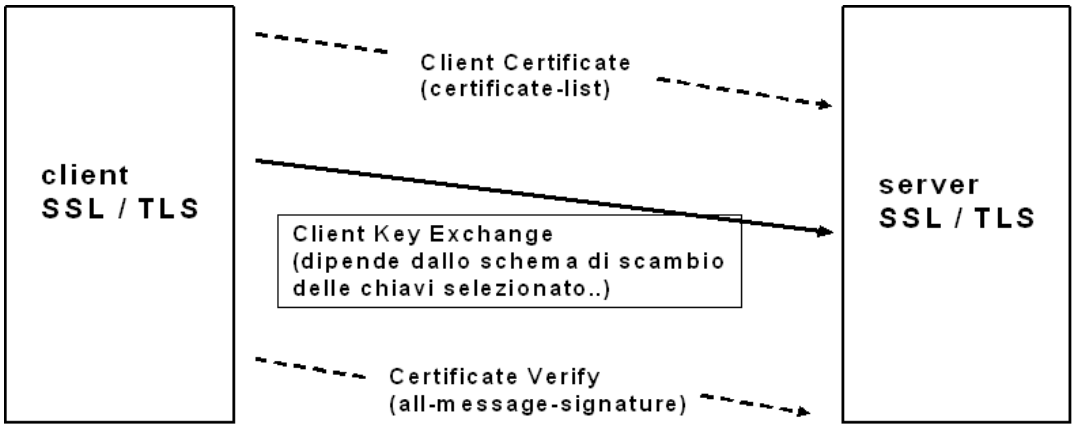
Fase 1:



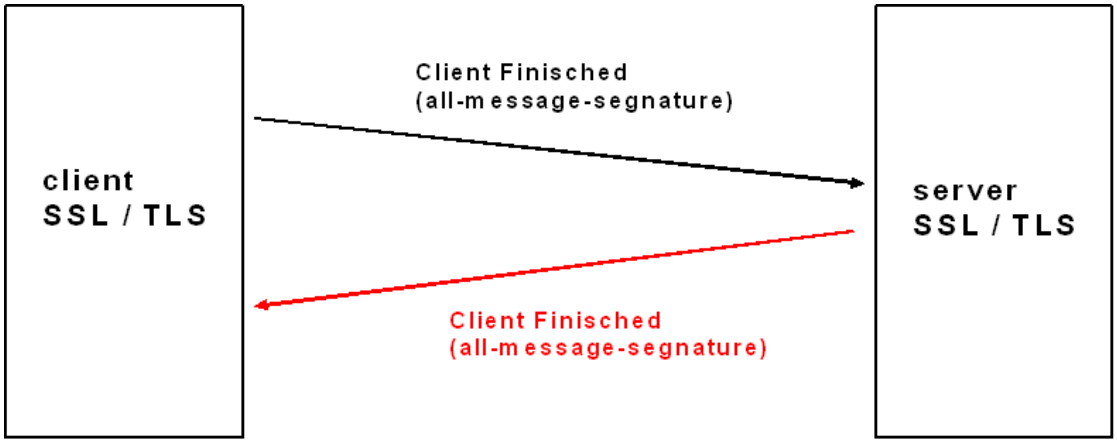
Fase 2: se il server acconsente ad utilizzare per la nuova connessione una sessione preesistente, la fase di handshake èdaconsiderarsi conclusa. Se i parametri associato ad una sessione SSL/TLS non possono essere condivisi tra più connessioni oppure non esiste alcuna sessione preesistente tra le due entità, occorre completare la fase di negoziazione scambiandosi gli altri messaggi



Fase 3:


client
SSL / TLS
Client Certificate
(certificate-list)
Client Key Exchange
(dipende dallo schema di scambio
delle chiavi selezionato..)
Certificate Verify
(all-message-signature)
server
SSL / TLS

Fase 4:


client
SSL / TLS
Client Finisched
(all-message-segnature)
Client Finisched
(all-message-segnature)
server
SSL / TLS