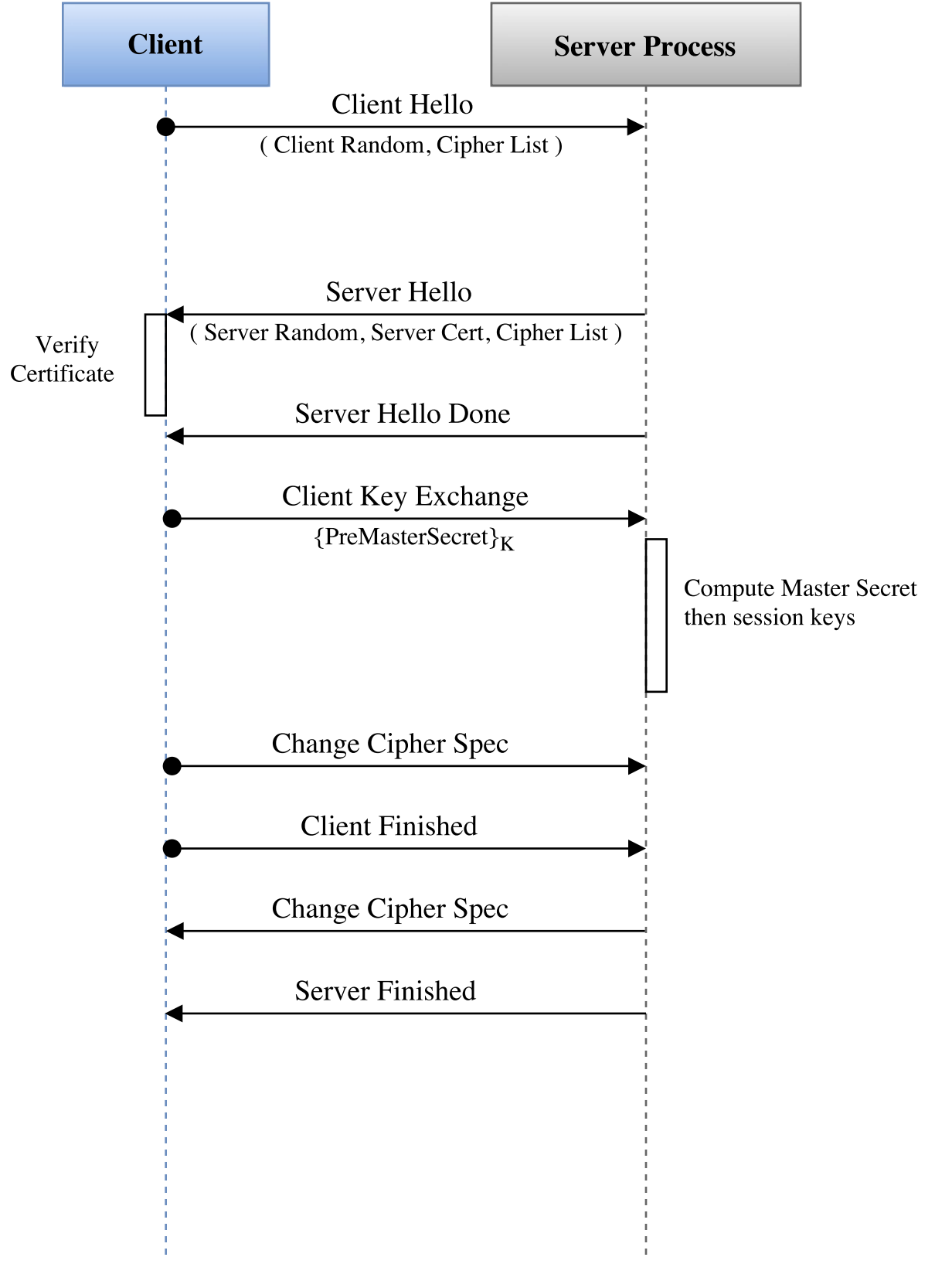
Client
Server Process
Client Hello
(Client Random, Cipher List)
Server Hello
(Server Random, Server Cert, Cipher List)
Verify Certificate
Server Hello Done
Client Key Exchange
{PreMasterSecret}K
Compute Master Secret then session keys
Change Cipher Spec
Client Finished
Change Cipher Spec
Server Finished