Common:

Both client and server created a SSL\_CTX, using the SSLv23 client method, with SSLv2 disabled using SSL\_CTX\_set\_options(…). The CA certificate and corresponding Private Key and certificates were loaded into to CTX. The passcode for the Private Key was set to be “password”.

Client:

A SSL object was created using the CTX object, and attached to the socket after connection is established (via TCP). SSL\_connect() was used for the SSL handshake.

Server:

A SSL object was created using the CTX object, and attached to the connected socket. SSL\_accept() is used by the server for the SSL handshake. The rest of the code is run by the child of the server process.

Common:

The verify mode was set to SSL\_VERIFY\_PEER, so that both sides will send a certificate. Both then retrieved the peer certificate, using SSL\_get\_peer\_certificate(…) and used SSL\_get\_verify\_results(…) to verify the certificate using the CA certificate set earlier in the CTX. Then the certificate details were verified though accessing certificate details (Common Name and Email of issuer) to ensure that the certificate belongs to the expected person.

Then the message was transferred, and the shutdown procedure initiated. The client sends “check\_notify” requests via the SSL\_shutdown() function until it returns a “1” (client has also received a “check\_notify” request from the server). Then, both having acknowledged that the other also sent a shutdown request, shuts down.