Subject: SSL handshake error
Posted by bryan.js00 on Sun, 02 Mar 2014 02:08:22 GMT
View Forum Message <> Reply to Message

I'm just beginning to use U++, and I'm trying to learn how to use sockets and SSL. I have modified the HttpServer example to use SSL, but I'm getting the following error:

ERROR socket(256) / SSL handshake: SSL_ERROR_SSL

Here is the full code that I'm using:

```
#include <Core/Core.h>

using namespace Upp;

TcpSocket   server;

String cert;
String key;

void Server()
{
 for(;;) {
  TcpSocket socket;
  LOG("Waiting...");
  bool b = socket.Accept(server);
  if(b) {
   LOG("Connection accepted");

   socket.SSLCertificate(cert, key, FALSE);

   if( !socket.StartSSL() ) {
    LOG("Cannot start SSL\r\n");
    return;
   } else {
    LOG("SSL Started\r\n");
   }

   while( socket.SSLHandshake() ) { };

   LOG("Responding");

   HttpHeader http;
   http.Read(socket);
   String html;
```

```
   html << "<html>"
        << "<b>Method:</b> " << http.GetMethod() << "<br>"
        << "<b>URI:</b> " << http.GetURI() << "<br>";
   for(int i = 0; i < http.fields.GetCount(); i++)
    html << "<b>" << http.fields.GetKey(i) << ":</b> " << http.fields[i] << "<br>";
   int len = (int)http.GetContentLength();
   if(len > 0)
    socket.GetAll(len);
   html << "<b><i>Current time:</i></b> " << GetSysTime() << "</html>";
   HttpResponse(socket, http.scgi, 200, "OK", "text/html", html);

  }
 }
}

CONSOLE_APP_MAIN
{
 StdLogSetup(LOG_COUT|LOG_FILE);

 cert = LoadFile("D:/Develop/MyApps/ERPLib/erp.cert");
 key = LoadFile("D:/Develop/MyApps/ERPLib/erp.key");

 if(!server.Listen(4000, 10)) {
  LOG("Cannot open server port for listening\r\n");
  return;
 }

 Server();
}
```

The error occurs in the call to socket.StartSSL() and socket.StartSSL() returns FALSE.

Am I even using the SSL portion of sockets correctly? I'm kind of shooting in the dark.

Also, the 'client' portion of this test is FireFox web browser. I'm typing my computer's IP address plus the port 4000 into the address bar:
https://10.10.10.101:4000
Is there any problem with creating a connection that way?

Edit: forgot to mention I'm using OpenSSL 1.0.1f. Also, the cert and key information was generated using an online utility.
