CS469 Distributed Systems
Creating and Using Self-Signed X.509 Certificates

SSL makes use of public key cryptography, in which asymmetric public/private key pairs are used to establish a symmetric key used to encrypt the communications between two processes that are communicating over a network. For Programming Assignment 4, the client and server will communicate over a secure channel using the OpenSSL library. This document explains how to create the certificate needed by the server.

To create a self-signed certificate your server can use, at the command prompt type:

```
openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out cert.pem
```

This will create two files: a private key contained in the file 'key.pem' and a certificate containing a public key in the file 'cert.pem'. Your server will require both in order to operate properly. Both files must reside in the working directory of your server.

The client does not require any such setup to work properly.