# Security Certificates for OpenFresco

1. Download openSSL (for win32) from the following webpage: http://www.slproweb.com/products/Win32OpenSSL.html
2. Install in "C:\Program Files\OpenSSL\" by following the onscreen instructions

## Creating Self-Signed Certificates:

1. Run openssl.exe from a command prompt:
   C:\Program Files\OpenSSL\bin> openssl
2. Generate a private key for the server:
   a) with password:
      OpenSSL> genrsa -des3 -out server.key 4096
   b) without password:
      OpenSSL> genrsa -out server.key 4096
3. Generate a self-signed certificate from the private key:
   OpenSSL> req -new -x509 -days 365 -key server.key -out server.crt
   *provide the required information (an example is shown below, but you should use the information for your location, organization, and identification):*
   Country Name: US
   State or Province Name: California
   Locality Name: Berkeley
   Organization Name: NEES
   Organizational Unit Name: UCB
   Common Name: OpenFresco
   Email Address: .
4. Generate a client CA certificate by making a copy:
   > copy server.crt client_ca.crt
5. Repeat the above four steps to generate the following files.
   client.key, client.crt, server_ca.crt
6. Place the server files in folder where server-program will be run and the client files in folder where client-program will be run.

## Creating Certificates using your own CA (Certificate Authority):

1. Run openssl.exe from a command prompt:
   C:\Program Files\OpenSSL\bin> openssl
2. Generate a private key for your own local CA:
   a) with password (preferably):
      OpenSSL> genrsa -des3 -out ca.key 4096
   b) without password:
      OpenSSL> genrsa -out ca.key 4096
3. Generate a CA certificate from the private key (copies will be made in 9):

OpenSSL> req -new -x509 -days 3650 -key ca.key
-out ca.crt
*provide the required information (an example is shown below, but you should use the information for your location, organization, and identification):*
Country Name: US
State or Province Name: California
Locality Name: Berkeley
Organization Name: NEES
Organizational Unit Name: UCB
Common Name: OpenFrescoCA
Email Address: .

4. Create a directory called “localCA” with a subdirectory “private” and move ca.key into ..\localCA\private\ and ca.crt into ..\localCA\. This concludes the generation of the local certificate authority. In the next few steps the server and client certificate requests are generated and signed by the CA.

5. Generate a private key for the server:
   c) with password:
      OpenSSL> genrsa -des3 -out server.key 4096
   d) without password:
      OpenSSL> genrsa -out server.key 4096
6. Generate a certificate request from the private key:
   OpenSSL> req -new -key server.key -out server.csr
   *provide the required information (an example is shown below, but you should use the information for your location, organization, and identification):*
   Country Name: US
   State or Province Name: California
   Locality Name: Berkeley
   Organization Name: NEES
   Organizational Unit Name: UCB
   Common Name: OpenFrescoServer
   Email Address: .
   A challenge password: *******
   An optional company name:
7. Sign the certificate request with the CA:
   OpenSSL> x509 -req -days 365 -in server.csr -CA ..\localCA\ca.crt
   -CAkey ..\localCA\private\ca.key -set_serial 01 -out server.crt
8. Repeat steps 5, 6 & 7 to generate the following files.
   client.key, client.csr, client.crt
9. Place server_ca.crt (a copy of ca.crt), server.key & server.crt files in folder where server-program will be run and client_ca.crt (a copy of ca.crt), client.key & client.crt files in folder where client-program will be run.

## Some References:

http://www.openssl.org/docs/HOWTO/
http://sial.org/howto/openssl/
http://www.tc.umn.edu/~brams006/
http://www.g-loaded.eu/2005/11/10/be-your-own-ca/