Tutorial – Digital Certificates

http://keytool.sourceforge.net/update

Q1.

Using the Eclipse keytool plugin, create a digital certificate and store it in a file called “keystore”. You need to specify an alias (paul) password (1243) filename (keystore) and keystore password (file).

Run C1Show.java to print the contents of the keystore.

Q2.

Export the certificate from keystore to a file called name.cer (paul.cer). Run C3PrintCert .java to print the contents of the certificate.

Q3.

Copy the file cacerts from the JRE lib/security folder into your project.

Q4.

Run the SSL server E1Server.java. It should get its certificate from your certificate file (paul.cer). Run E2SSLCLient.java. Its default truststore location should be the current folder (root of the Eclipse project). Demonstrate that the handshake will fail. The client will not accept the servers certificate. (it is signed by paul.)

Q5.

Open the cacerts file with keytool. (The password is changeit).

Import your own certificate into cacerts using keytool. (You might need to close it and open it again in keytool before it becomes visible.) You are now a recognised Certificate Authority.

Q6.

Run the SSL server and client again. Now the SSL handshake should succeed.