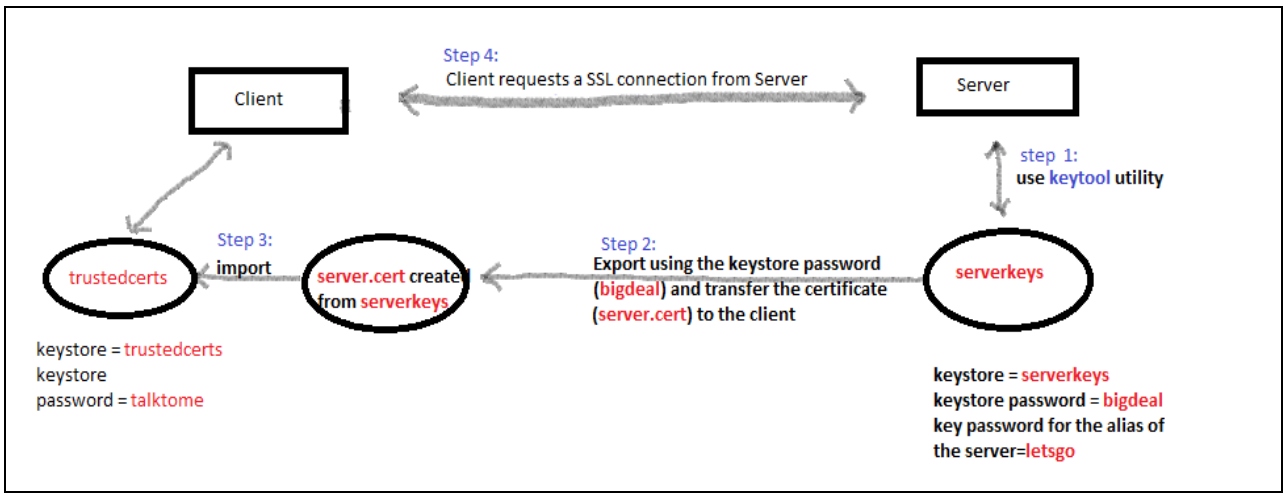
Using SSLSocket and SSLServerSocket for Secure Connection

- Uses Secure Socket Layer (SSL) technology which has been widely been used for online business and financial applications.

- SSL was part of Java Secure Socket Exrension (JSSE), and now has been integrated with the latest Java SDK since Java 2 SDK (version 1.4).

- Below is a diagram to summarize the steps required for supporting SSL connection (Server Authentication) between Java client and server programs:



Here are the steps required:

1. Go to the Server's directory at the command prompt, type:
   > keytool -genkey -keystore serverkeys -keyalg rsa -alias goody

   //It will generate a certificate to be referenced by the alias goody, and the following steps
   //will show you how the certificate is created:

   Enter keystore password: bigdeal
   What is your first and last name?
   [unkown]: cosc.okanagan.bc.ca
   What is the name of your organizational unit?
   [unkown]: cosc
   What is the name of your organization?
   [unkown]: OC
   What is the name of your city or locality?
   [unkown]: Kelowna
   What is the name of your state or province?

[unkown]: BC
What is the two-letter country code for this unit?
[unkown]: CA
Is CN=cosc.okanagan.bc.ca, OU= cosc, ...C = CA correct?
[no]: yes
Enter key password for <goody>
<RETURN if same as keystore password): letsgo

- Now we can run the Server and test to see if the Server is sending out the certificate when requested with a browser by entering the URL: https://localhost:8888

2. Next let's export the server's certificate using keytool inside the server's directory:
> keytool -export -keystore serverkeys -alias goody -file server.cert

Enter keystore password: bigdeal
Certificate stored in file <server.cert>

// copy the server.cert file to the client's directory
- copy server.cert ..\client\

3. Create a new keystore (trustedcerts) and import server.cert certificate into it inside the Client's directory:
> keytool -import -keystore trustedcerts -alias goody -file server.cert

Enter keystore password: talktome
Owner: CN=cosc.okanagan.bc.ca, OU= cosc, ...

Serial number :8ddf826b
Valid from : Mon October 3, 2011 .....
Certificate fingerprint:
MD5: 36: 35: 4D: 3A: .....
SHA1: BB:7C:A2:25: .....
Trust this certificate? [no]: yes
Certificate was added to keystore.

4. Run the client program and inform it where to look for the certificate:
- java -Djavax.net.ssl.trustStore=trustedcerts SSLDateClient
or
- java SSLDateClient1 //What is special about SSLDateClient1 ?