# 12.1 - Creating a Certificate Signing Request (CSR)

### To Generate a Certificate Signing Request (CSR) from your SHRINE keystore

Please run the following command:

```
$ keytool -certreq -alias $KEYSTORE_ALIAS -keyalg RSA -file shrine-client.csr -keypass $KEYSTORE_PASSWORD -
storepass $KEYSTORE_PASSWORD -keystore $KEYSTORE_FILE
```

This should output a file called **shrine-client.csr** (feel free to pick another more descriptive name instead), which should then be sent off to the network hub administrator. The hub administrator will review the CSR and check for validity. The most common reason for rejection of a CSR is an invalid CN value. The CN of a certificate should match the publicly-accessible hostname of the machine that will use the certificate. Using other values can cause problems with verifying the identity of that host. If the CSR is validated, the Hub administrator will sign the request and send back the signed certificate in the form of a .crt file. You can check the CN of your CSR file before sending by running this command:

```
$ openssl req -in shrine-client.csr -subject -noout | sed 's~^.*CN=~~'
```