SHRINE 3.2.1 Chapter 12 - Setting Up the SHRINE Keystore

SHRINE utilizes a Java keystore to house certificates that are signed by the Network Hub to encrypt or "sign" queries when they are sent through the network.

To Generate a New Keystore

To generate a new keystore, run the following command (on one line) within the /opt/shrine/ directory. Please use your own values wherever you see $variables.

Most importantly, ensure that $KEYSTORE_ALIAS matches the publicly-accessible hostname of the machine that will be using this keystore.

```
$ keytool -genkeypair -keysize 2048 -alias $KEYSTORE_ALIAS -dname "CN=$KEYSTORE_ALIAS, OU=$KEYSTORE_HUMAN,
O=SHRINE Network, L=$KEYSTORE_CITY, S=$KEYSTORE_STATE, C=$KEYSTORE_COUNTRY" -keyalg RSA -keypass
$KEYSTORE_PASSWORD -storepass $KEYSTORE_PASSWORD -keystore $KEYSTORE_FILE -storetype pkcs12 -validity 7300
```

For example, a sample site might run this:

```
$ keytool -genkeypair -keysize 2048 -alias shrine-example.harvard.edu -dname "CN=shrine-example.harvard.edu,
OU=SHRINE Example, O=SHRINE Network, L=Boston, S=MA, C=US" -keyalg RSA -keypass password -storepass password -
keystore shrine.keystore -storetype pkcs12 -validity 7300
```

This will generate a shrine.keystore file within the /opt/shrine directory. You can then verify the creation of the keystore by running:

```
$ keytool -list -keystore shrine.keystore -storepass password
```

You used keytool to create a new keystore - but you have not yet created any certificates. You have created a private key that you will use to generate a certificate signing request (CSR) in the next step to send to the hub administrator. That admin will create a certificate for you in return. (The "genkeypair" keyword is a misnomer.)