

## 12.3 - Configuring Certificates

After importing all the certificates into your SHRINE keystore, you will need to configure two places to utilize the new keystore:

The first place, is in the keystore section within shrine.conf:

```
keystore {  
    file = "/opt/shrine/shrine.keystore"  
    password = "password"  
    privateKeyAlias = "$KEYSTORE_ALIAS"  
    keyStoreType = "JKS"  
    caCertAliases= [ "HUB_CA_CERT_ALIAS" ]  
}
```

This is to make sure SHRINE uses the signed certificate to sign queries going out from your site.

The second place, is in the keystore section within /opt/shrine/tomcat/conf/server.xml:

```
<Connector port="6443" protocol="org.apache.coyote.http11.Http11NioProtocol"  
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"  
    clientAuth="false" sslProtocol="TLS"  
    keystoreFile="/opt/shrine/shrine.keystore"  
    keystorePass="password"  
    keyAlias="$KEYSTORE_ALIAS" />
```

This is to configure Tomcat to use the same signed certificate to serve your site's HTTPS traffic.

After making changes to these two files, please restart Tomcat services.