

Chapter 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" ]  
}
```

SHRINE will use privateKeyAlias to find the signed certificate to sign queries going out from your site, and caCertAliases to verify queries before running them.