**JAVA SSL:**

The specific keys you have to set are below:

**javax.net.ssl.keyStore**- Location of the Java keystore file containing an application process's own certificate and private key. On Windows, the specified pathname must use forward slashes, /, in place of backslashes.

**javax.net.ssl.keyStorePassword** - Password to access the private key from the keystore file specified by javax.net.ssl.keyStore. This password is used twice: To unlock the keystore file (store password), and To decrypt the private key stored in the keystore (key password).

**javax.net.ssl.trustStore** - Location of the Java keystore file containing the collection of CA certificates trusted by this application process (trust store). On Windows, the specified pathname must use forward slashes, /, in place of backslashes, \.

If a trust store location is not specified using this property, the SunJSSE implementation searches for and uses a keystore file in the following locations (in order):

1. $JAVA\_HOME/lib/security/jssecacerts
2. $JAVA\_HOME/lib/security/cacerts

**javax.net.ssl.trustStorePassword** - Password to unlock the keystore file (store password) specified by javax.net.ssl.trustStore.

**javax.net.ssl.trustStoreType** - (Optional) For Java keystore file format, this property has the value jks (or JKS). You do not normally specify this property, because its default value is already jks.

**javax.net.debug** - To switch on logging for the SSL/TLS layer, set this property to ssl.