**How to setup MariaDB SSL and secure connections from clients**

Link 1: <https://www.cyberciti.biz/faq/how-to-setup-mariadb-ssl-and-secure-connections-from-clients/>

Link 2: <https://github.com/properssl/java-jdbc-mariadb/blob/master/src/test/java/org/properssl/MariaDBJdbcTest.java>

Link 3: <https://stackoverflow.com/questions/875467/java-client-certificates-over-https-ssl>

Link 4: <http://emo.sourceforge.net/cert-login-howto.html>

1. Install MariaDB server/client on Ubuntu/Debian Linux

sudo apt-get install mariadb-server mariadb-client

1. Secure MariaDB

mysql\_secure\_installation

1. Create the CA certificate in a specified directory

sudo openssl genrsa 2048 > ca-key.pem

sudo openssl req -new -x509 -nodes -days 365000 -key ca-key.pem -out ca-cert.pe

You should now have ca-cert.pem and ca-key.pem

1. Create the server certificate

Create the server key: (NOTE: THE COMMON NAME HAS TO BE DOMAIN NAME, EX: localhost)

sudo openssl req -newkey rsa:2048 -days 365000 -nodes -keyout server-key.pem -out server-req.pem

Process the server RSA key:

sudo openssl rsa -in server-key.pem -out server-key.pem

Sign the server certificate:

sudo openssl x509 -req -in server-req.pem -days 365000 -CA ca-cert.pem -CAkey ca-key.pem -set\_serial 01 -out server-cert.pem

1. Create the client certificate

Create the client key: (NOTE: THE COMMON NAME HAS TO BE DOMAIN NAME, EX: localhost)

sudo openssl req -newkey rsa:2048 -days 365000 -nodes -keyout client-key.pem -out client-req.pem

Process client RSA key:

**sudo openssl rsa -in client-key.pem -out client-key.pem**

Sign the client certificate:

sudo openssl x509 -req -in client-req.pem -days 365000 -CA ca-cert.pem -CAkey ca-key.pem -set\_serial 01 -out client-cert.pem

1. Verify the certificates:

openssl verify -CAfile ca-cert.pem server-cert.pem client-cert.pem

(NOTE: There should not be any error and must get OK answer for server and client certificates)

1. Configure MariaDB server and client to use SSL (LOOK AT THE LINK 1)
2. Configure Java to use SSL to connect with MariaDB

Create the PKCS#12 Certificate from the client-certificate and client-key

openssl pkcs12 -export -in client-cert.pem -inkey client-key.pem -out clientcertificate.p12 -name "MariaDB Client Certificate"

Create the PKCS#12 Certificate from the server-certificate and server-key

openssl pkcs12 -export -in server-cert.pem -inkey server-key.pem -out servercertificate.p12 -name "MariaDB Server Certificate"

Import the self-signed server certificate into a truststore:

keytool -import -alias mariadbserver -file servercertificate.p12 -storepass $PASS -keystore mariadbserver.keystore

Set the proper properties in Java:

Properties info = new Properties();  
info.setProperty("useSSL", "true");  
System.*setProperty*("javax.net.ssl.keyStoreType", "pkcs12");  
System.*setProperty*("javax.net.ssl.trustStoreType", "jks");  
System.*setProperty*("javax.net.ssl.keyStore", "/Path/to/clientcertificate.p12");  
System.*setProperty*("javax.net.ssl.trustStore", "/Path/to/mariadbserver.keystore");

System.*setProperty*("javax.net.ssl.keyStorePassword", "$YOUR-PASSWORD”);