http://blog.regolit.com/2010/02/16/personal-ca-and-self-signed-certificates

https://github.com/chef-cookbooks/openssl/issues/37

http://cyber01.ru/manuals/rabota-mysql-s-ssl/

Установить в настройках соединения с сервером:

?autoReconnect=true;useSSL=false

------- Создание сертификата для СА (центар сертификации)-----------

- Создать приватный ключ CA (key):

openssl genrsa -des3 -out ca.key 4096

- Создать публичный ключ CA (crt):

openssl req -new -x509 -days 365 -key ca.key -out ca.crt

------- Создание сертификата для сайта -------------

- Создать ключ:

openssl genrsa -out server.key 4096

- Создать запрос на подпись:

openssl req -new -key server.key -config openssl-csr.cnf -reqexts req\_ext -out server.csr

-Подписать ключ (выполняется на стороне СА):

НУЖНО ИЗМЕНИТЬ СЕРИЙНЫЙ НОМЕР!

openssl x509 -req -days 365 -CA ca.crt -CAkey ca.key -set\_serial 004 -extfile openssl-csr.cnf -extensions req\_ext -in server.csr -out server.crt

- Преобразовать подписанный сертификат в pkcs12:

openssl pkcs12 -export -in server.crt -inkey 47895.key -out server.p12 -name escom -CAfile ca.crt -caname root

openssl pkcs12 -export -in server.crt -inkey server.key -out server.p12 -name escom -CAfile ca.crt -caname root

- Установить сертификат pkcs12 в хранилище jks:

keytool -importkeystore -deststorepass Qwerty -destkeypass Qwerty -destkeystore wildfly.jks -srckeystore server.p12 -srcstoretype PKCS12 -srcstorepass qwerty -alias escom

Посмотреть сертификат:

openssl req -noout -text -in server.csr