Creating your keystorefile for SSL authentication

You can connect to a running server through a SSL tunnel by specifying the location of the trusted keystore file to `org.apache.geronimo.keyStoreTrustStorePasswordFile`, especially when you connect to a Geronimo server with JCsonle. The default SSL keystore of the Geronimo server is `geronimo-default`, which locates at `/var/security/keystores/` directory.

Follow the instructions below to complete a SSL connection to the Geronimo server.

1. Enable a system plug-in named `org.apache.geronimo.framework/jmx-security//car` using **start** sub-command or via the administrative console on the server.
2. Create a key file containing the password pairs used to connect to the server, which will be like:

   keystorePasswordfile.key

   keyStorePassword=*secret*
   trustStorePassword=*secret*

   Where *secret* is the default password of keystore `geronimo-default` in the server. For better security, use **encrypt** sub-command to encrypt the plain text password in the file. By default, the content of `keystorePasswordfile.key` file is from `/var/config/config-substitutions.properties` file.
3. Save the file to your preferred location such as *myDir* and then export the location of keystorePasswordfile.key file to `org.apache.geronimo.keyStoreTrustStorePasswordFile`.
   ${renderedContent}
   ${renderedContent}
4. Initiate a connecting request to the server via SSL, then you will see the connection is successfully acquired. For example, using available commands on the server that support **--secure** option.