This directory contains test certificates used for testing ssl handling.

These keystores and certificates can be used via applying the `elasticsearch.test-with-ssl` plugin.

The generated certificates are valid till 05. Jun 2030.

The certificates are generated using catch-all SAN in the following procedure:

1. Generate the node's keystore: `keytool -genkey -alias test-node -keystore test-node.jks -keyalg RSA -keysize 2048 -validity 3654 -dname CN="Elasticsearch Build Test Infrastructure" -keypass keypass -storepass keypass -ext san=dns:localhost,dns:localhost.localdomain,dns:localhost4,dns:localhost4.localdomain4,dns:localhost6,dns:localhost6.localdomain`

2. Generate the client's keystore: `keytool -genkey -alias test-client -keystore test-client.jks -keyalg RSA -keysize 2048 -validity 3654 -dname CN="Elasticsearch Build Test Infrastructure" -keypass keypass -storepass keypass -ext san=dns:localhost,dns:localhost.localdomain,dns:localhost4,dns:localhost4.localdomain4,dns:localhost6,dns:localhost6.localdomain`

3. Export the node's certificate: `keytool -export -alias test-node -keystore test-node.jks -storepass keypass -file test-node.crt`

4. Import the node certificate in the client's keystore: `keytool -import -alias test-node -keystore test-client.jks -storepass keypass -file test-node.crt -noprompt`

5. Export the client's certificate: `keytool -export -alias test-client -keystore test-client.jks -storepass keypass -file test-client.crt`

6. Import the client certificate in the node's keystore: `keytool -import -alias test-client -keystore test-node.jks -storepass keypass -file test-client.crt -noprompt`

7. Convert the node's keystore to PKCS#12 temporarily so that we can export the private key (as keytool doesn't allow this) `keytool -importkeystore -srckeystore test-node.jks -srcstorepass keypass -destkeystore test-node.p12 -deststoretype PKCS12 -deststorepass keypass`

8. Export the node's private key `openssl pkcs12 -in test-node.p12 -passin pass:keypass -nocerts -passout pass:test-node-key-password -out test-node.key`

9. Convert the client's keystore to PKCS#12 temporarily so that we can export the private key (as keytool doesn't allow this) `keytool -importkeystore -srckeystore test-client.jks -srcstorepass keypass -destkeystore test-client.p12 -deststoretype PKCS12 -deststorepass keypass`

10. Export the client's private key `openssl pkcs12 -in test-client.p12 -passin pass:keypass -nocerts -passout pass:test-client-key-password -out test-client.key`