Cheatography

JAVA keytool Cheat Sheet

by TME520 (TME520) via cheatography.com/20978/cs/15513/

trustStore, keyStore

The only difference between trustStores and keyStores is what they store:
- *trustStore*: certificates from other parties that you expect to communicate with, or from Certificate Authorities that you trust to identify other parties,
- *keyStore*: private keys, and the certificates with their corresponding public keys.

Learn more: Javarevisited - Difference between trustStore and keyStore in Java

How do you spot a root CA ?

- Root certificates are self-signed,
- Self-signed certificates have the same issuer and subject,
- The "CA" field is set to true.

Create, generate

Generate a Java keystore and key pair	keytool -genkey -alias mydomain -keyalg RSA -keystore keystore.jks -keysize 2048
Generate a keystore and self-signed certificate	keytool -genkey -keyalg RSA -alias selfsigned -keystore keystore.jks -storepass password -validity 360 -keysize 2048
Generate a certificate signing request (CSR) for an existing Java keystore	keytool -certreq -alias mydomain -keystore keystore.jks -file mydomain.csr

Import, export

Import a root or intermediate CA certificate to an existing Java keystore	keytool -import -trustcacerts -alias root -file Thawte.crt -keystore keystore.jks
Import a signed primary certificate to an existing Java keystore	keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore keystore.jks
Import New CA into Trusted Certs	keytool -import -trustcacerts -file /path/to/ca/ca.pem -alias CA_ALIAS -keystore $JAVA_HOME/jre/lib/security/cacerts

Check, list

Check a stand-alone certificate	keytool -printcert -v -file mydomain.crt
Check which certificates are in a Java keystore	keytool -list -v -keystore keystore.jks
Check a particular keystore entry using an alias	keytool -list -v -keystore keystore.jks -alias mydomain
List Trusted CA Certs	keytool -list -v -keystore $JAVA_HOME/jre/lib/security/cacerts

Delete

Delete a certificate from a Java Keytool keystore	keytool -delete -alias mydomain -keystore keystore.jks

Passwords

Change a Java keystore password	keytool -storepasswd -new new_storepass -keystore keystore.jks

The password must be provided to all commands that access the keystore contents. For such commands, if a *-storepass* option is not provided at the command line, the user is prompted for it.

By **TME520** (TME520)
cheatography.com/tme520/
tme520.com

Published 18th April, 2018.
Last updated 18th April, 2018.