Java Applets

Notes

Author	Faram Khambatta
Created	2011-02-25
Last updated	2011-02-25

Digitally signing a jar

- Any applet that performs restricted ops must have its jars digitally signed.
- **keytool -genkey** generates public/private key pair wrapped in self-signed certificate.
- **keystore** is a file containing key certs. Each entry has an **alias** that refers to it.
- **keytool -import** imports certs from a file.
- **keytool -export** exports cert to file. Cert contains public key of the public/private key pair.
- **keytool -list** lists entries in keystore.
- **keytool -printcert -file xyz.cer** displays cert in given file.
- **keytool -delete** deletes given alias.
- Default alias name is **mykey**.
- **jarsigner xyz.jar alias** signs jar with private key of given alias.
- After signing, META-INF of the jar contains a .SF and .RSA files. RSA file contains signature (derived using private key on contents of jar) and public key cert (corresponding to encoding private key).
- **jarsigner -verify xyz.jar** verifies jar.