

How to Sign Java Applets (Using a PKCS#12 format certificate)

Introduction:

Using a PKCS#12 file (AKA: .PFX or .P12) is a very short and simple way of signing applets.

Since certificates generated with a CSR from a Java Key Store (JKS) are restricted to one machine, this option would be ideal when more than one developer needs to sign the code from different stations.

Instructions:

1/. Download and install the Java SE Development Kit (JDK) – It is recommended to register in order to keep updated with latest releases and access to all support pages.

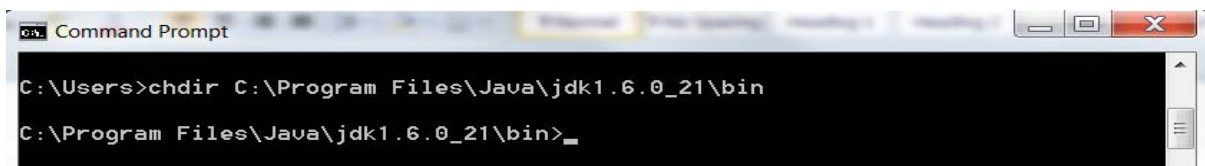
<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

2/. For Vista/Windows 7, you will need to be logged in as the **Administrator**.

3/. Run the “Command Prompt”- **Start -> Run -> cmd**

4/. Browse to the Java directory- **chdir C:\Program Files\Java\jdk1.6.0_21\bin**

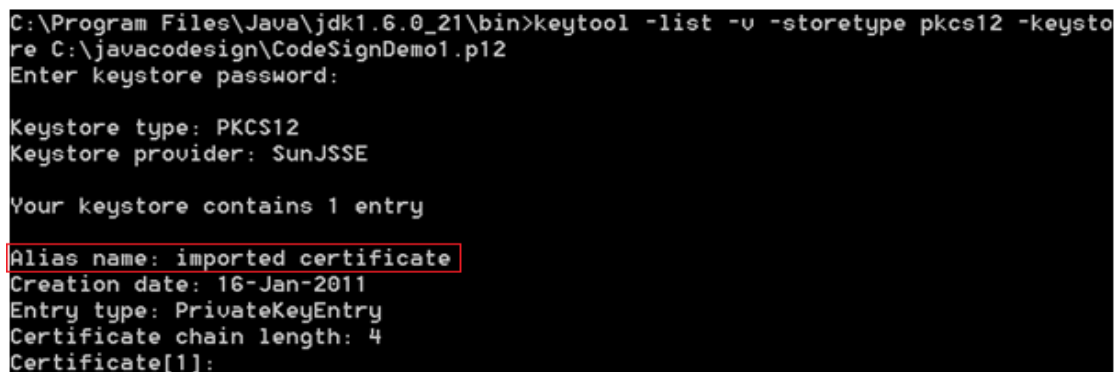
(**Note:** the jdk1.6.0_21 corresponds to the Java version and it is likely to be different for you).



```
Command Prompt
C:\Users>chdir C:\Program Files\Java\jdk1.6.0_21\bin
C:\Program Files\Java\jdk1.6.0_21\bin>
```

5/. Retrieve your PFX file (See our Java CodeSigning FAQ’s if you are unsure how to generate a certificate in this Extension).

6/. Test that your PFX file is accessible from Keytool and retrieve the certificate’s alias name:



```
C:\Program Files\Java\jdk1.6.0_21\bin>keytool -list -v -storetype pkcs12 -keystore C:\javacodesign\CodeSignDemo1.p12
Enter keystore password:
Keystore type: PKCS12
Keystore provider: SunJSSE

Your keystore contains 1 entry
Alias name: imported certificate
Creation date: 16-Jan-2011
Entry type: PrivateKeyEntry
Certificate chain length: 4
Certificate[1]:
```

(**Tip:** Drag the PKCS#12 certificate to the shell after “-keystore” to avoid path and extension errors)

7a/. If no errors are experienced, then sign the JAR file using:

```
C:\Program Files\Java\jdk1.6.0_21\bin>jarsigner -storetype pkcs12 -keystore C:\javacodesign\CodeSignDemo1.p12 C:\javacodesign\rubik.jar "imported certificate"
Enter Passphrase for keystore:
```

7b/. If you need to add a timestamp to the file, you can do so by including in the command above the function "-tsa" and adding the timestamping URL:

```
C:\Program Files\Java\jdk1.6.0_21\bin>jarsigner -storetype pkcs12 -keystore C:\javacodesign\CodeSignDemo1.p12 C:\javacodesign\rubik.jar "imported certificate" -tsa http://timestamp.globalsign.com/scripts/timestamp.dll
Enter Passphrase for keystore:
```

8/. You can now verify the signed file by using:

```
C:\Program Files\Java\jdk1.6.0_21\bin>jarsigner -verify -verbose -certs C:\javacodesign\rubik.jar

    135 Sun Jan 16 10:56:46 GMT 2011 META-INF/MANIFEST.MF
    256 Sun Jan 16 11:13:32 GMT 2011 META-INF/IMPORTED.SF
   4565 Sun Jan 16 11:13:32 GMT 2011 META-INF/IMPORTED.RSA
      0 Sat Aug 30 09:49:36 BST 2008 META-INF/
smk   13816 Sat Aug 30 09:47:14 BST 2008 rubik.class
```

```
s = signature was verified
m = entry is listed in manifest
k = at least one certificate was found in keystore
i = at least one certificate was found in identity scope

jar verified.
```