SIGN JAVA .JAR FILES WITH A HARDWARE TOKEN-BASED CODE SIGNING CERTIFICATE IN WINDOWS

Signing Java .jar Files with the CLI (Command Line Interface) Command Jarsigner

These instructions are for signing Java .jar files with a code signing or EV code signing installed on a hardware token.

When you use your certificate to sign code, a digital signature is applied to your code. This digital signature boosts customer confidence in the code they are about to download and helps to improve the adoption of your Java applications. Many end-users cancel downloads or installations when they receive a warning that an unknown publisher signed the code.

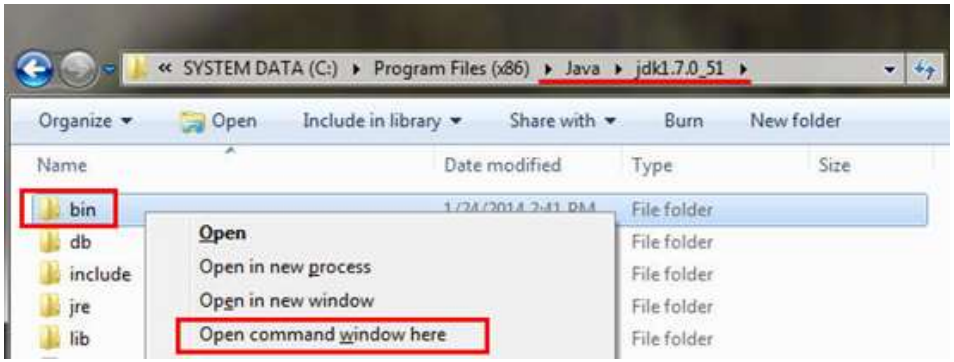
Sign .jar Files using the CLI Command Jarsigner

1. Create a file named eToken.cfg that contains the following lines, and save it to your JDK bin folder (C:\Program Files (x86)\Java\jdk1.7.0_05\bin).

```
name=eToken
library=c:\WINDOWS\system32\eTPKCS11.dll
```

2. In Windows Explorer, navigate to the JDK folder.

3. In the JDK folder, push and hold Shift, right-click on the bin folder, and select Open command window here.



4. To view your code signing or EV code signing certificate and the certificate alias on the token:
   - Plug in your token.
   - Run the following command from the command prompt:

```
Keytool -list -keystore NONE -storetype PKCS11 -providerclass
sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg
enter keystore password: [enter password]
```

   - Sample output:

In this example, **7800FA4C81523ACA** is the certificate alias you use to sign .jar files.

```
Keystore type: PKCS11
Keystore provider: SunPKCS11-eToken
Your keystore contains 1 entry
7800FA4C81523ACA, PrivateKeyEntry,
Certificate fingerprint (SHA2):
XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX
```

5. To use the code signing certificate on the token to sign file.jar, run the following command from the command prompt:

```
jarsigner -tsa http://timestamp.digicert.com -verbose -keystore NONE -
storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -
providerArg ./eToken.cfg "C:\path\to\file.jar" "7800FA4C81523ACA"
```

6. If the command executed successfully, you should see something similar to the following sample output:

```
Enter Passphrase for keystore:

  adding: META-INF/7800FA4C.SF

requesting a signature timestamp

TSA location: http://timestamp.digicert.com

  adding: META-INF/7800FA4C.RSA

  signing: DigiCertTest.class

jar signed.
```

Troubleshooting

- **The program pauses and does not prompt you to enter your password.**
  If you run the keytool or jarsigner command and the program pauses and does not prompt you for a password, unplug the device (token) and plug it back in. Run the command again. This time it should work.

- "*jarsigner error: java.lang.ClassNotFoundException: sun.security.pkcs11.SunPKCS11*"
  This error occurs when using a 64-bit version of the JDK. To eliminate this error, download and use a 32-bit version of the JDK.

- "*jarsigner error: java.lang.RuntimeException: keystore load: load failed*"
  This error may occur if you enter the wrong password.

- "*keytool error: java.security.KeyStoreException: PKCS11 not found*"
  This error occurs if your config file fails to load correctly or the config file points to a file that does not exist (e.g., *library=c:\WINDOWS\system32\eTPKCS11.dll*).

  This error sometimes indicates that the token's device drivers are not installed on your computer. For more information about installing the drivers, see the following knowledge base articles:
  - How to Install the SafeNet Drivers and Client Software (Windows)

- How to download SafeNet Authentication Client

---

digicert®

The most-trusted global provider of high-assurance TLS/SSL, PKI, IoT and signing solutions.