Add Certificate in Java on macOS

Information  
I was using the [ant get task](https://ant.apache.org/manual/Tasks/get.html) to get files from https://www.mobilefish.com/..   
  
The ant task shows the following error message:   
  
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)  
  
To solve this problem you need to add the [SSL certificate](https://www.mobilefish.com/developer/apache/apache_quickguide_install_macos_sierra.html) to the Java keystore.   
  
**Create or download your apple/own certificate:**

**First go to the browser and paste URL: https://api.development.devicecheck.apple.com/**

**Click on the URL LOCK: -->Certificate-->Details-->Copy To File...--> Next -->Next-->Browse-->Select File Location and Give a name "apple-safety"-->Save--Next-->Finish**

# Procedure

1. The Java keystore is located at.  
   Type: **echo $JAVA\_HOME/jre/lib/security**   
     
   The Java keystore is the file: $JAVA\_HOME/jre/lib/security/cacerts   
     
   Note:  
   This means that every installed java version has its own cacerts file.  
   If you use another java version you need to reinstall the certificate.
2. To show all certificates installed in the keystore.  
   Type: **cd $JAVA\_HOME/jre/lib/security**  
   Type: **keytool -list -keystore cacerts**  
   The keystore password is (default): **changeit**   
     
   You should see:  
   **Enter keystore password:   
     
   Keystore type: JKS  
   Keystore provider: SUN   
     
   Your keystore contains 104 entries   
     
   verisignclass2g2ca [jdk], Aug 25, 2016, trustedCertEntry,  
   Certificate fingerprint (SHA1): B3:EA:C4:4  
   :**  
     
   Note:  
   If you want to see more detailed information, add the -v flag.  
   Type: **keytool -list -v -keystore cacerts**
3. Before you import the certificate in the keystore make a backup of the keystore.  
   Type: **cd $JAVA\_HOME/jre/lib/security**  
   Type: **sudo cp cacerts cacerts.orig** /**copy** **cacerts cacerts.orig**
4. Import your self-signed certificate in the keystore.  
   Type: **cd $JAVA\_HOME/jre/lib/security**  
   Type: **sudo keytool -importcert -alias domain-name -file /path/to/certificate.crt -keystore cacerts**   
     
   For example, type:   
   **sudo keytool -importcert -alias apple.developer.com -file /etc/apache2/ssl/sand.mobilefish.crt -keystore cacerts**   
     
   You should see:  
   **Password: your\_root\_password  
   Enter keystore password: changeit  
   Owner: EMAILADDRESS=rd@mobilefish.com, CN=sand.mobilefish.com, OU=Research and development, O=Mobilefish.com, L=Zaandam, ST=Noord-Holland, C=NL  
   Issuer: EMAILADDRESS=rd@mobilefish.com, CN=sand.mobilefish.com, OU=Research and development, O=Mobilefish.com, L=Zaandam, ST=Noord-Holland, C=NL  
   Serial number: 8a7362fba9376522  
   Valid from: Fri Aug 25 13:04:25 CEST 2017 until: Mon Aug 23 13:04:25 CEST 2027  
   :  
   Trust this certificate? [no]: yes  
   Certificate was added to keystore**  
     
   More information about the keytool.  
   Type: **keytool -help**
5. To check the certificate is stored in the keystore:

Type: **cd $JAVA\_HOME/jre/lib/security**  
Type: **sudo keytool -list -keystore cacerts -alias apple.developer.com**   
  
You should see:  
**Enter keystore password: changeit  
sand.mobilefish.com, Aug 26, 2017, trustedCertEntry,  
Certificate fingerprint (SHA1): 35:BB:57:11:56:55:12:FF:23:98:22:11:2D:22:00:24:A2:78:77:2**

1. To see the detailed information, add –v flag:  
     
   Type:  **keytool -v -list -keystore cacerts -alias apple.developer.com**
2. To delete the added certificate from keystore:

Type: **keytool -delete -alias apple.developer.com -keystore cacerts**

1. Note: Before deleting check the total certificate count in the list command.

**For Further Hand shaking Exception**

* 1. Add the chain certificates



# Further Reading

1. <https://www.thesslstore.com/blog/tls-handshake-failed/>
2. Incorrect Certificate Chain—Check all the chain certificate is valid or not.
3. Incorrect SSL/TLS Certificate
4. Incorrect System Time