**Preventing Java warning popups on the eTrustEx applet**

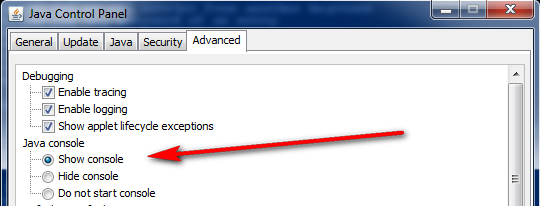
This document provides technical instructions on how to add certificates to your Java keystore in order to prevent Java warning message popups when using the eTrustEx applet. These instructions are made for technical and system administrators only.

**1 Determine the Java version being used in the eTrustEx applet**

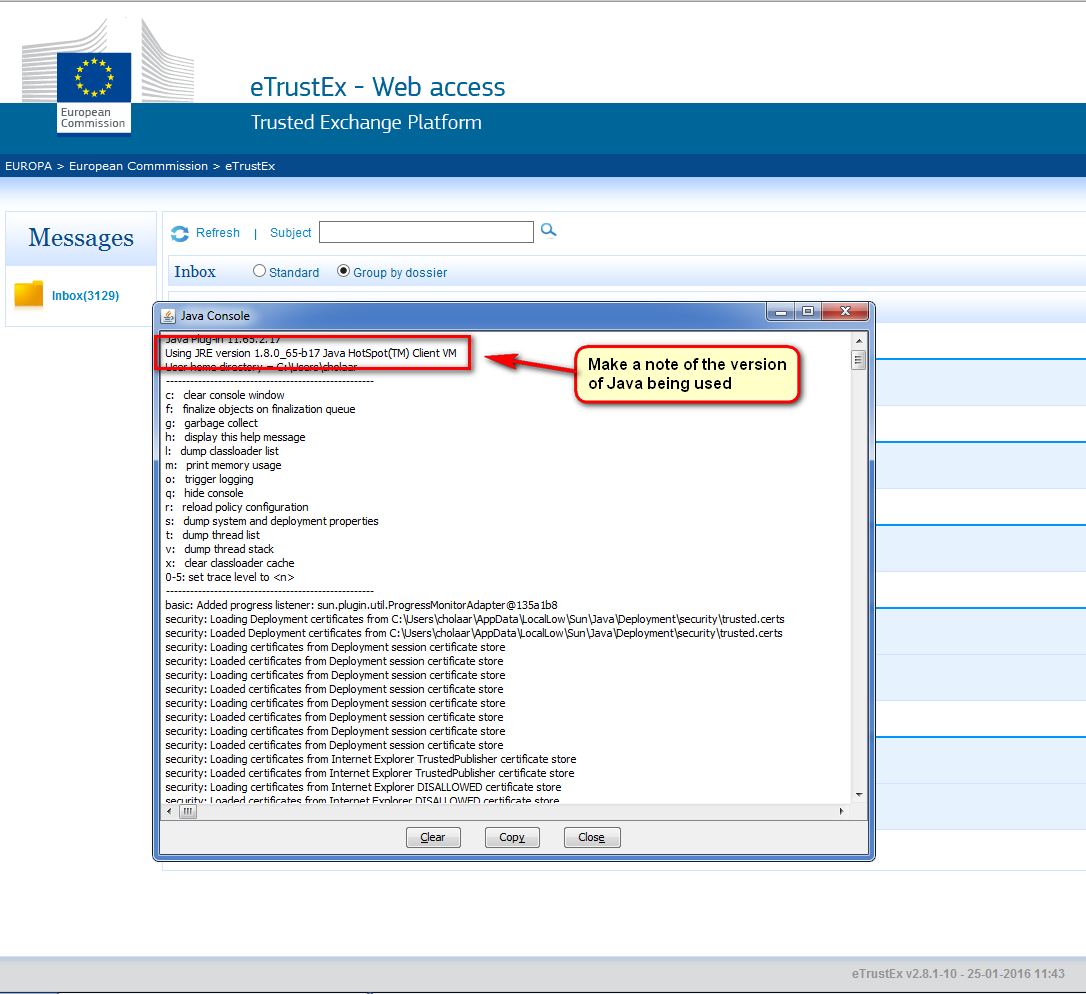
In order to check which version of Java is being used in the application, we need to enable the Java console.

Go to "Control Panel" and then click on the "Java" icon.

Click on the "Advanced" tab and select the option "Show console" in the section "Java console".



Open the eTrustEx web interface and open an incoming message – when the message details appears, the Java console will also open.



In our example, the Java version being used is 1.8.0\_65. Make a note of your Java version as it will be used in the next step.

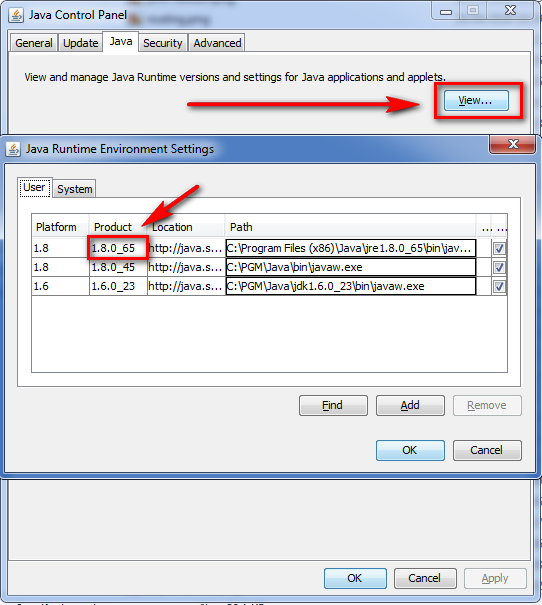
Once you determine the Java version you can revert the Java console setting from above back to "Hide console".

**2 Locate the directory of the Java version being used for eTrustEx**

It may be possible that you have more than one version of Java installed on your computer, we need to identify the location of the actual one being used for eTrustEx.

Go to "Control Panel" and then click on the "Java" icon.

Select the "Java" tab and click on "View".



From the previous step, we determined which version is being used for eTrustEx. In our example we are using Java version 1.8.0\_65.

Select the "Path" of this version and copy it.

In our example the path looks like:

C:\Program Files (x86)\Java\jre1.8.0\_65\bin\javaw.exe

Remove the "bin" and "javaw.exe" parts from the path and then paste it into Windows Explorer to open this location.

ie C:\Program Files (x86)\Java\jre1.8.0\_65\

Now navigate to the following folder inside this location:

C:\Program Files (x86)\Java\jre1.8.0\_65\lib\security

Make a note of this location as it will be used in the next step.

**3 Downloading the certificates**

To download the CommisSign Root certificates of the European Commission you must navigate to the following page:

<http://ec.europa.eu/dgs/human-resources/commissign/index_en.htm>

From this page you need to download the following two certificates:

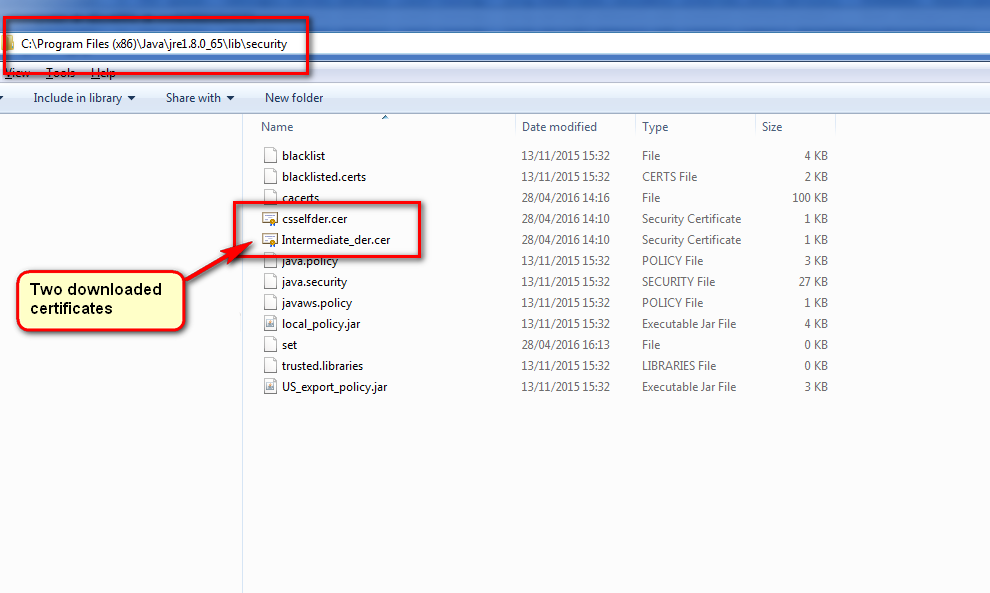
CommisSign root certificate (X.509 Encoded Binary)

and

CommisSign intermediate certificate (X.509 Encoded Binary)

Download both files into the folder from the previous step – in our example the folder location is:

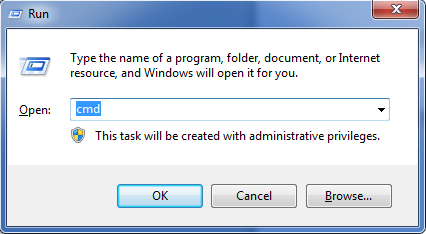
C:\Program Files (x86)\Java\jre1.8.0\_65\lib\security



**4 Adding the European Commission certificates to your Java keystore**

**4.1 Using Command prompt to add the certificates**

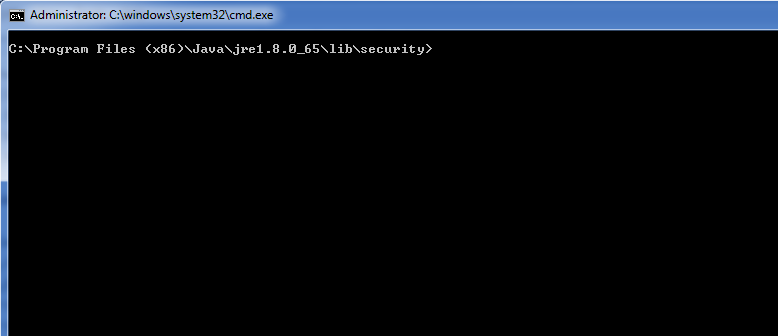
Open a command prompt console – this can be done in many ways – one example is press the "Windows key" + "R" – this opens a "Run" window.



Now type "cmd" to open a command prompt window.

Change the directory in the window to the location of the downloaded certificates from the above step. In our example this is located here:

C:\Program Files (x86)\Java\jre1.8.0\_65\lib\security



In order to include these two certificates in the cacerts, we will have to use the keytool application. If the keytool application is not accessible, please update the Path variable as described below.

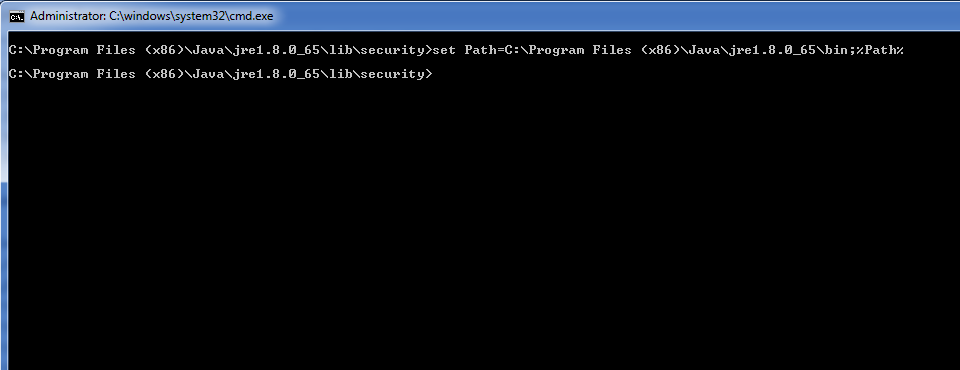
**4.2 – Setting the execution path for the keytool (Optional)**

It is possible that the keytool cannot be executed from the directory mentioned above. In this case we need to manually set the path to the keytool, in order to execute the command to add the certificates to the keystore.

Type the following:

set Path=C:\Program Files (x86)\Java\jre1.8.0\_65\bin;%Path%

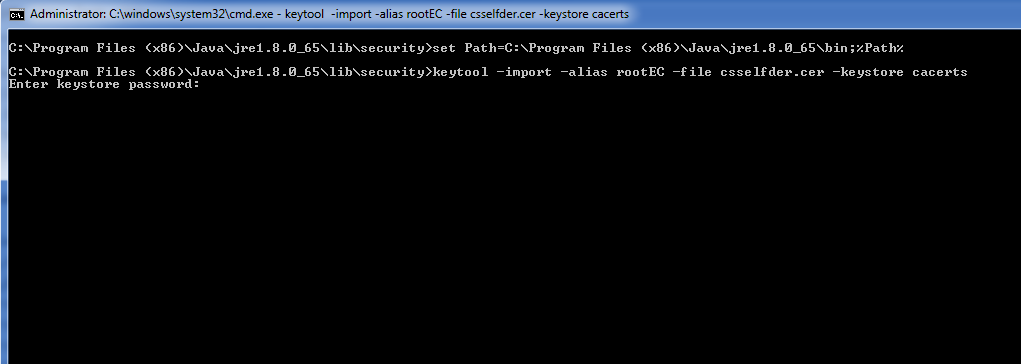
Note that the part in red is also derived from the location of your Java path.



**4.3 Adding the certificates to the the keystore**

Type the following:

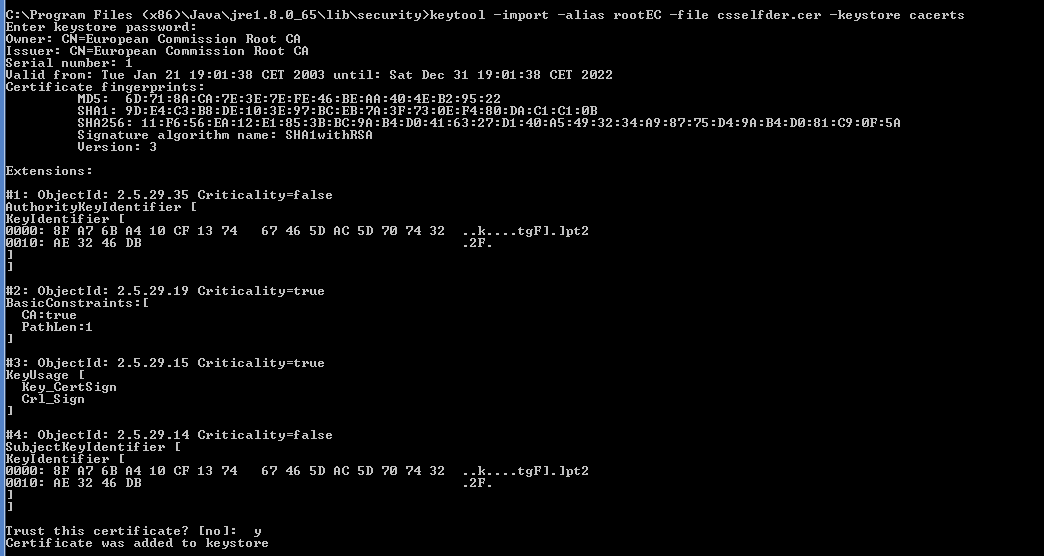
keytool -import -alias rootEC -file csselfder.cer -keystore cacerts



You are now prompted to enter a password – enter the password changeit

Then you are prompted to "Trust this certificate?" – type y

The certificate should be successfully added to your keystore.



We need to repeat the process to add the second certificate – type the following:

keytool -import -alias intermEC -file Intermediate\_der.cer -keystore cacerts

You are again prompted to enter a password – enter the password changeit

The second certificate should now also be added to your keystore.

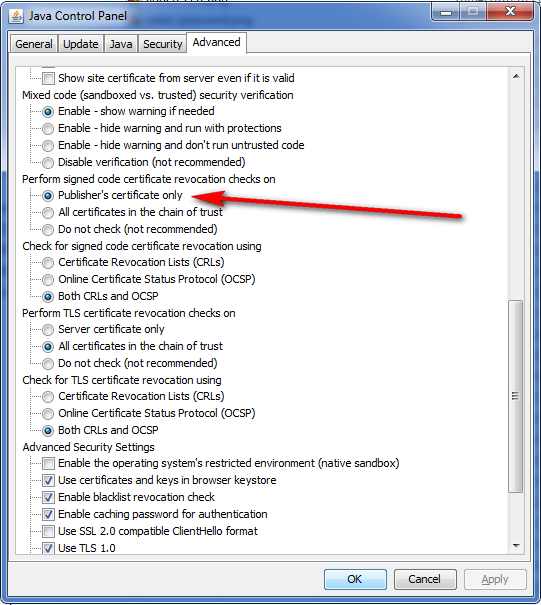
**5 Java configuration**

Finally we need to make one more setting change in the Java.

Go to "Control Panel" and then click on the "Java" icon.

Click on the "Advanced" tab and locate the option "Perform signed code certificate revocation checks on"

Change the value of this option to "Publisher's certificate" only.



Now you should be able to use the eTrustEx application without being presented with Java warning popups.