How to Create a New Timestamping Keystore

The EFT Nominations timestamping functionality requires a CA issued certificate and private key to authenticate with the external timestamping service. This certificate and private key need to be held in a java keystore file. In addition, the CA certificates (both intermediate and root) are required within the keystore file.

Since the certificate issued from the CA is issued as a PKCS#12 file, the following steps need to be undertaken to convert this into a usable format.

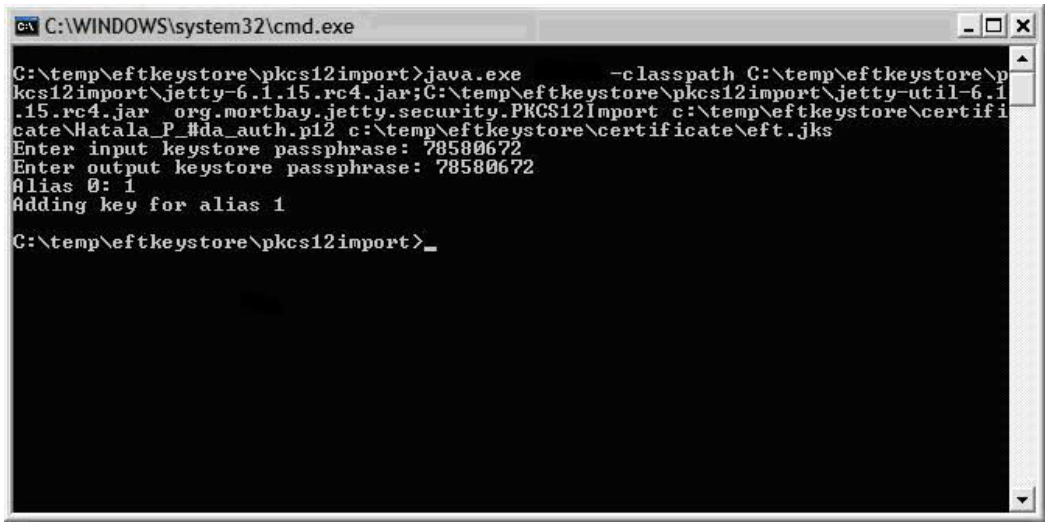
Convert the pkcs12 file to a java keystore

To convert the pkcs#12 file into a keystore, the *PKCS12Import* utility is used. This utility is provided in the attached zip file, and forms part of the Jetty project, further information is available here: http://www.mortbay.org/jetty/. The examples below assume that the zip file is uncompressed into the c:\temp directory.

To convert this file, open a command window and run the following command:

java.exe -classpath C:\temp\eftkeystore\pkcs12import\jetty-6.1.15.rc4.jar;C:\temp\eftkeystore\pkcs12import\jetty-util-6.1.15.rc4.jar org.mortbay.jetty.security.PKCS12Import c:\temp\eftkeystore\certificate\Hatala_P_#da_auth.p12 c:\temp\eftkeystore\certificate\eft.jks

You will need to specify the input certificate password, and then specify the output keystore password.

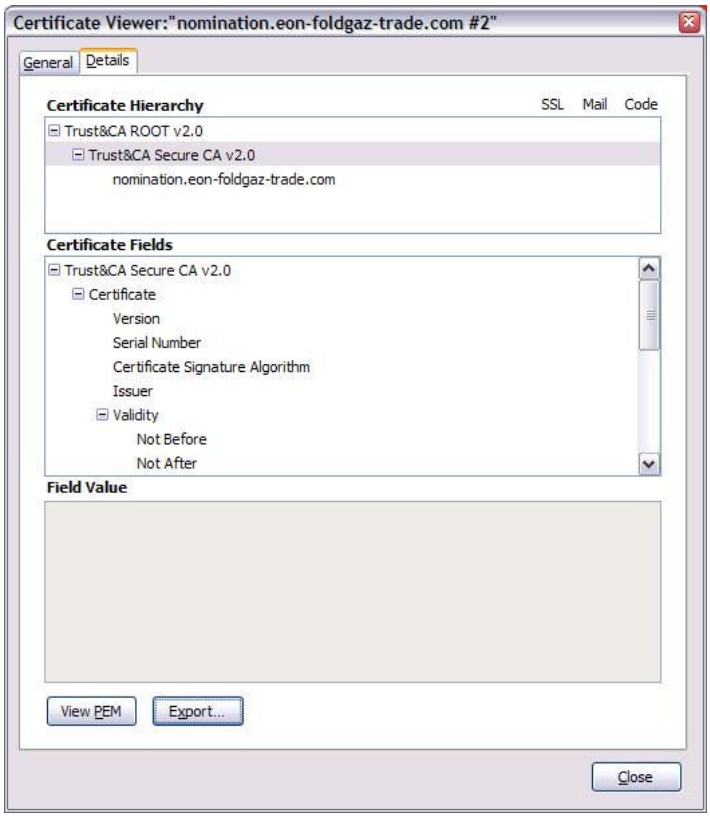


The keystore will be generated in the certificate directory

Install the certificate chain into the keystore

To get the current intermediate and root certificates for the CA, navigate to a site that uses these certificate (for example, https://nomination.eon-foldgaz-trade.com) and export both the root and intermediate certificates individually. In firefox this may be done by:

- Double click on the padlock on the footer bar
- Click on the view certificate button
- Select the details tab



Then, when selecting the root and intermediate certificate in turn:

- Click Export and save into the certificate directory

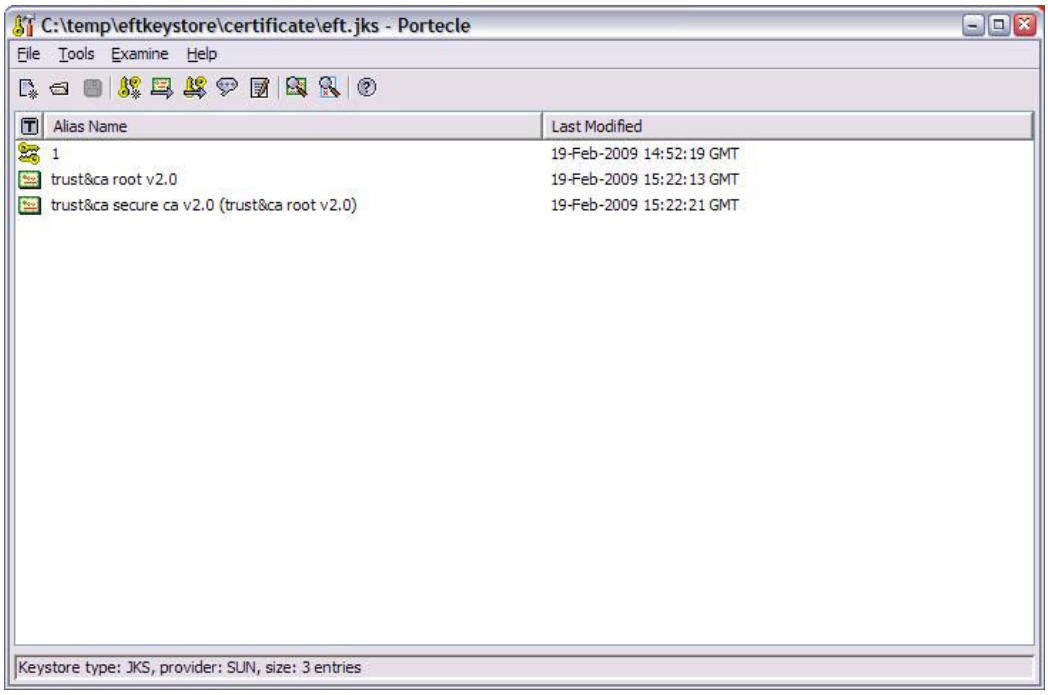
Once this is done, run *Portecle*:

Start -> Run -> c:\temp\eftkeystore\portecle-1.2\portecle.jar

Open the newly generated jks file by clicking file, open Keystore file, navigating to the file and clicking open.

You will be prompted for a password, enter the password used when creating the keystore

Once open import both the root and intermediate certificates by going to Tools, Import Trusted Certificate.



Then save the modified keystore by selecting File, Save Keystore.

Test the keystore

Run the test utility:

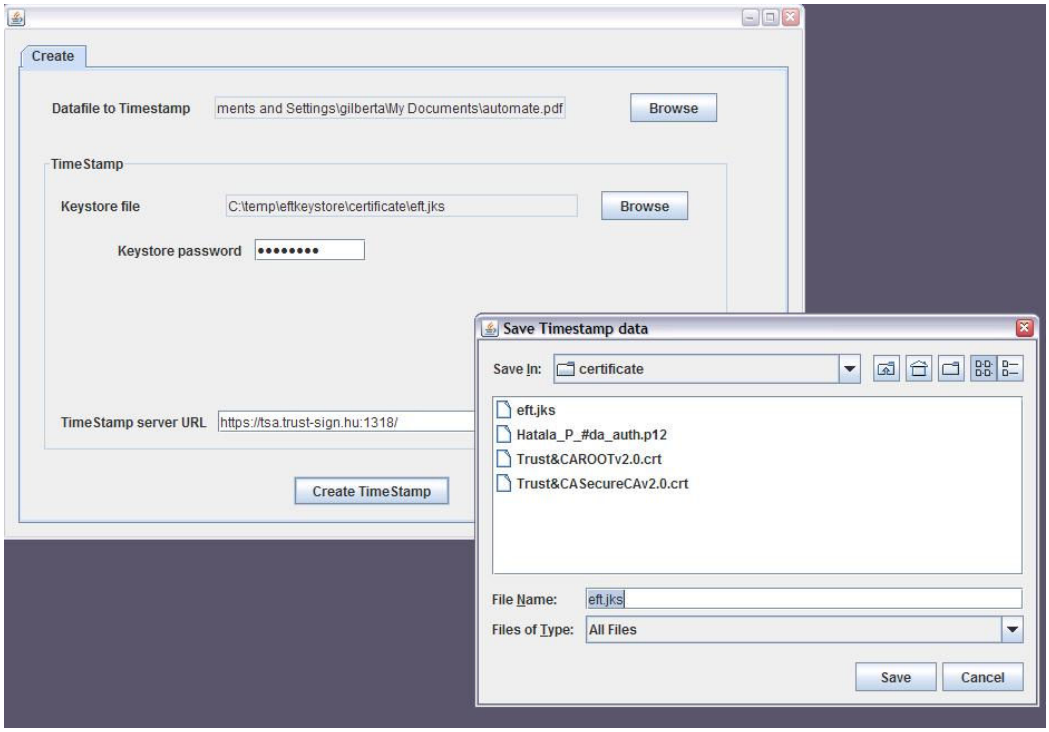
Start -> Run -> C:\temp\eftkeystore\Client\TestClient.exe

- Select any datafile to timestamp

- Select the new keystore file

- Enter the keystore password

- Click Create Timestamp



If a window pops up asking to save the timestamp data, the utility has successfully managed to contact the timestamping service and the keystore is valid. Otherwise, the most likely explanation is that the keystore is invalid.

NOTE - Difficulties may be encountered when running the keystore test utility inside the corporate environment since the timestamping service uses TCP ports outside the usual range. A direct internet connection may be required to test this function