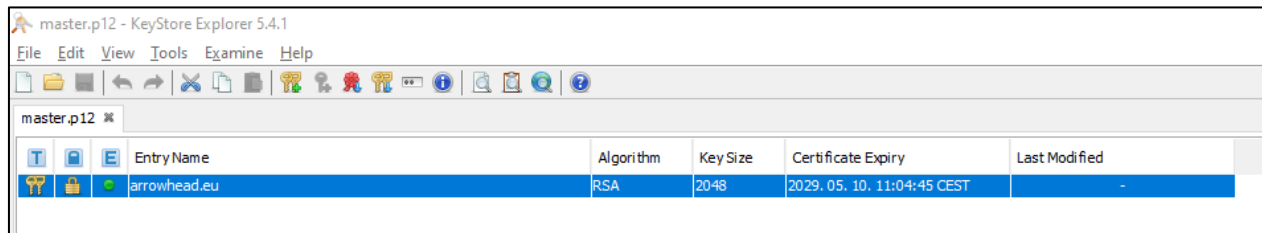


CREATE ARROWHEAD CLOUD SELF SIGNED CERTIFICATE with KeyStore Explorer 5.4.1

KeyStore Explorer is a free GUI tool for managing certificates, which is available for all common operation systems: <https://keystore-explorer.org/downloads.html>

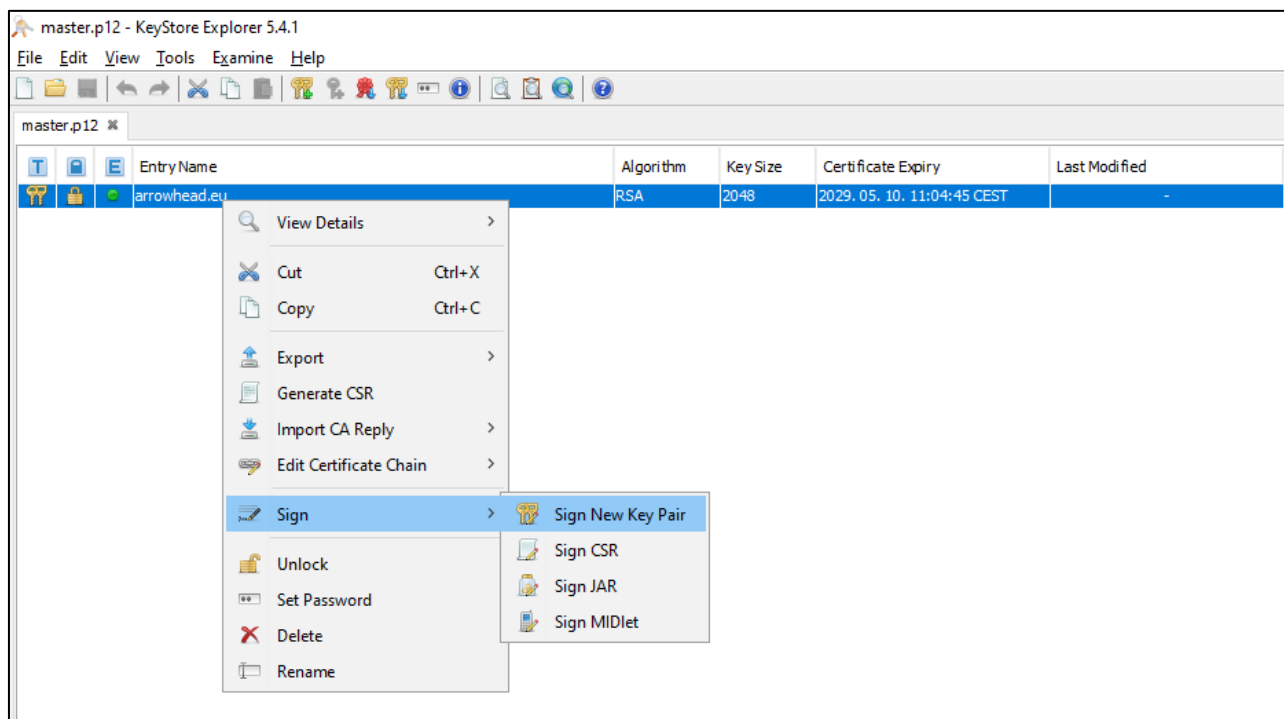
1st STEP:

Open the **master.p12** located in “certificate” folder.



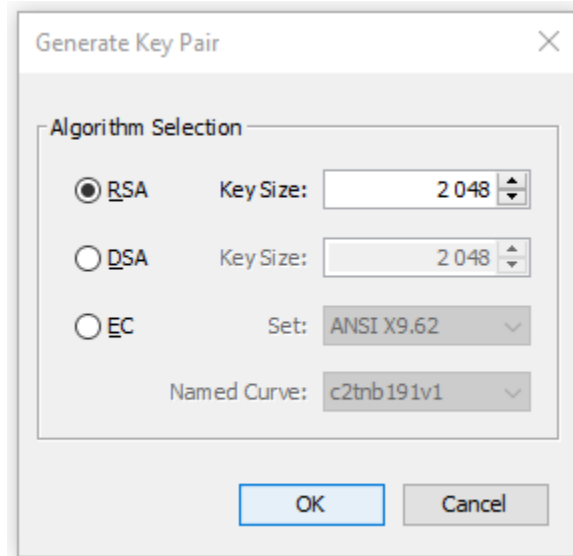
2nd STEP:

Right click on “arrowhead.eu” key pair entry and select “Sign New Key Pair” and enter its password (123456):



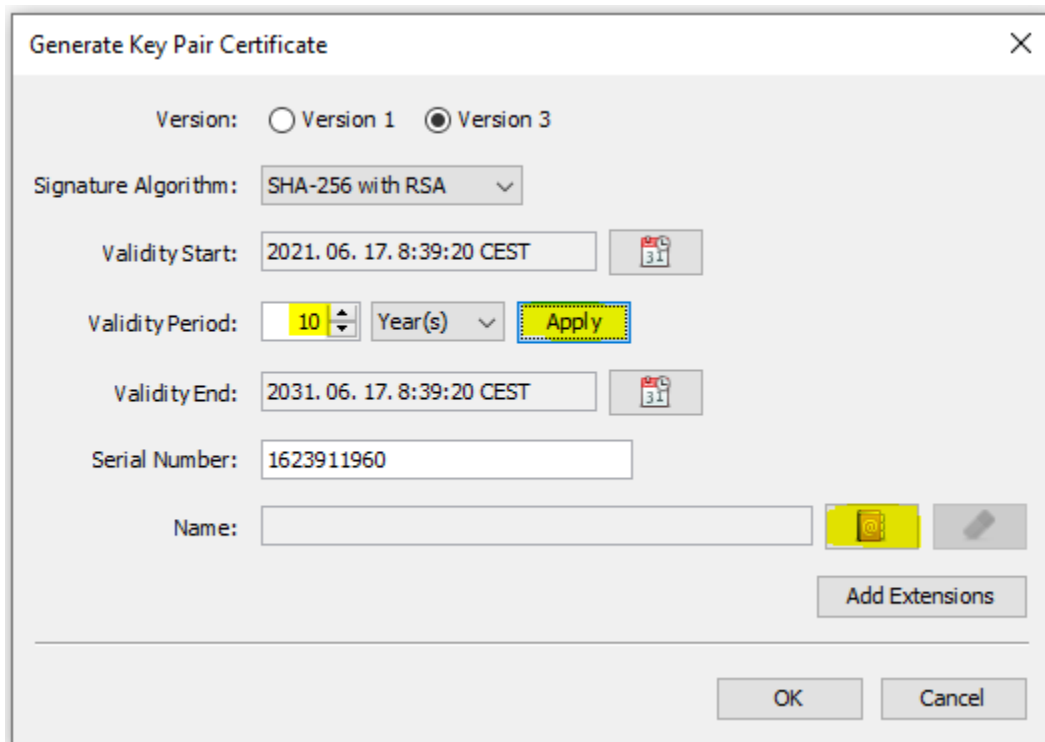
3rd STEP:

Select “RSA” and set “Key Size” to 2048:



4th STEP:

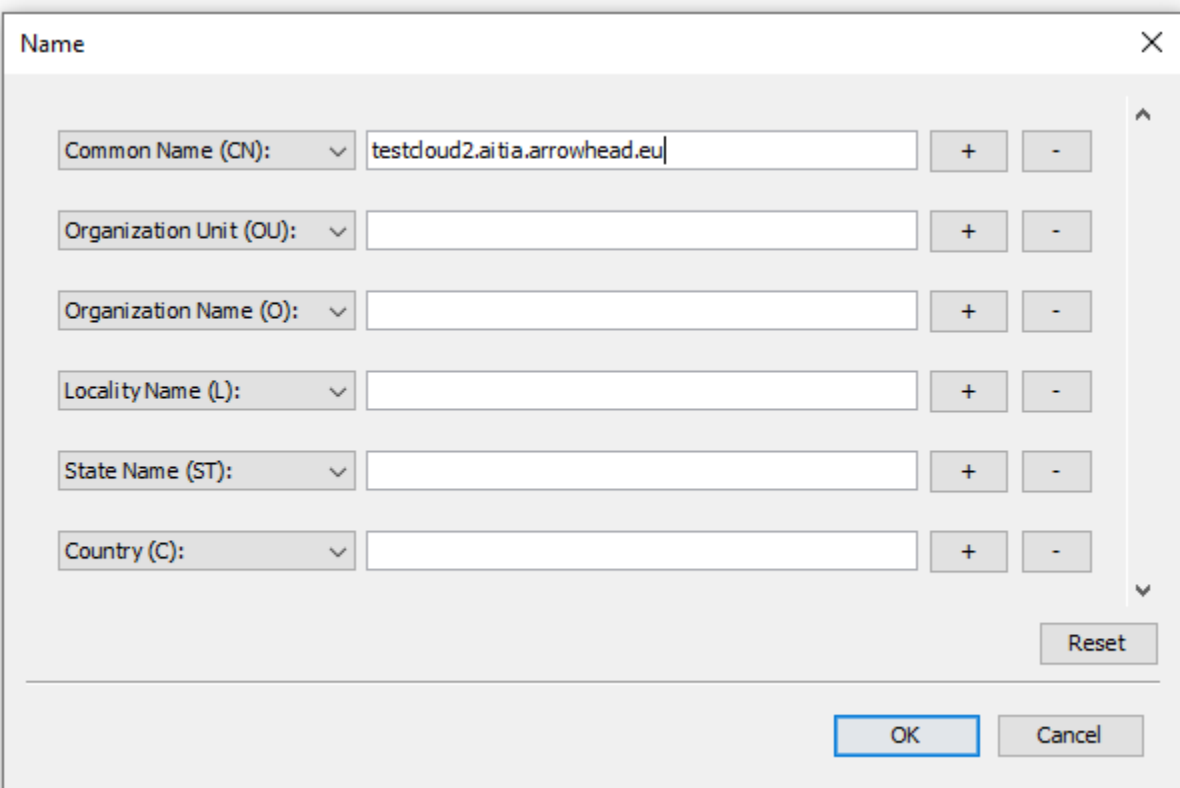
Set the “Validity Period” and hit “Apply”, then click on “Edit name”:



5th STEP:

Fill out the “Common Name (CN)” and hit “OK”. The certificate naming convention have strict rules:

- The different parts are delimited by dots, therefore parts are not allowed to contain any of them.
- A single part is allowed to contain maximum 63 character of letters (english alphabet), numbers and dash (-), and has to start with a letter (also cannot ends with dash).
- A cloud certificate name has to consist of four part and the last two part have to be 'arrow-head' and 'eu'.



The image shows a 'Name' dialog box with a close button (X) in the top right corner. It contains six rows of input fields, each with a dropdown menu on the left and a text box on the right. To the right of each text box are two buttons: a '+' button and a '-' button. The first row is filled with 'testcloud2.aitia.arrowhead.eu' in the 'Common Name (CN)' field. The other five rows are empty. At the bottom right of the dialog box is a 'Reset' button. At the very bottom, centered, are 'OK' and 'Cancel' buttons.

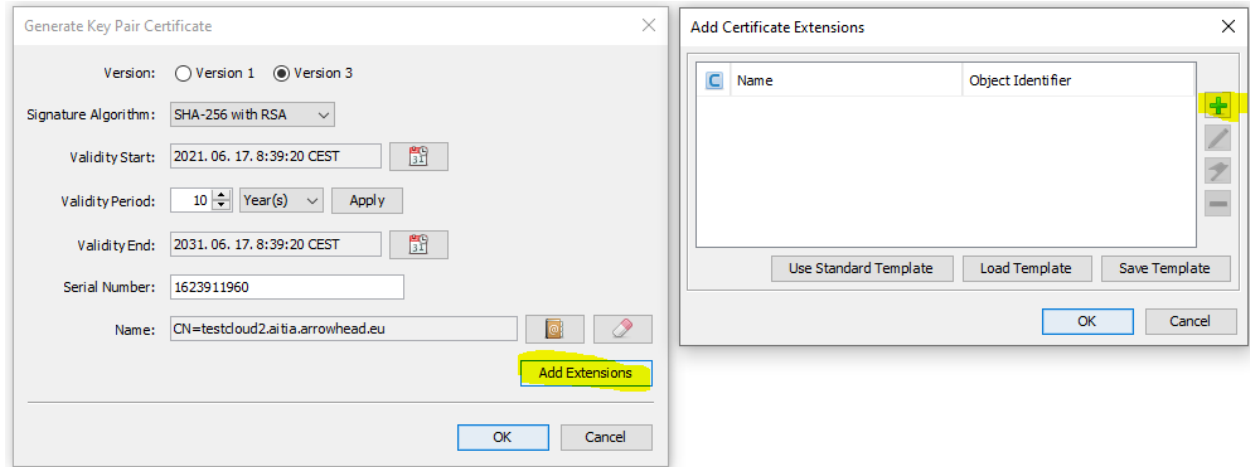
Field	Value	+	-
Common Name (CN):	testcloud2.aitia.arrowhead.eu		
Organization Unit (OU):			
Organization Name (O):			
LocalityName (L):			
State Name (ST):			
Country (C):			

Reset

OK Cancel

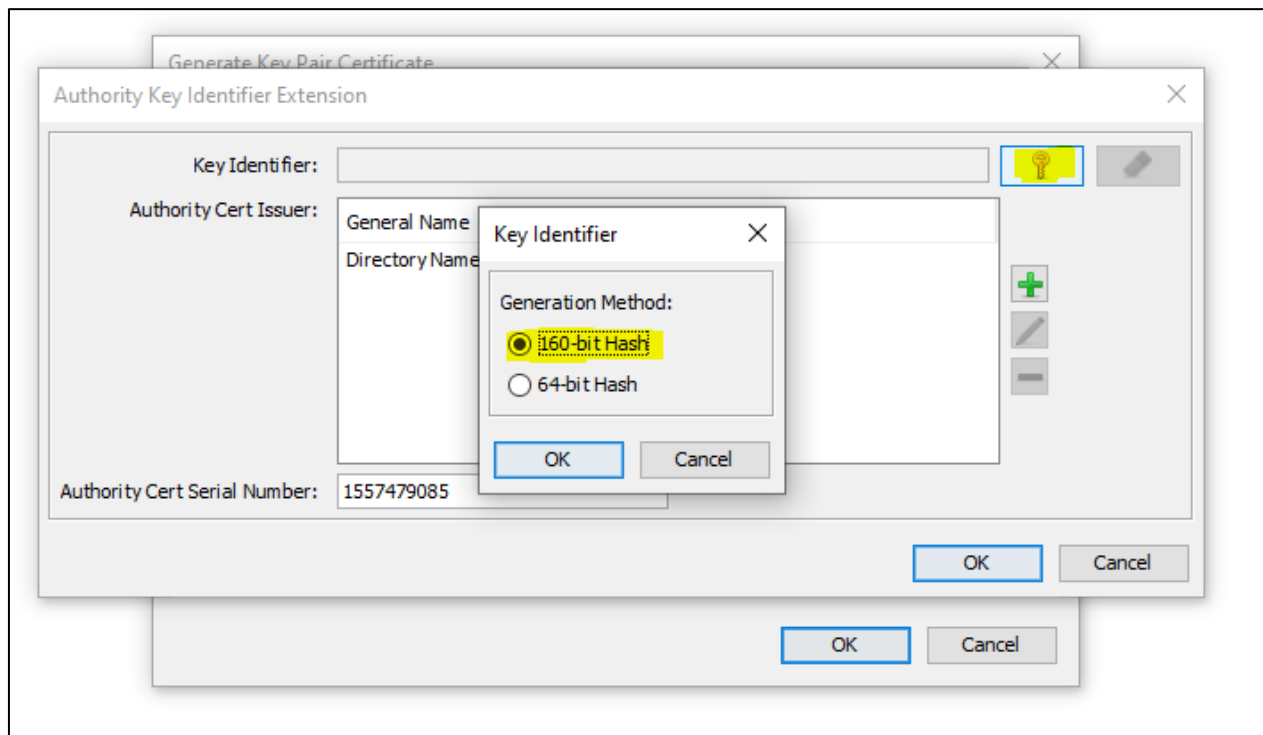
6th STEP:

Click on “Add Extension”, then on the green “+” button:



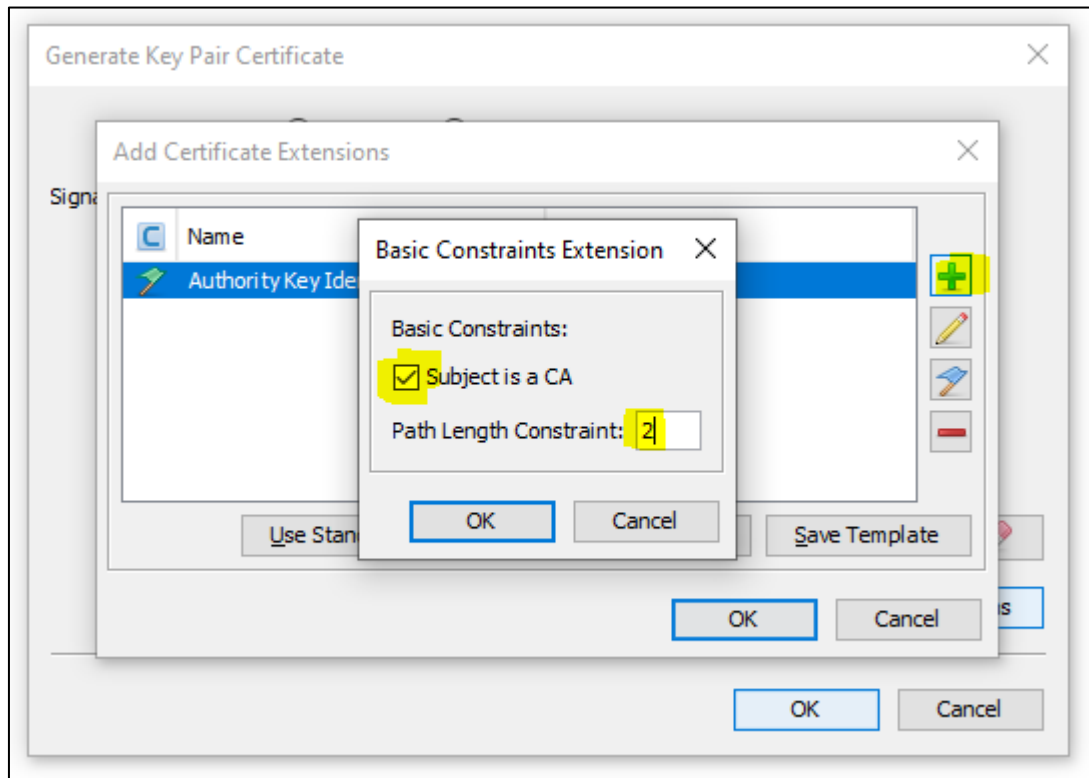
7th STEP:

Select “Authority Key Identifier”, then click on “key” button and select “160-bit Hash”:



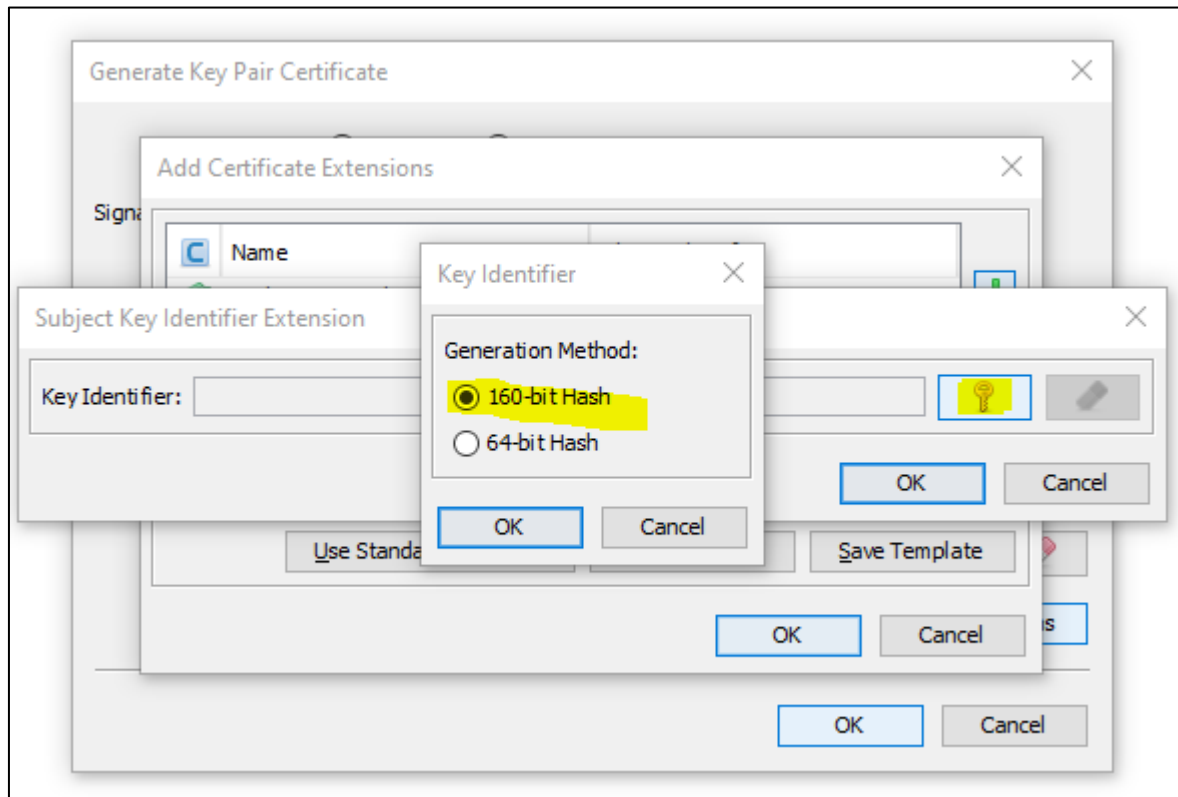
8th STEP:

Click again on the green “+” button of “Add Certificate Extensions” window, select “Basic Constraints”, then tick “Subject is a CA” and set “Path Length Constraint” to 2:



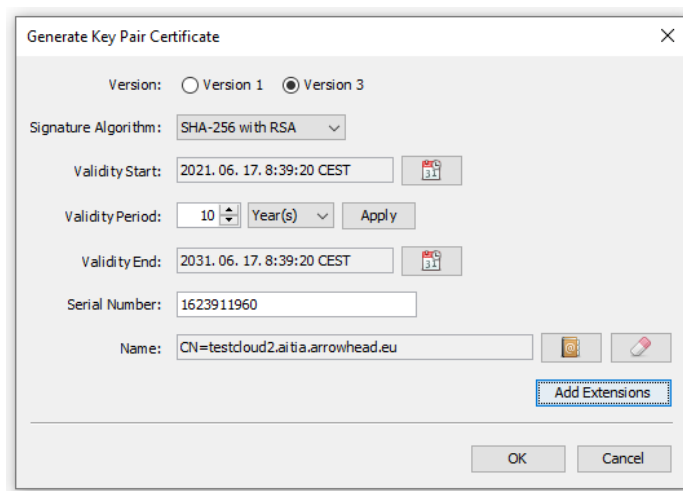
9th STEP:

Click again on the green “+” button of “Add Certificate Extensions” window, select “Subject Key Identifier”, then click on “key” button and select “160-bit Hash”:



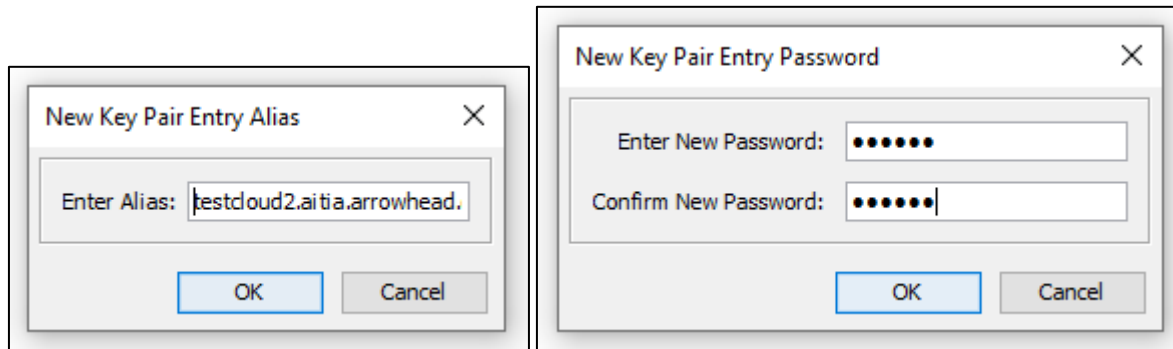
10th STEP:

Click on “OK” button of “Generate Key Pair Certificate” window:



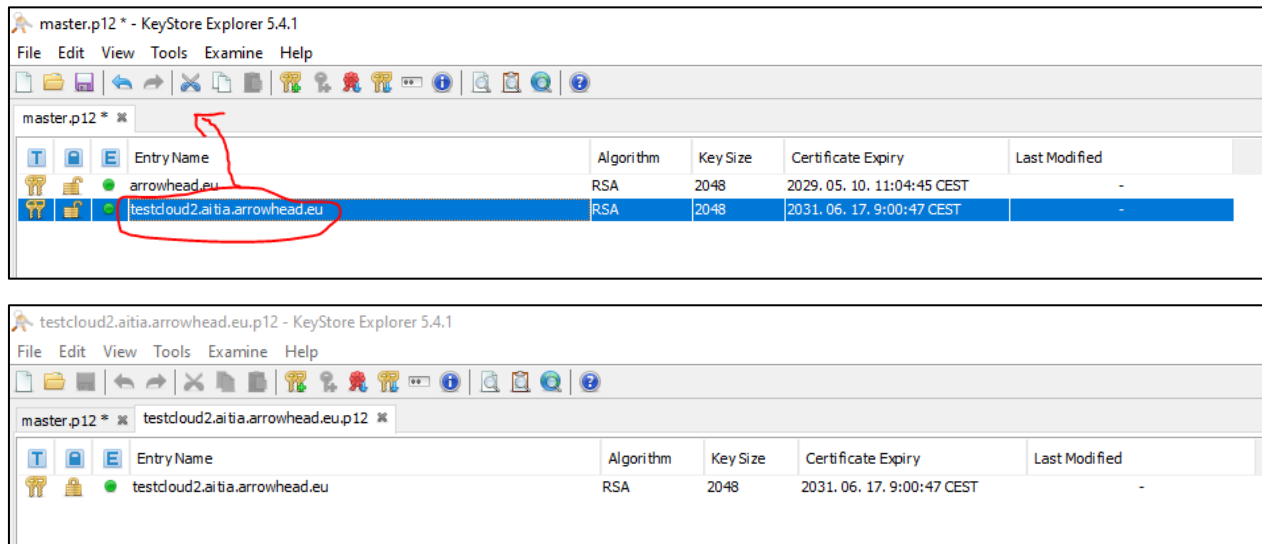
11th STEP:

Set alias equals to the Certificate Common name (eg.: "testcloud2.aitia.arrowhead.eu"), then give a password.



12th STEP:

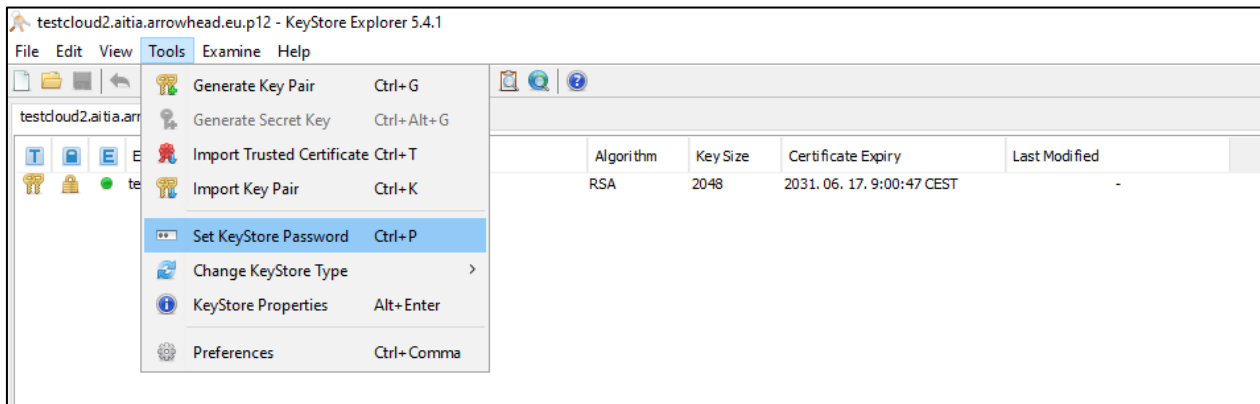
Drag & Drop you newly created key-pair entry to a new tab (It will ask for the password given in the step before.):



Close the "master.p12" and DO NOT SAVE THE CHANGES!

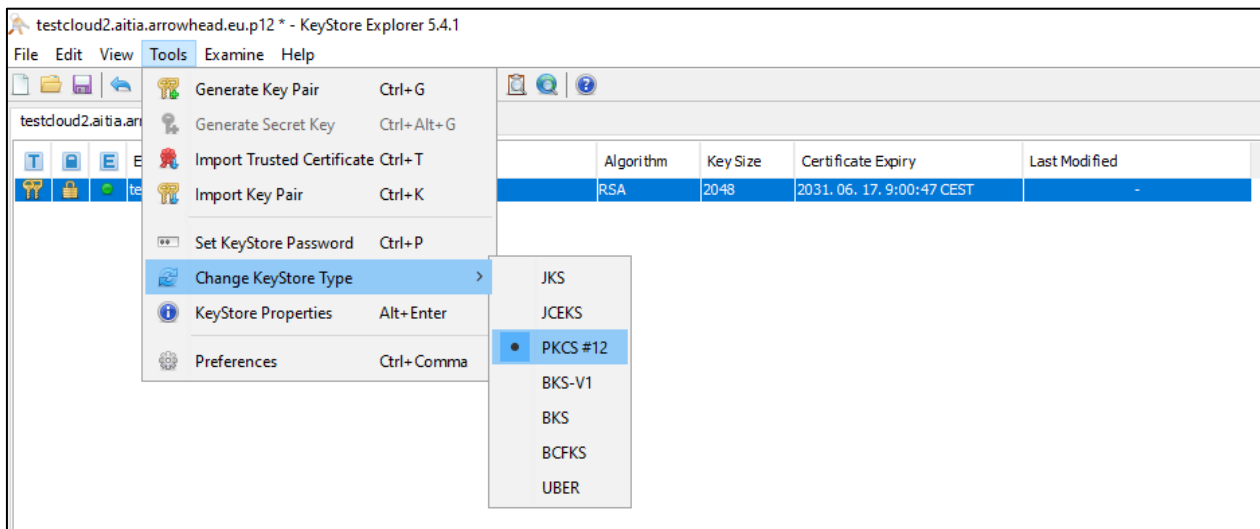
13th STEP:

Click on “Tools” menu and set the “KeyStore Password” (It must be the same as the key-pair password given in the 11th step.):



14th STEP:

Verify that the “KeyStore type” is settled to “PKCS#12”:



15th STEP:

Save your new key-pair certificate as testcloud2.p12.

(“File”->“Save as”-> declare the extension as “.p12”)

