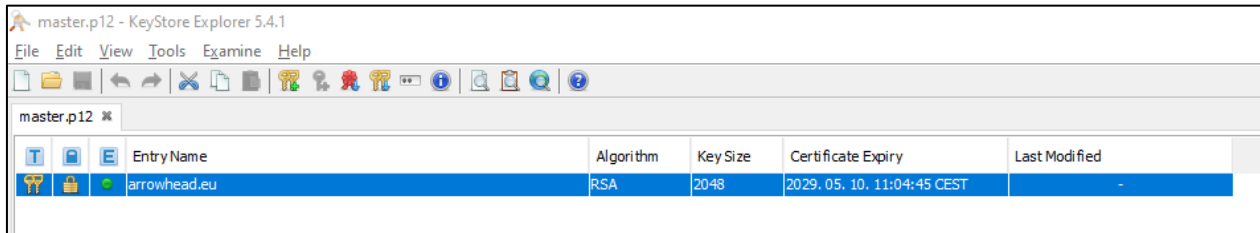


## CREATE ARROWHEAD CLOUD SELF SIGNED CERTIFICATE with KeyStore Explorer 5.4.1

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

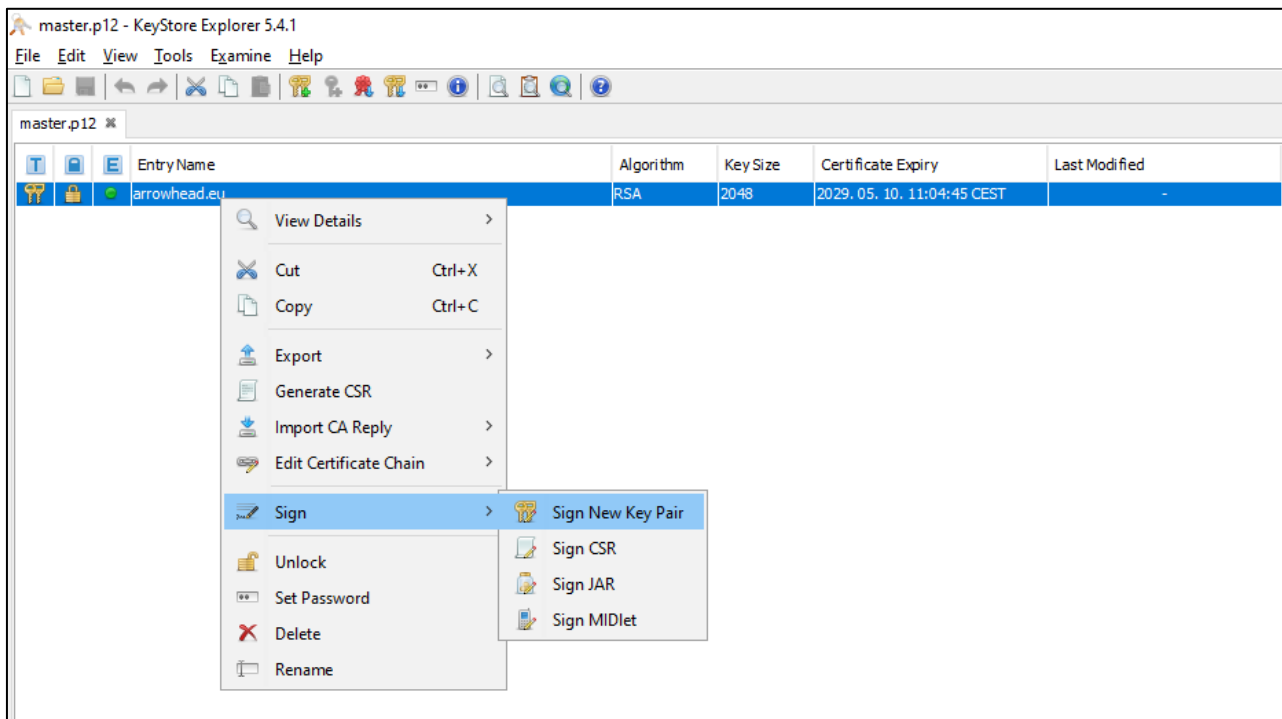
### **1<sup>st</sup> STEP:**

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



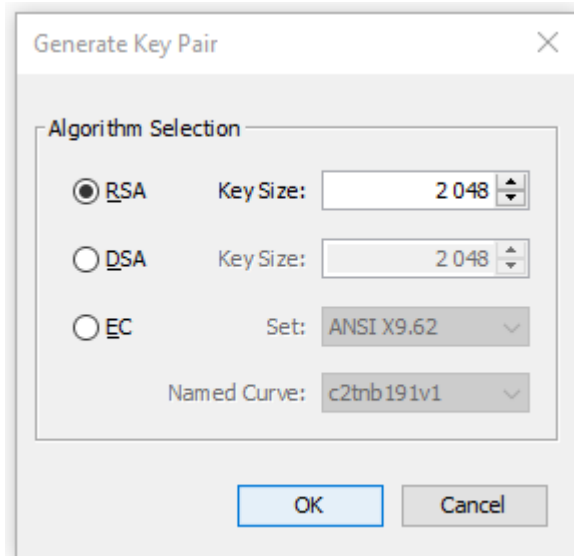
### **2<sup>nd</sup> STEP:**

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



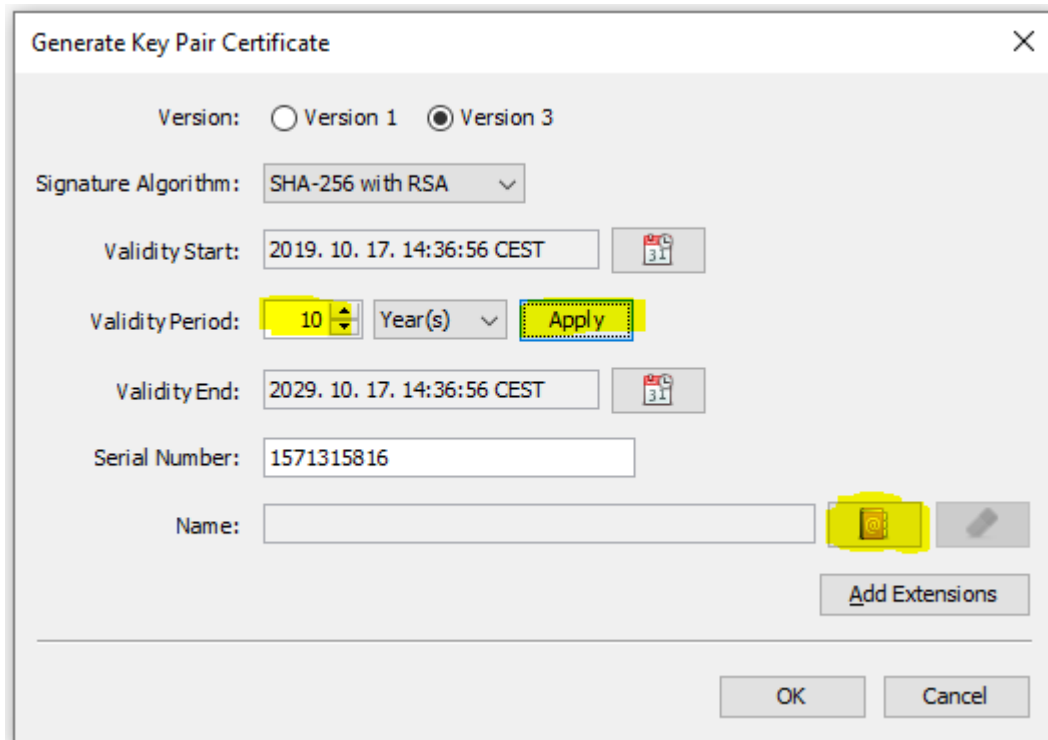
### **3<sup>rd</sup> STEP:**

Select "RSA" and set "Key Size" to 2048:



### **4<sup>th</sup> STEP:**

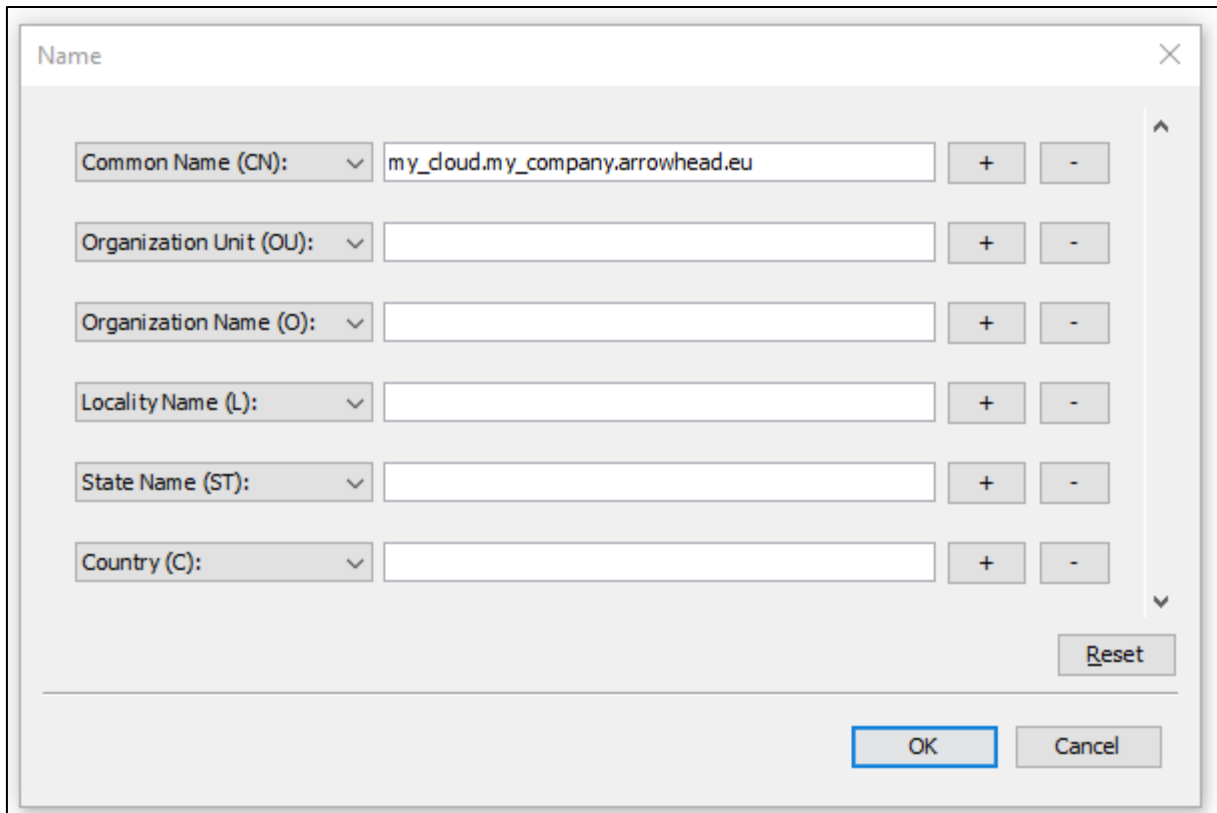
Set the "Validity Period" and hit "Apply", then click on "Edit name":



### 5<sup>th</sup> 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 cloud certificate name has to consist of four part and the last two part have to be 'arrow-head' and 'eu'.

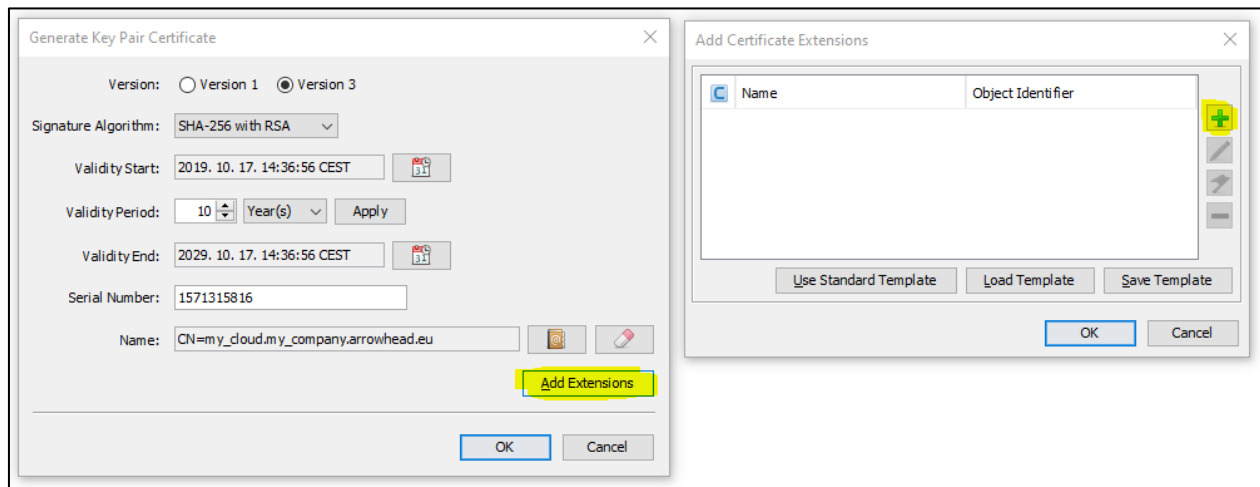


The screenshot shows a 'Name' dialog box with a close button (X) in the top right corner. It contains six rows of input fields, each with a dropdown menu on the left and '+' and '-' buttons on the right. The first row, 'Common Name (CN):', has the text 'my\_cloud.my\_company.arrowhead.eu' entered. The other five rows are empty: 'Organization Unit (OU):', 'Organization Name (O):', 'Locality Name (L):', 'State Name (ST):', and 'Country (C):'. A 'Reset' button is located at the bottom right of the input area. At the very bottom of the dialog are 'OK' and 'Cancel' buttons.

Field	Value
Common Name (CN):	my_cloud.my_company.arrowhead.eu
Organization Unit (OU):	
Organization Name (O):	
Locality Name (L):	
State Name (ST):	
Country (C):	

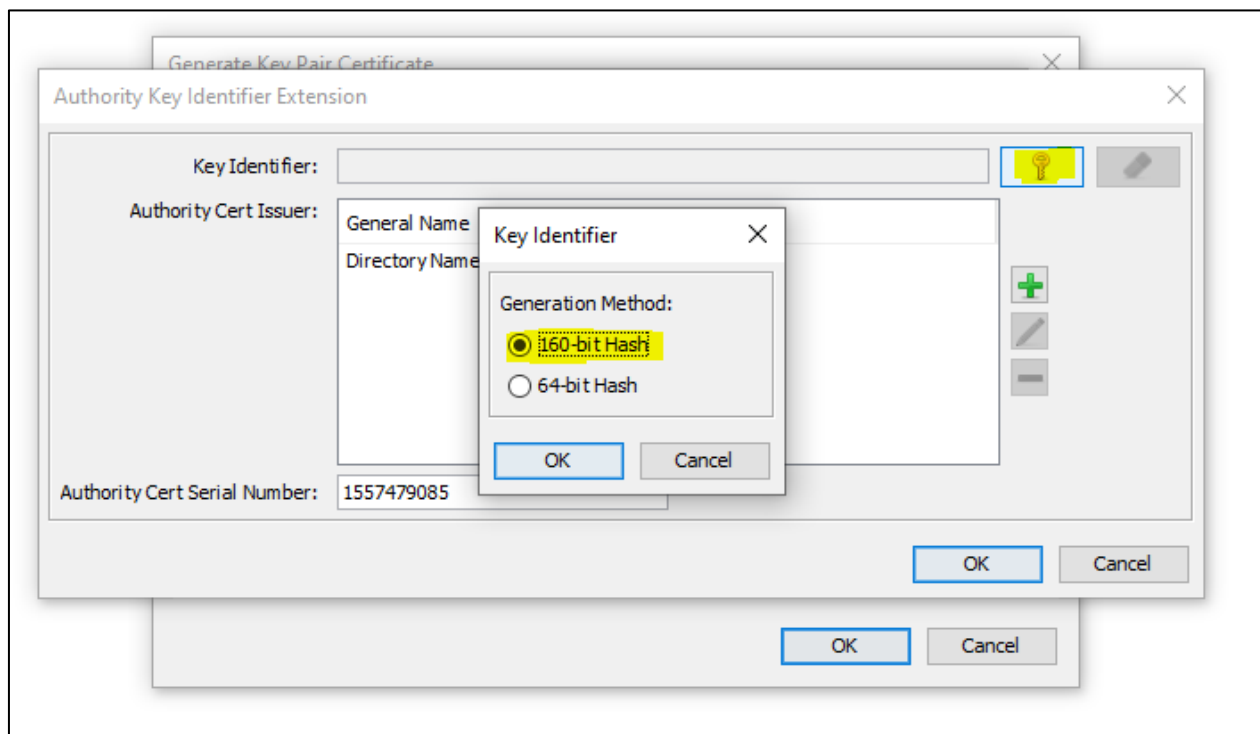
### 6<sup>th</sup> STEP:

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



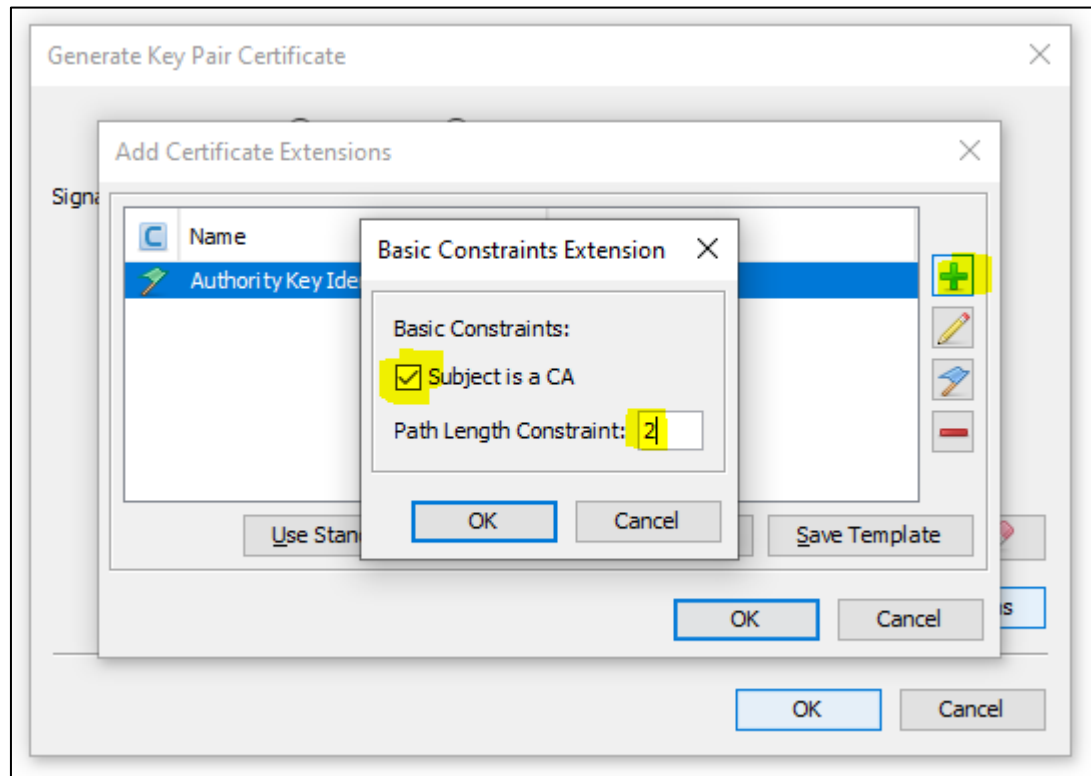
**7<sup>th</sup> STEP:**

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



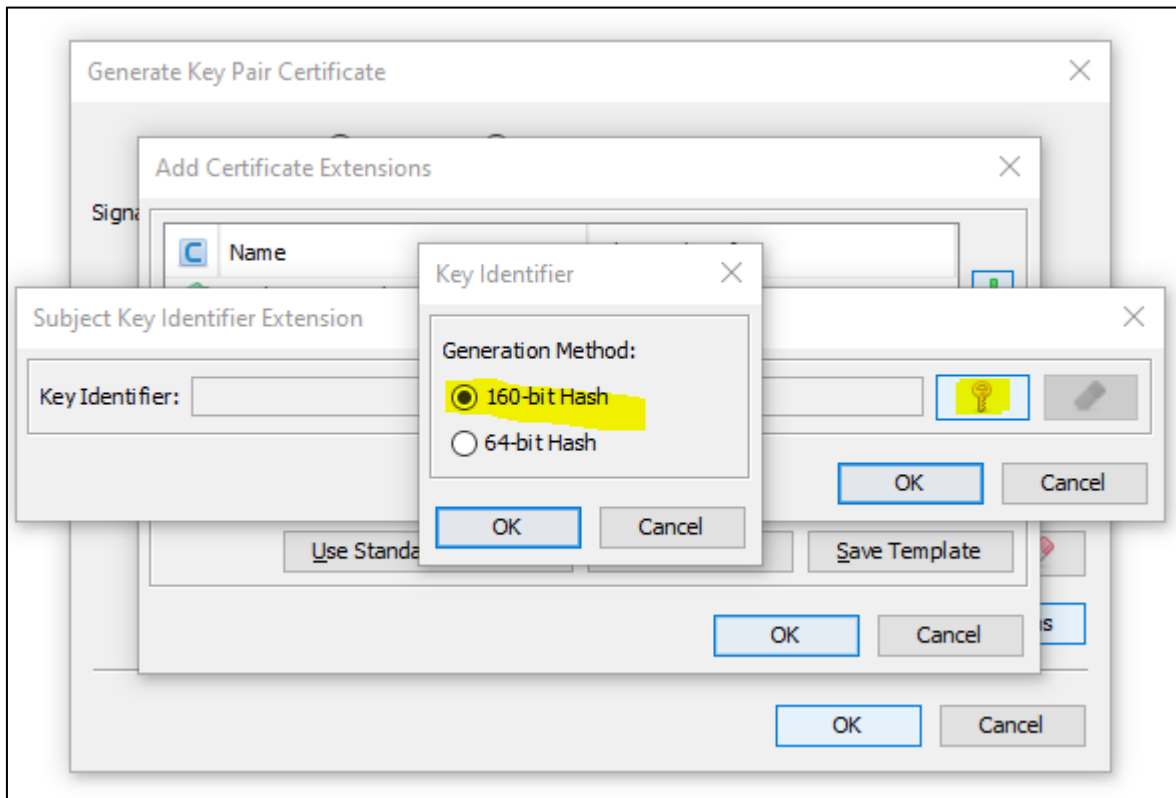
**8<sup>th</sup> STEP:**

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:



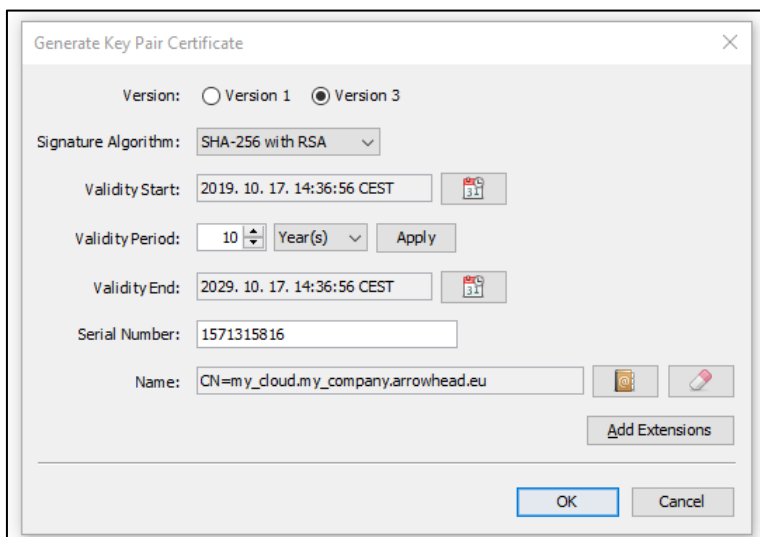
**9<sup>th</sup> STEP:**

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”:



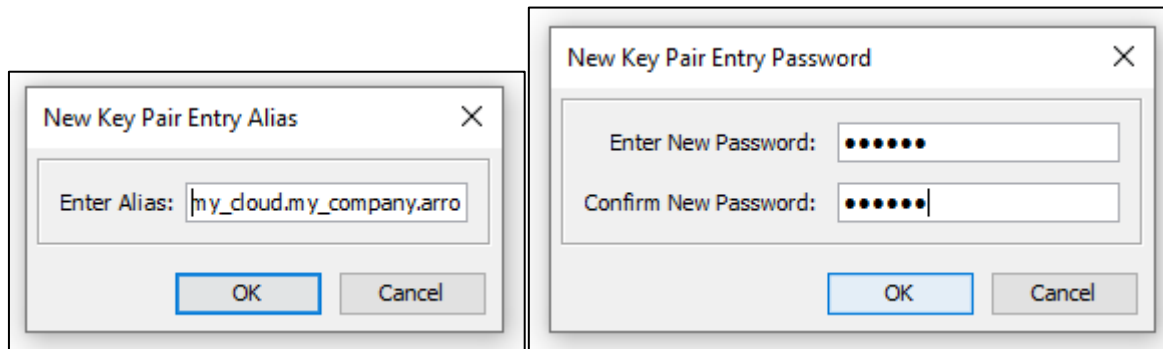
#### **10<sup>th</sup> STEP:**

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



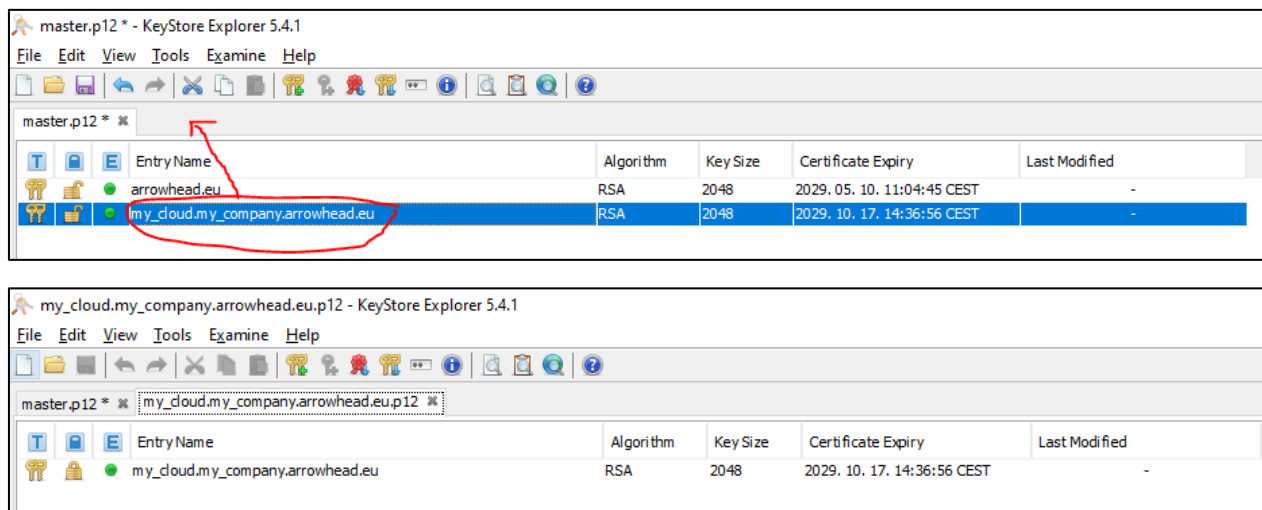
#### **11<sup>th</sup> STEP:**

Set alias equals to the Certificate Common name (eg.: “my\_cloud.my\_company.arrowhead.eu”), then give a password.



### 12<sup>th</sup> STEP:

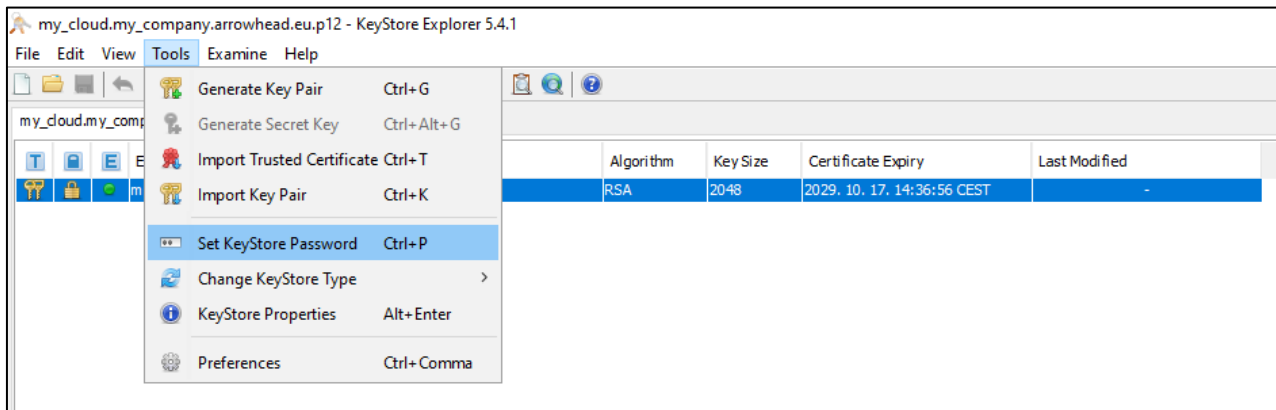
Drag & Drop you newly created key-pair entry to a new tab (It will ask for the password given in the step before.):



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

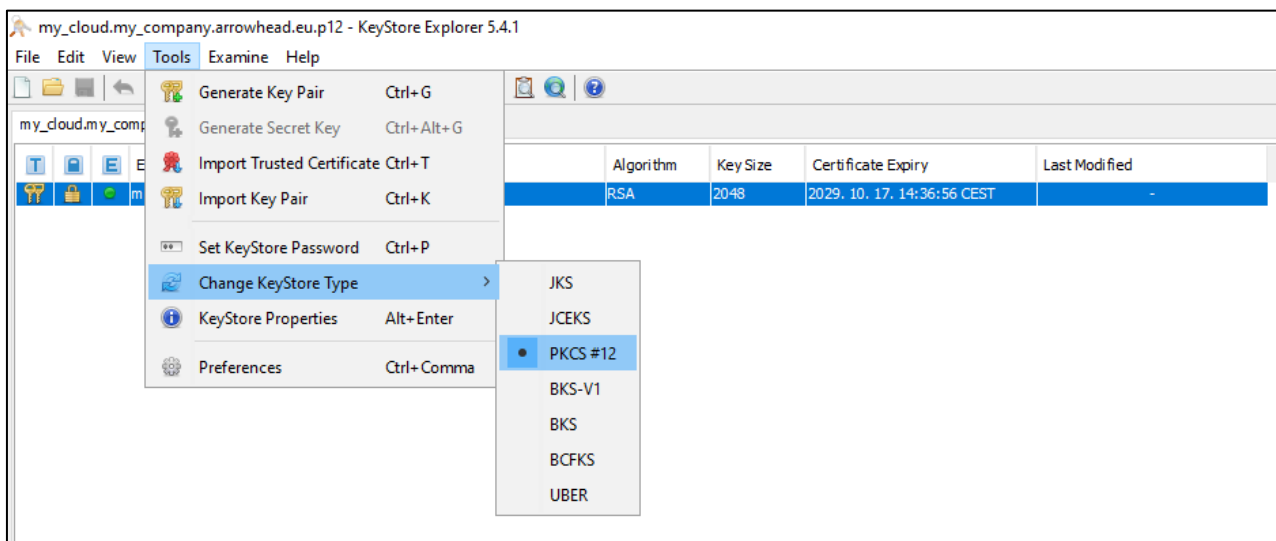
### 13<sup>th</sup> STEP:

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



#### **14<sup>th</sup> STEP:**

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



#### **15<sup>th</sup> STEP:**

Save your new key-pair certificate as my\_cloud.p12.

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



