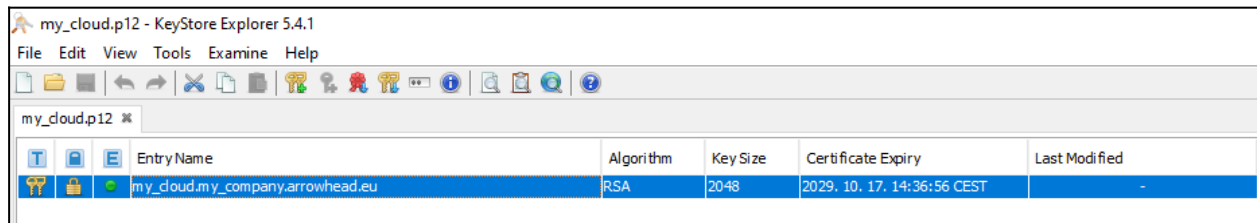


## CREATE ARROWHEAD CLIENT SELF SIGNED CERTIFICATE with KeyStore Explorer 5.4.1

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

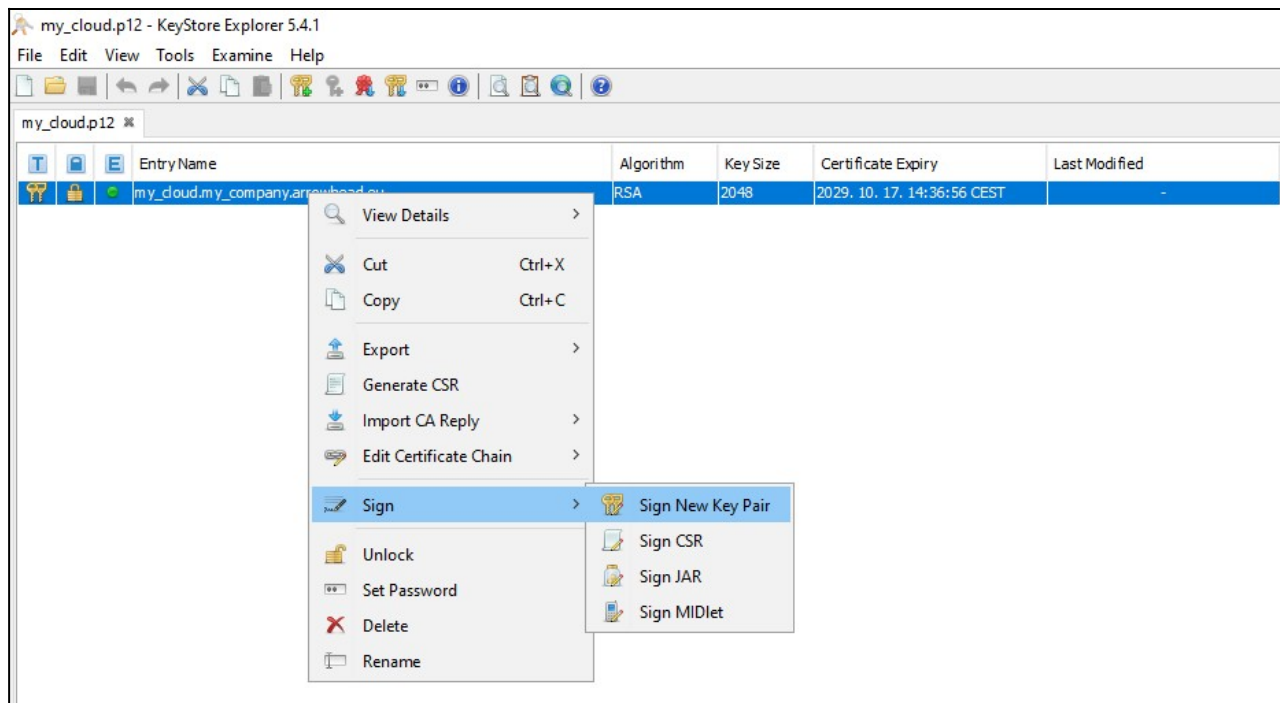
### **1<sup>st</sup> STEP:**

Open your cloud **p12** certificate file.



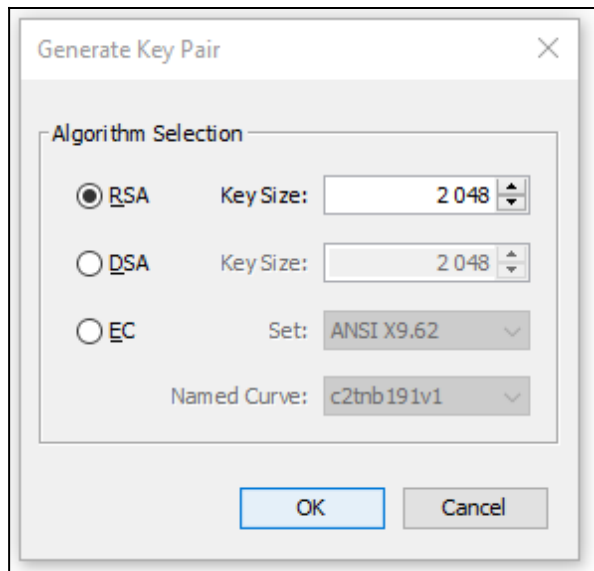
### **2<sup>nd</sup> STEP:**

Right click on your cloud key pair entry and select "Sign New Key Pair" and enter its password:



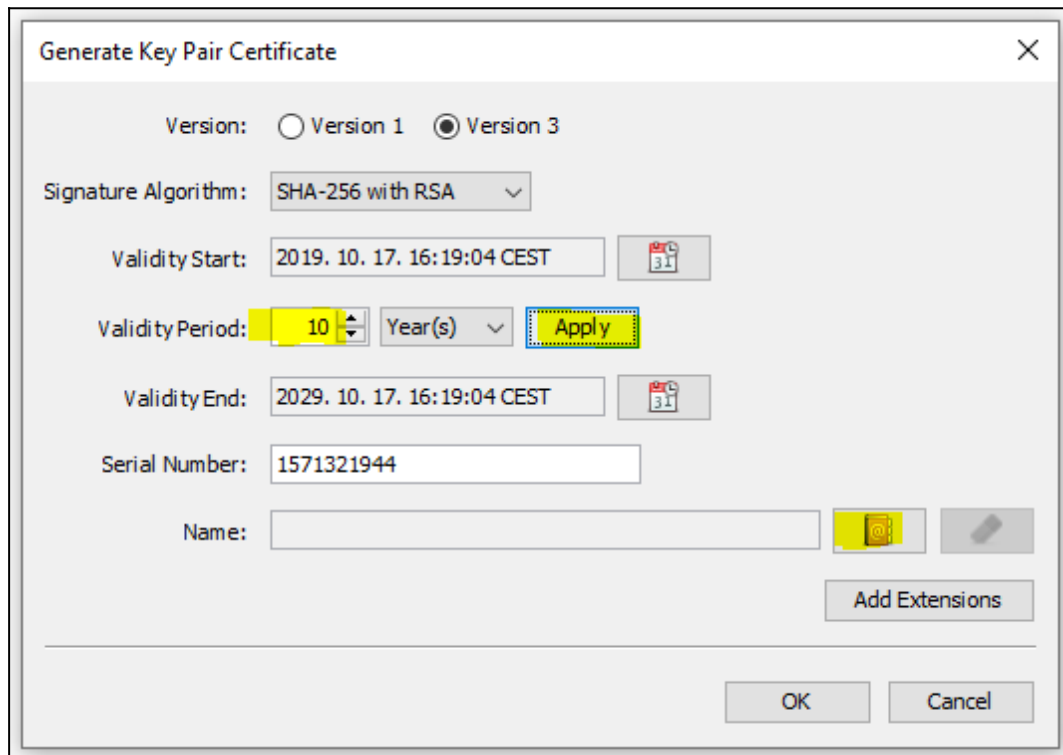
### **3<sup>rd</sup> STEP:**

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



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

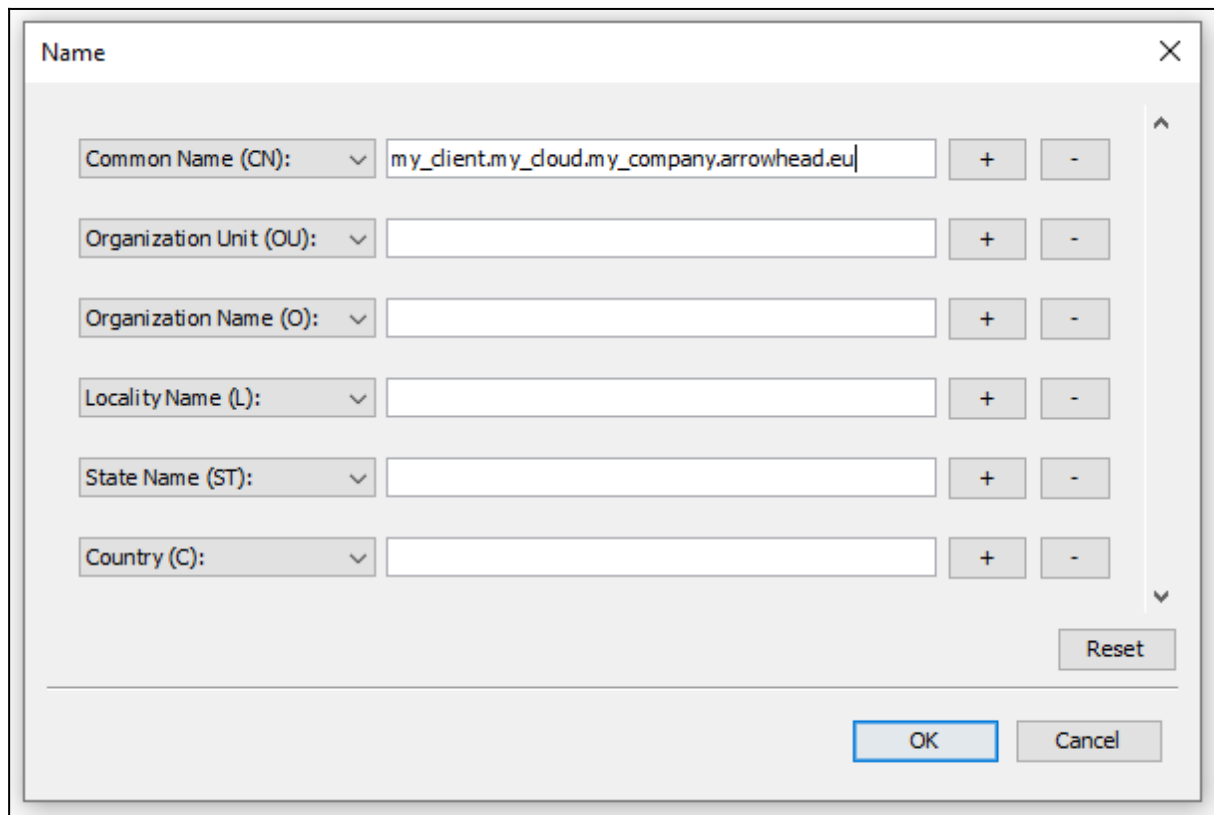
Set the “Validity Period” and hit “Apply”, then click on “Edit name”:



#### **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 client certificate name has to consist of five part and the last two part have to be 'arrowhead' and 'eu'.

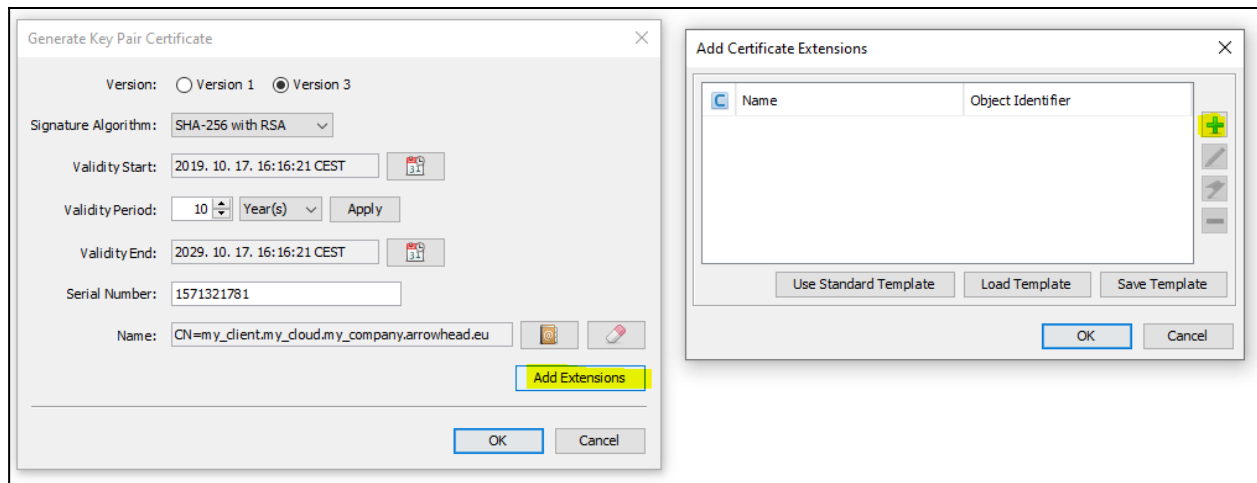


The image shows a 'Name' dialog box with a close button (X) in the top right corner. It contains six rows of input fields, each with a dropdown menu on the left and a text box on the right. To the right of each text box are two buttons: a '+' button and a '-' button. The first row is for 'Common Name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

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

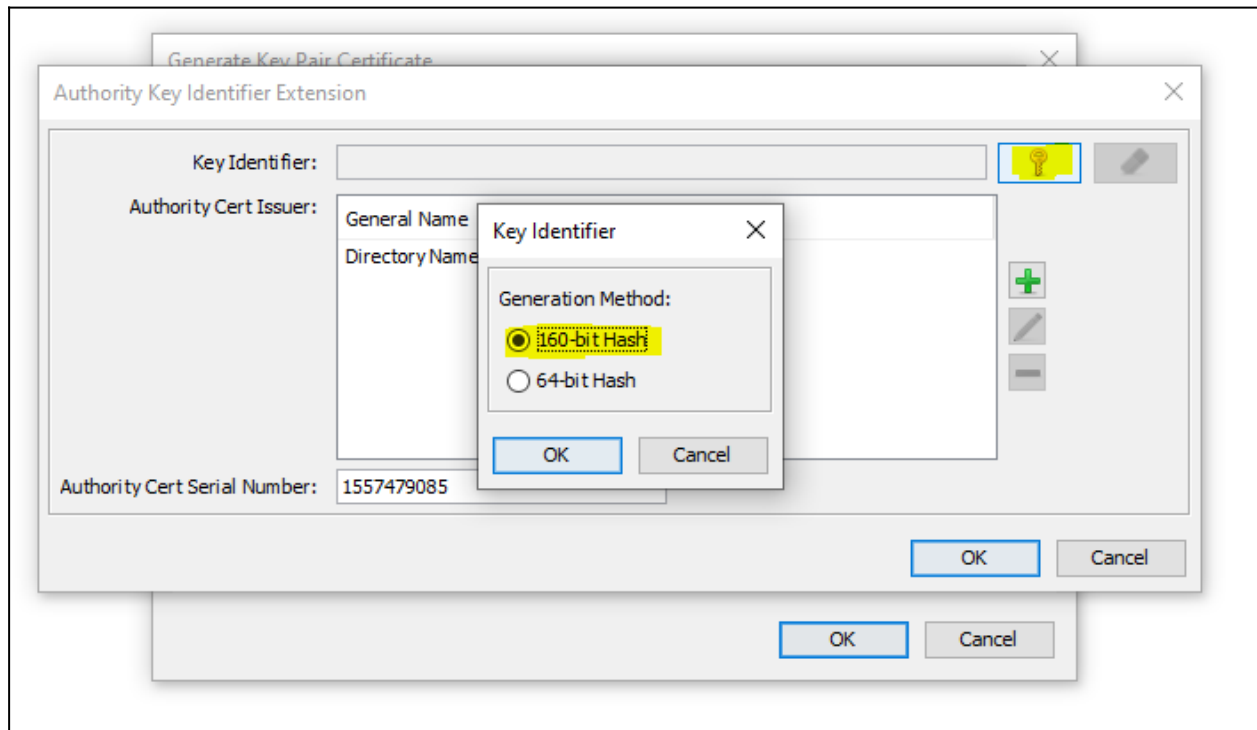
**6<sup>th</sup> STEP:**

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



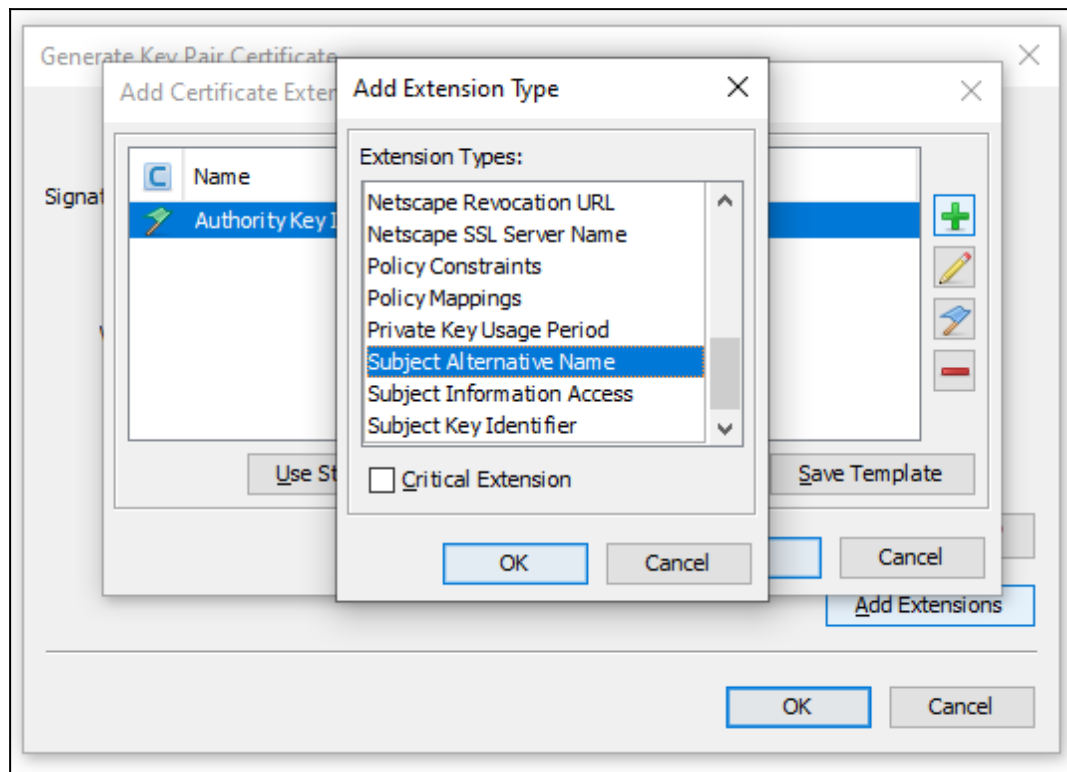
### **7<sup>th</sup> STEP:**

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



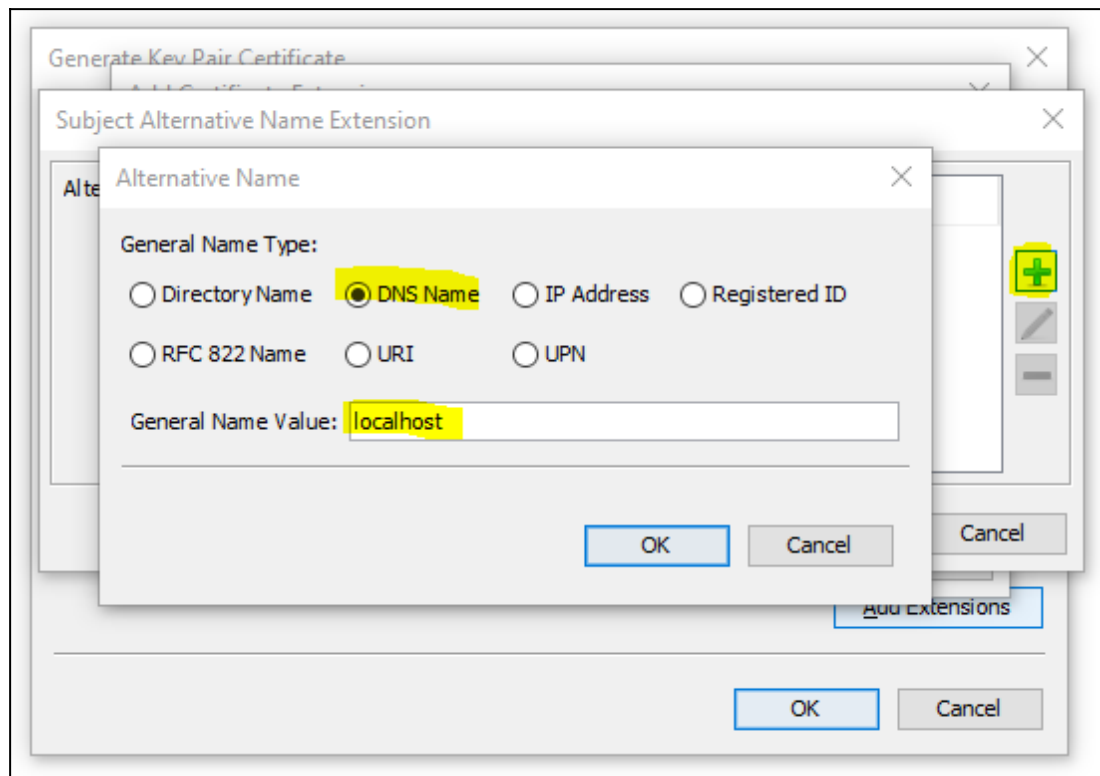
### **8<sup>th</sup> STEP:**

Click again on green “+” button of the “Add Certificate Extensions” window and choose “Subject Alternative Name”:



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

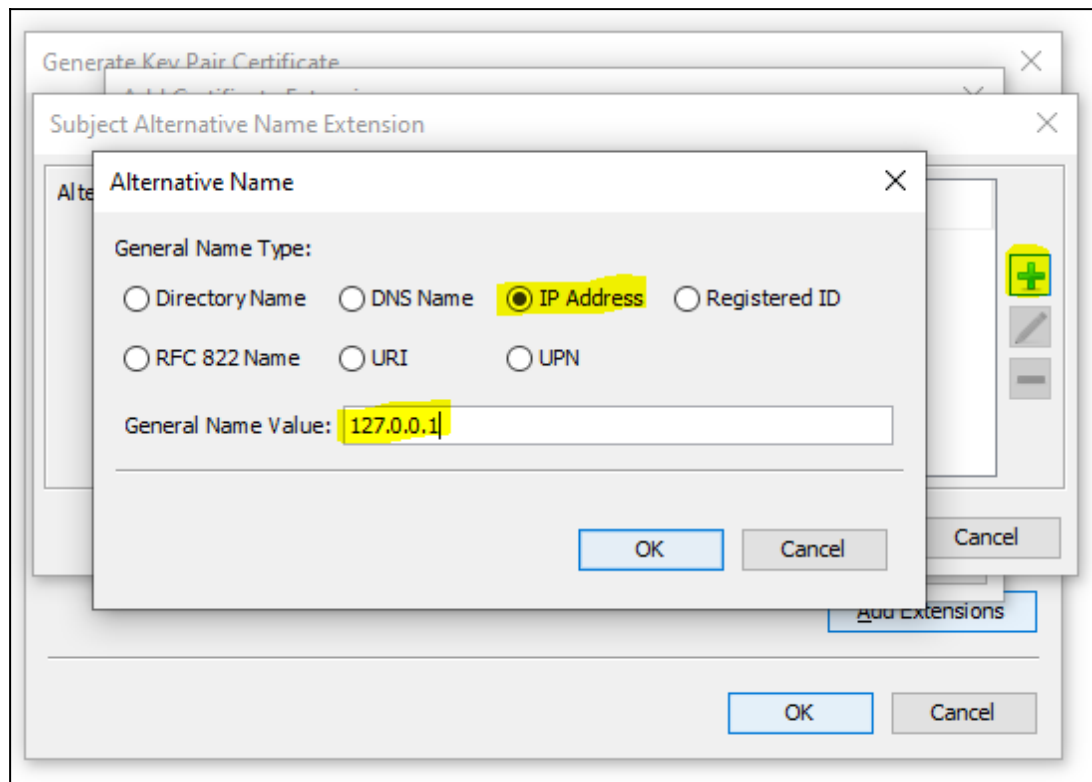
Click on green "+" button, select "DNS Name" and fill the "General Name Value" with "localhost" and press "OK":



Repeat if you want to add your other DNS Name (for accessing remote services).

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

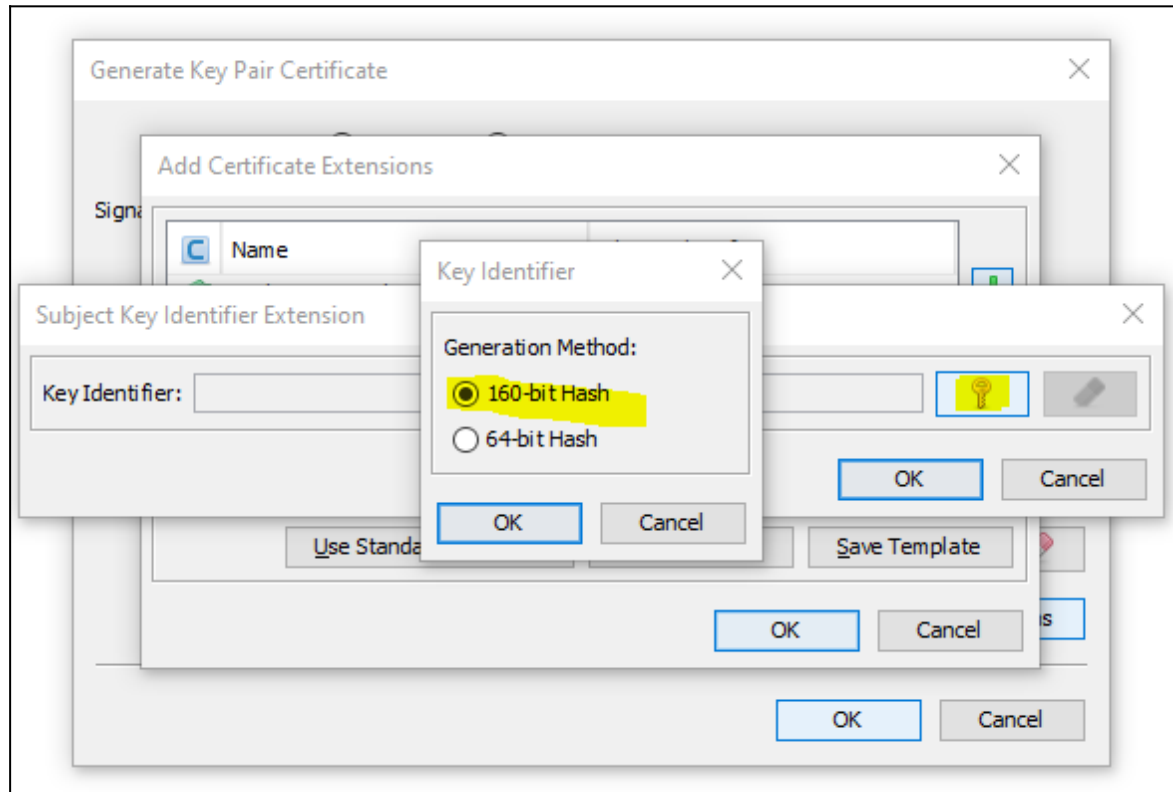
Click on green “+” button again, select “IP Address” and fill the “General Name Value” with “127.0.0.1” and press “OK”:



Repeat if you want to add your other IP Address (for accessing remote services).

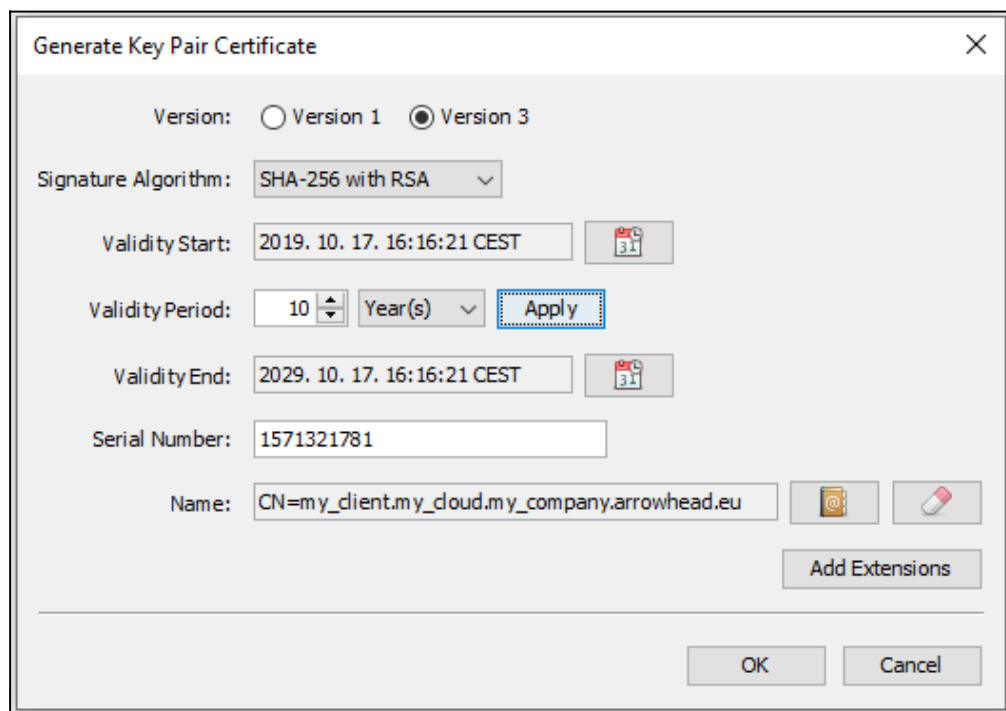
### **11<sup>th</sup> STEP:**

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”:



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

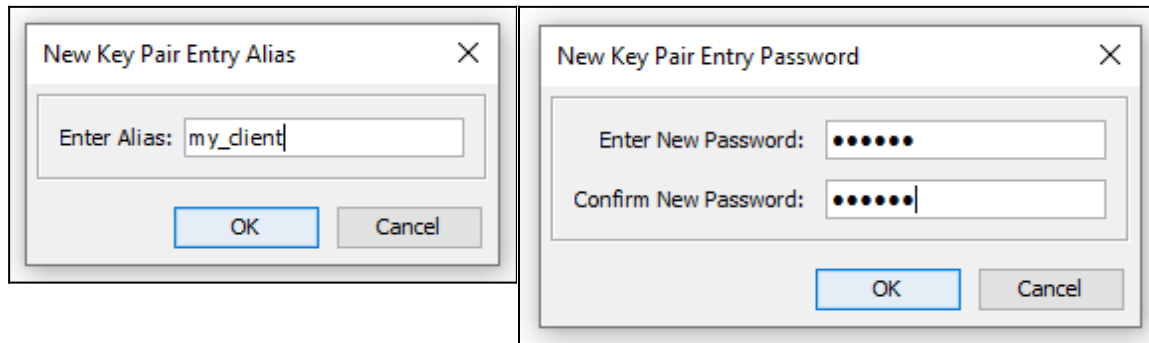
Click on “OK” button of “Generate Key Pair Certificate” window:





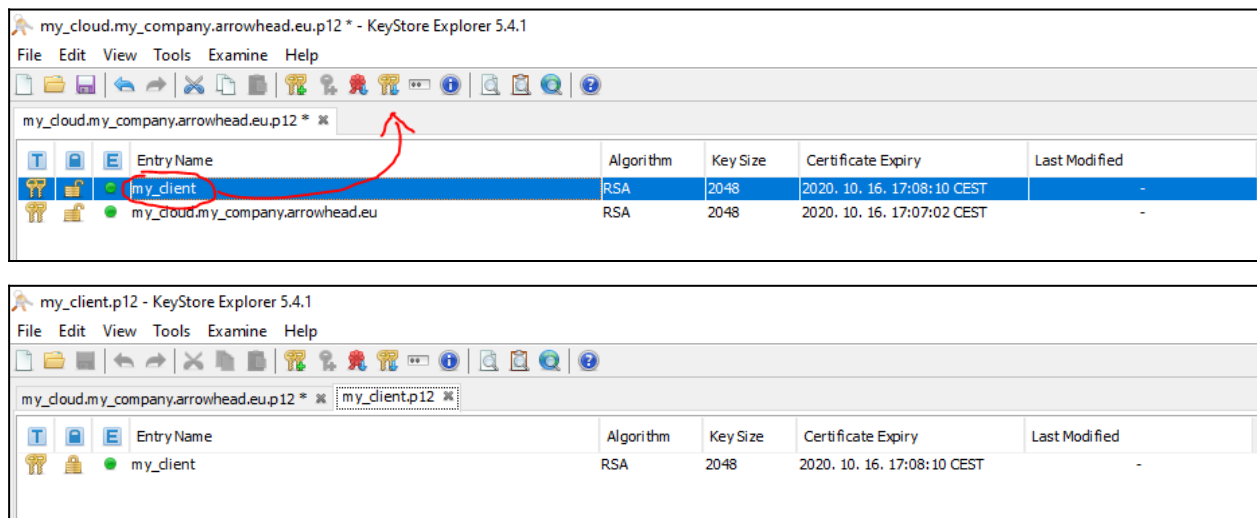
### 13<sup>th</sup> STEP:

Set alias (eg.: “my\_client”), then give a password.



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

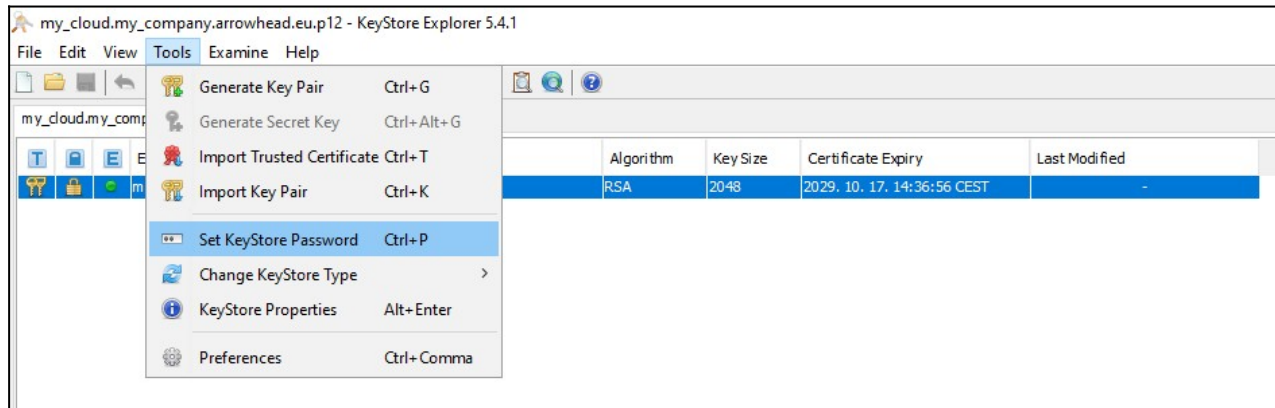
Drag & Drop your newly created key-pair entry to a new tab (It will ask for the password given in the step before.):



Close the “my\_cloud.p12” and DO NOT SAVE THE CHANGES!

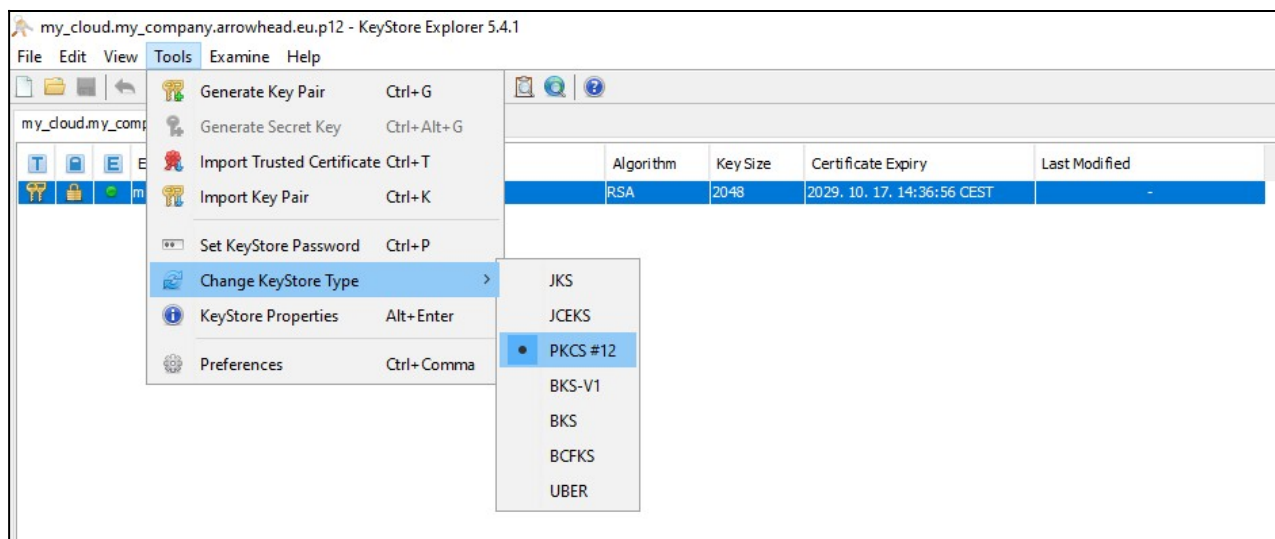
### 15<sup>th</sup> STEP:

Click on “Tools” menu and set the “KeyStore Password” (It must be the same as the key-pair password given in the 13<sup>th</sup> step.):



### **16<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\_client.p12.

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

