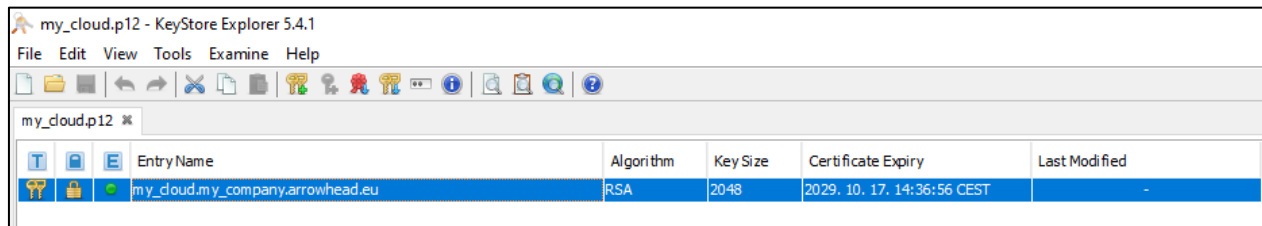


CREATE ARROWHEAD CLIENT SELF SIGNED CERTIFICATE with KeyStore Explorer 5.4.1

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

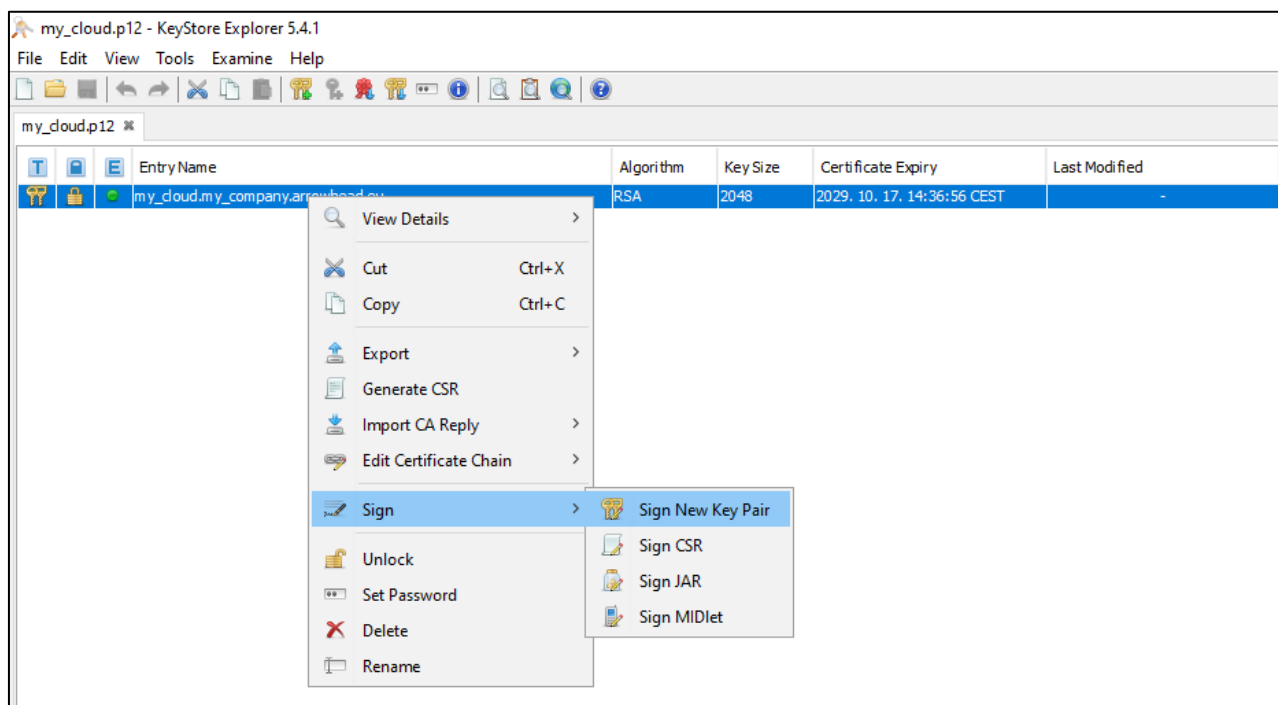
1st STEP:

Open your cloud **p12** certificate file.



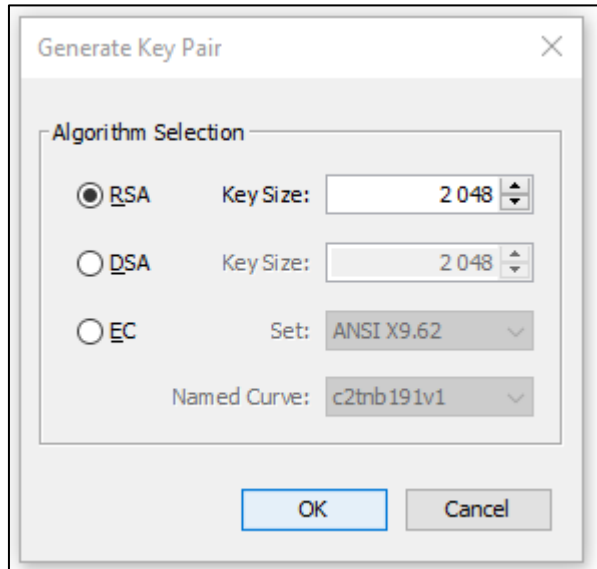
2nd STEP:

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



3rd STEP:

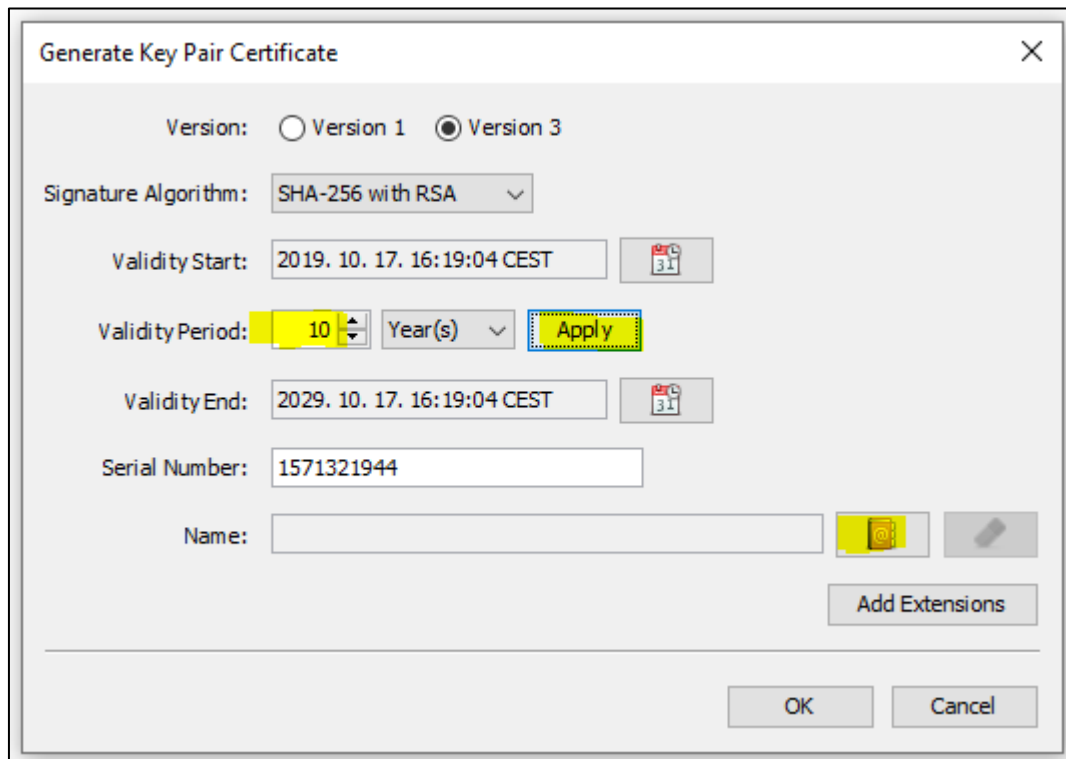
Select "RSA" and set "Key Size" to 2048:



The "Generate Key Pair" dialog box is shown. It has a title bar with a close button (X). Inside, there is a section titled "Algorithm Selection". Under this section, there are three radio buttons: "RSA" (selected), "DSA", and "EC". To the right of each radio button is a "Key Size" or "Set" field. For "RSA", the "Key Size" is set to "2 048". For "DSA", the "Key Size" is also set to "2 048". For "EC", the "Set" is set to "ANSI X9.62" and the "Named Curve" is set to "c2tnb191v1". At the bottom of the dialog, there are "OK" and "Cancel" buttons.

4th STEP:

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

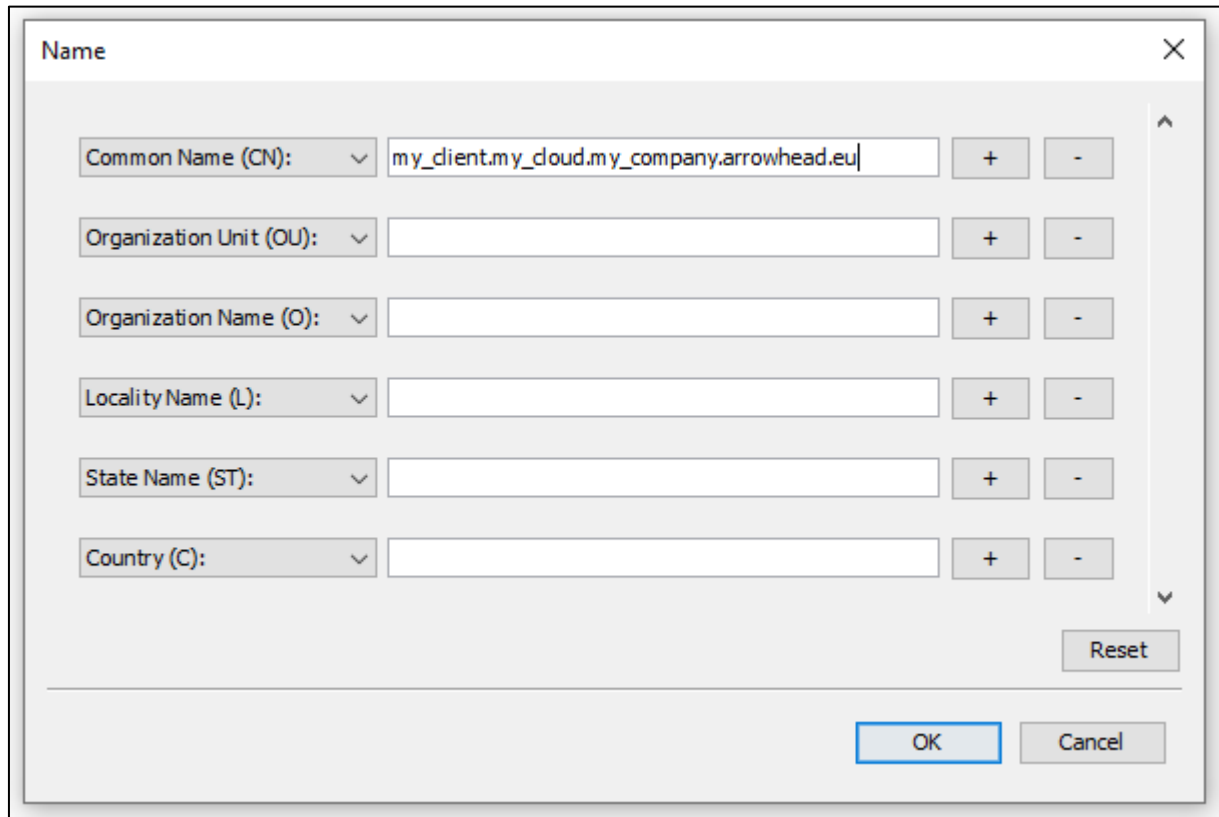


The "Generate Key Pair Certificate" dialog box is shown. It has a title bar with a close button (X). Inside, there is a "Version" section with two radio buttons: "Version 1" and "Version 3" (selected). Below this is a "Signature Algorithm" dropdown menu set to "SHA-256 with RSA". There are two date fields: "Validity Start" (2019. 10. 17. 16:19:04 CEST) and "Validity End" (2029. 10. 17. 16:19:04 CEST), each with a calendar icon. Between these fields is a "Validity Period" section with a spinner set to "10", a "Year(s)" dropdown, and an "Apply" button. Below the "Validity End" field is a "Serial Number" field set to "1571321944". At the bottom, there is a "Name" field, a yellow "Edit name" button, and a grey "Edit name" button. There is also an "Add Extensions" button. At the very bottom, there are "OK" and "Cancel" buttons.

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 client certificate name has to consist of five part and the last two part have to be 'arrow-head' and 'eu'.

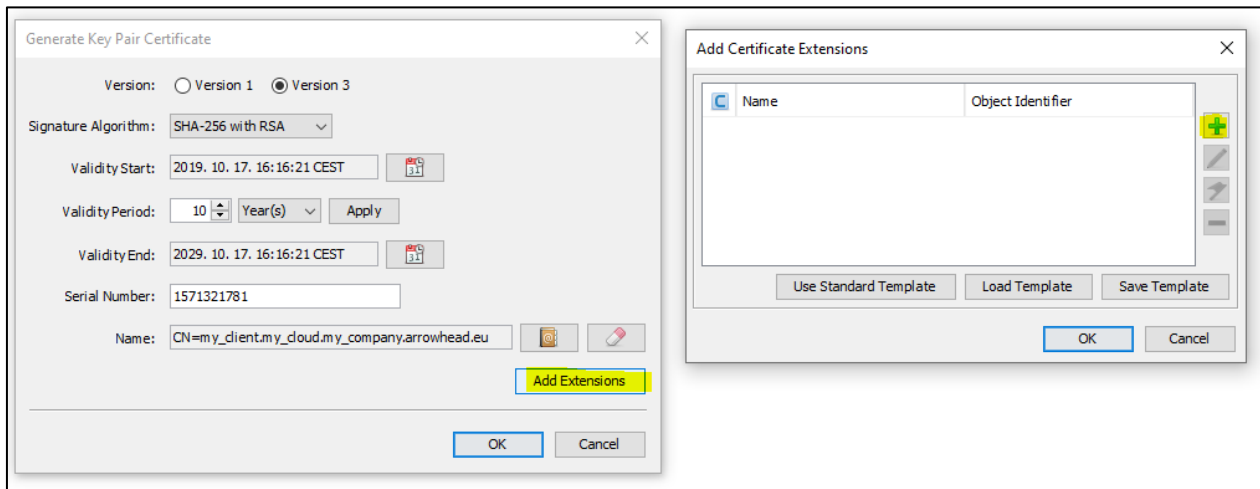


The image shows a 'Name' dialog box with a close button (X) in the top right corner. It contains six rows of input fields, each with a dropdown menu on the left and '+' and '-' buttons on the right. The first row, 'Common Name (CN):', has the text 'my_client.my_cloud.my_company.arrowhead.eu' entered. The other five rows are empty. 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_client.my_cloud.my_company.arrowhead.eu
Organization Unit (OU):	
Organization Name (O):	
Locality Name (L):	
State Name (ST):	
Country (C):	

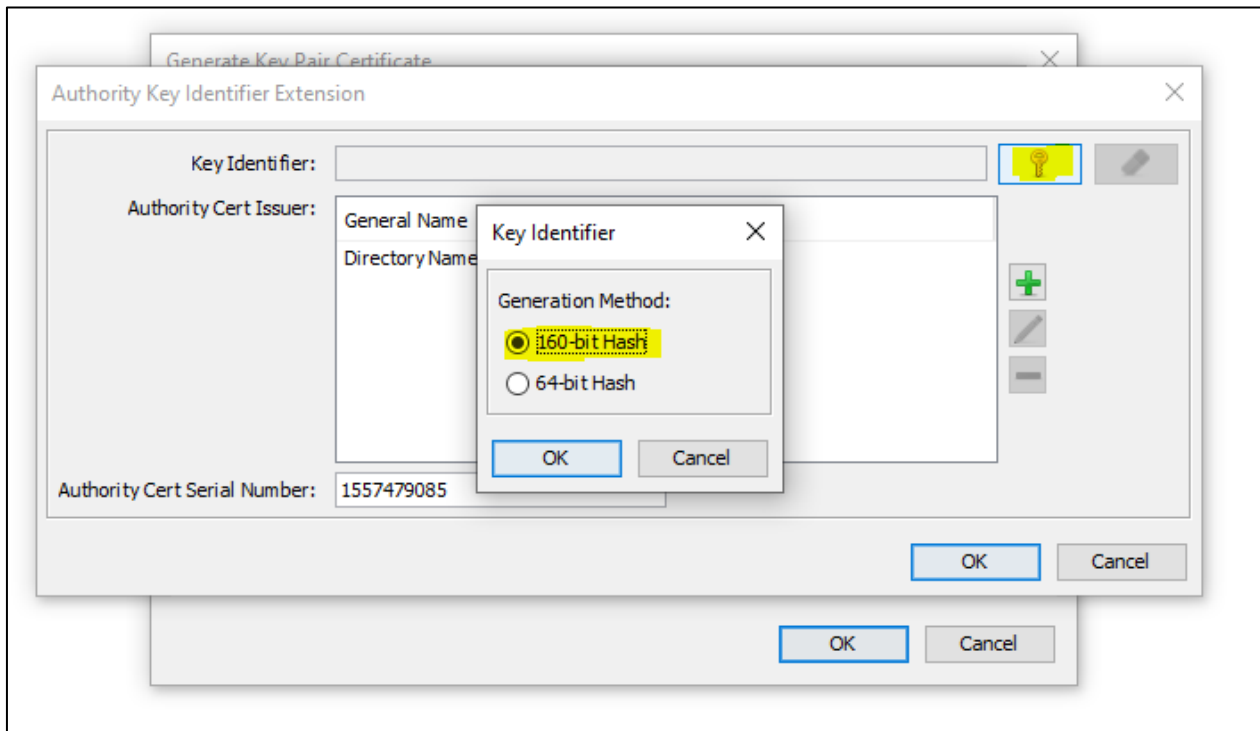
6th STEP:

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



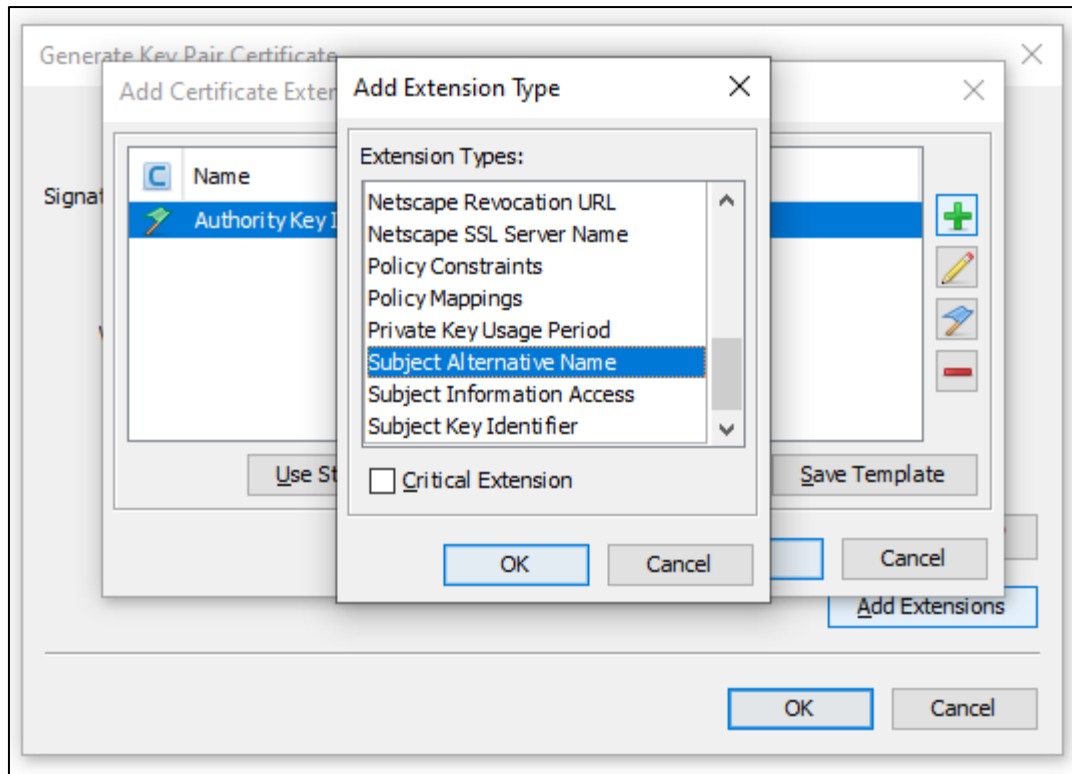
7th STEP:

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



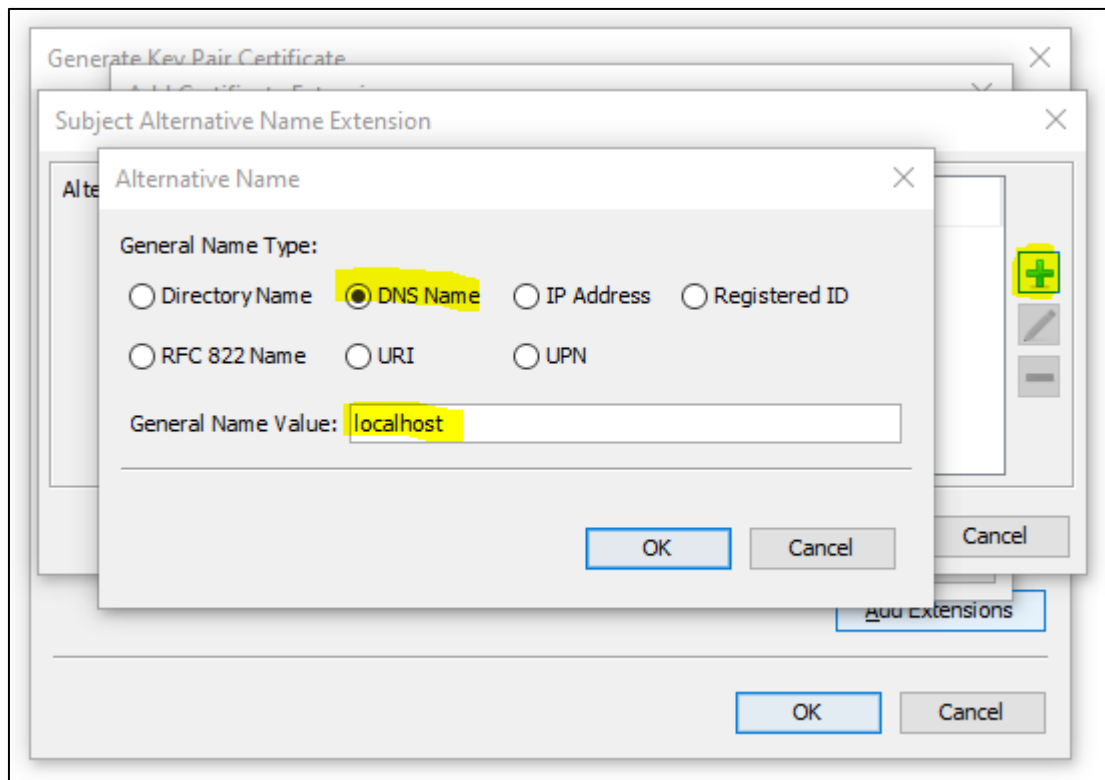
8th STEP:

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



9th STEP:

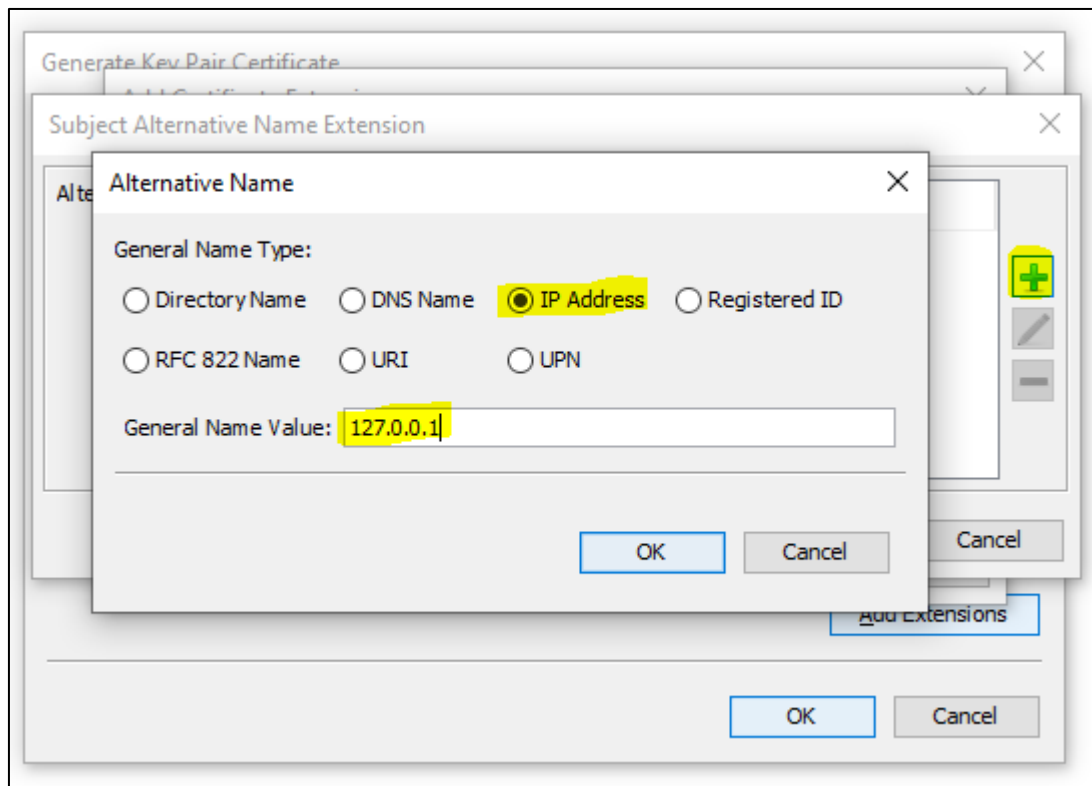
Click on green “+” button, select “DNS Name” and fill the “General Name Value” with “localhost” and press “OK”:



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

10th STEP:

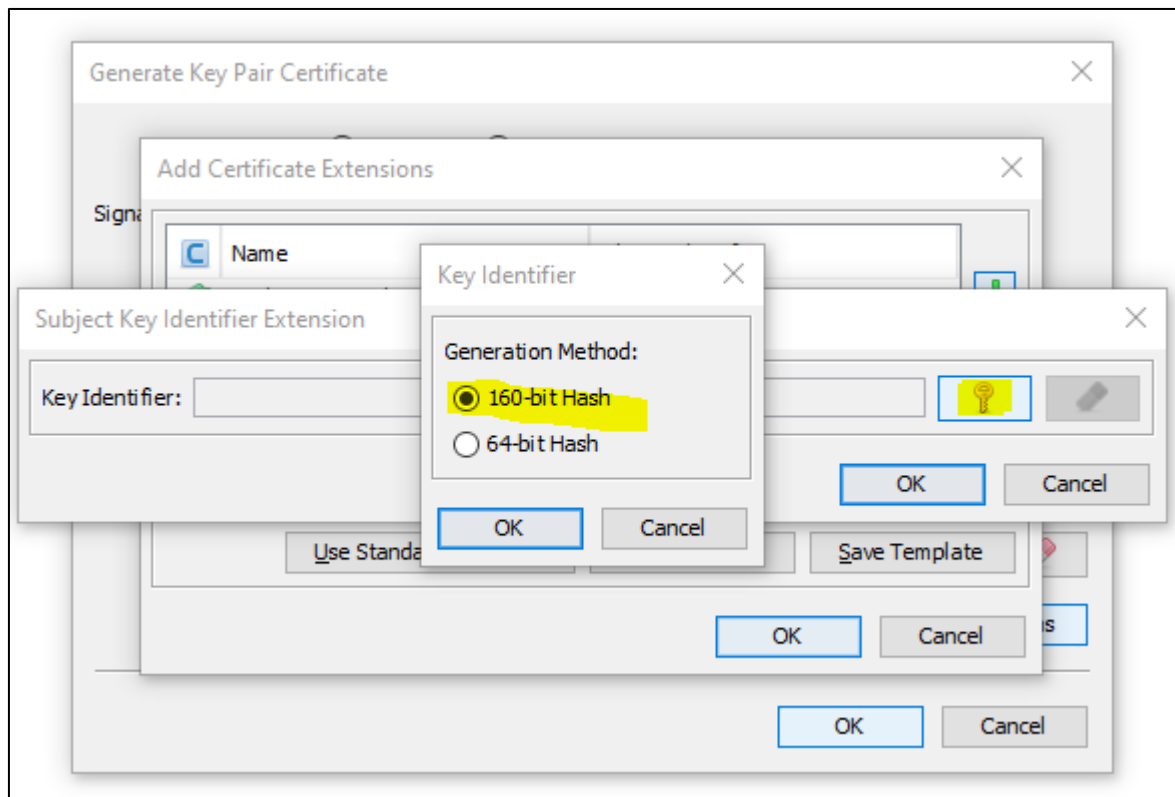
Click on green “+” button again, select “IP Address” and fill the “General Name Value” with “127.0.0.1” and press “OK”:



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

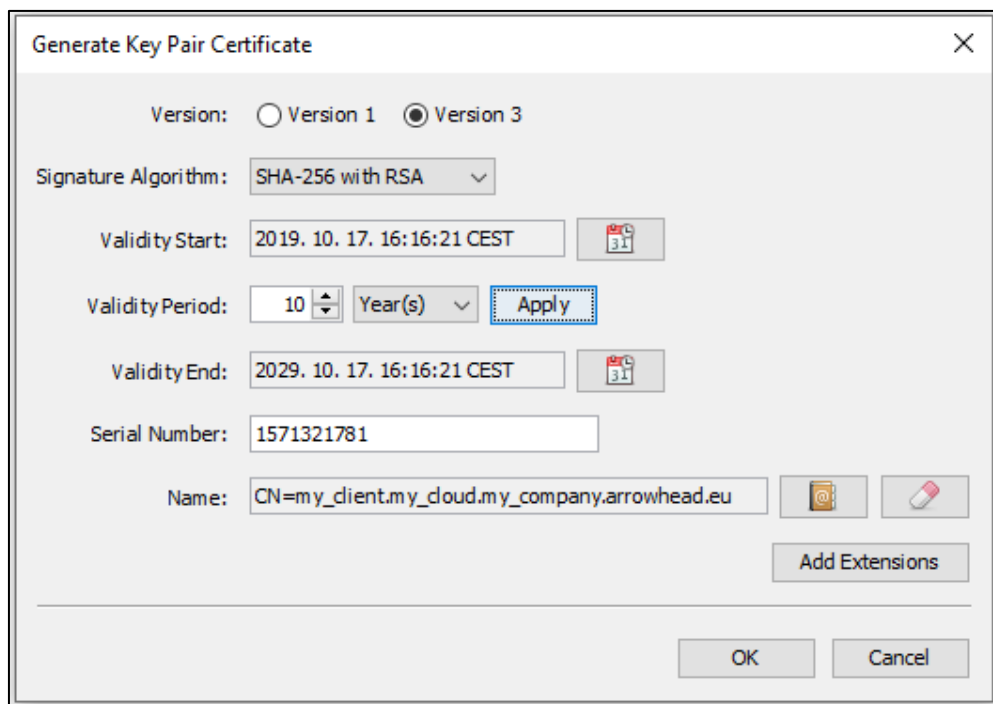
11th STEP:

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”:



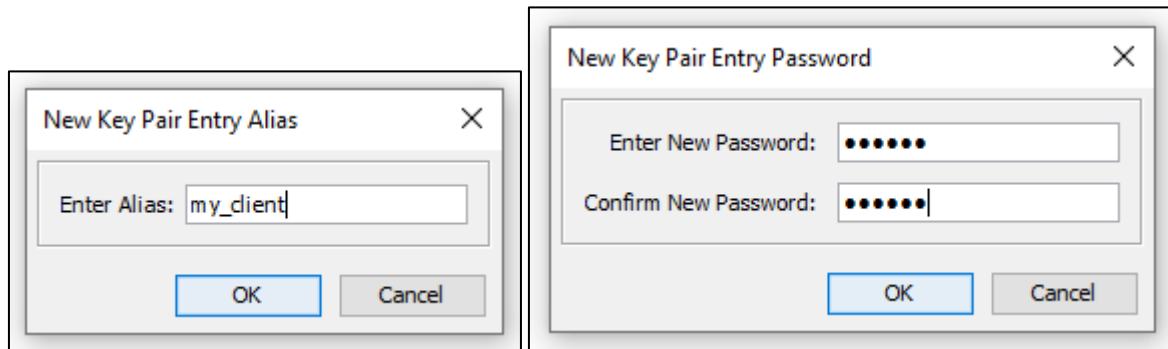
12th STEP:

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



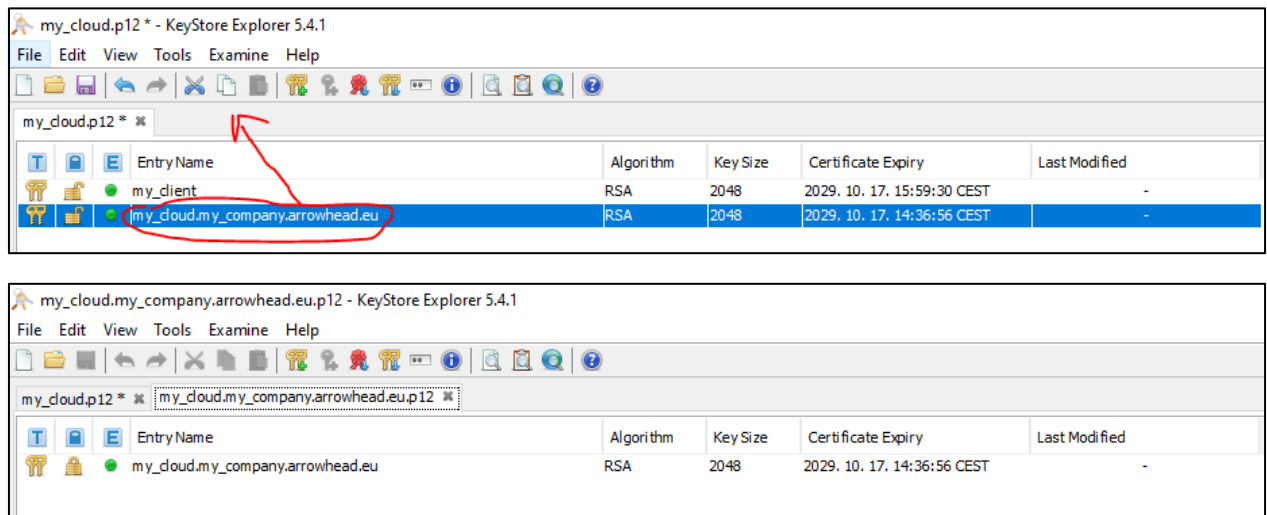
13th STEP:

Set alias (eg.: “my_client”), then give a password.



14th STEP:

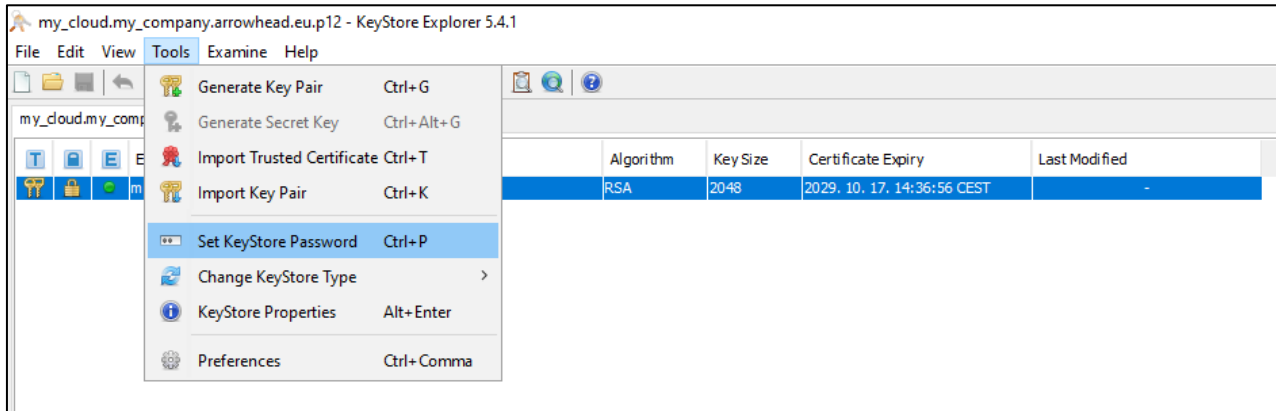
Drag & Drop your newly created key-pair entry to a new tab (It will ask for the password given in the step before.):



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

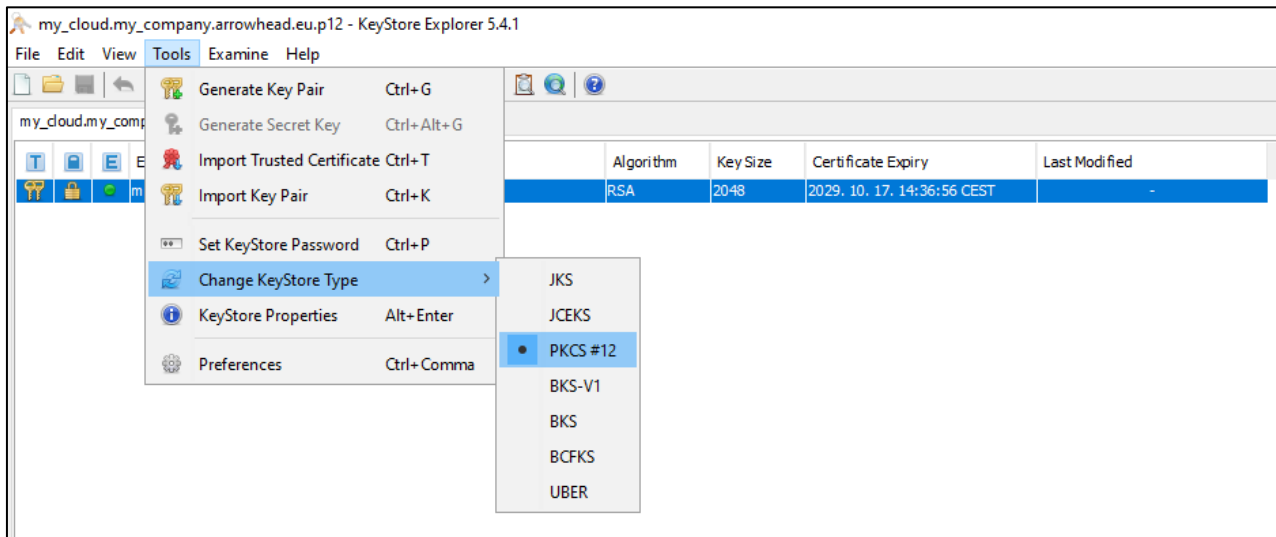
15th STEP:

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



16th STEP:

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



15th STEP:

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

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

