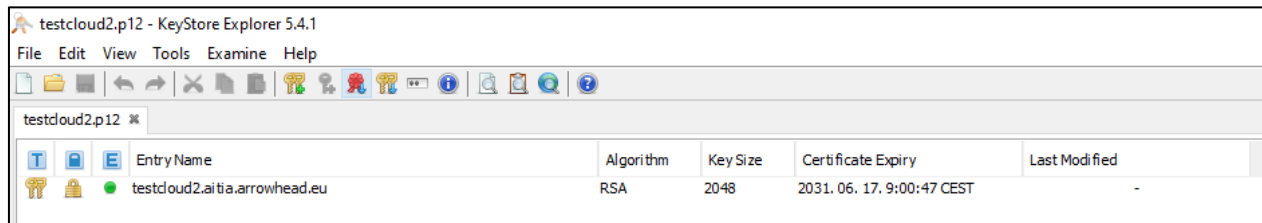


CREATE ARROWHEAD CLIENT SELF SIGNED CERTIFICATE with KeyStore Explorer 5.4.1

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

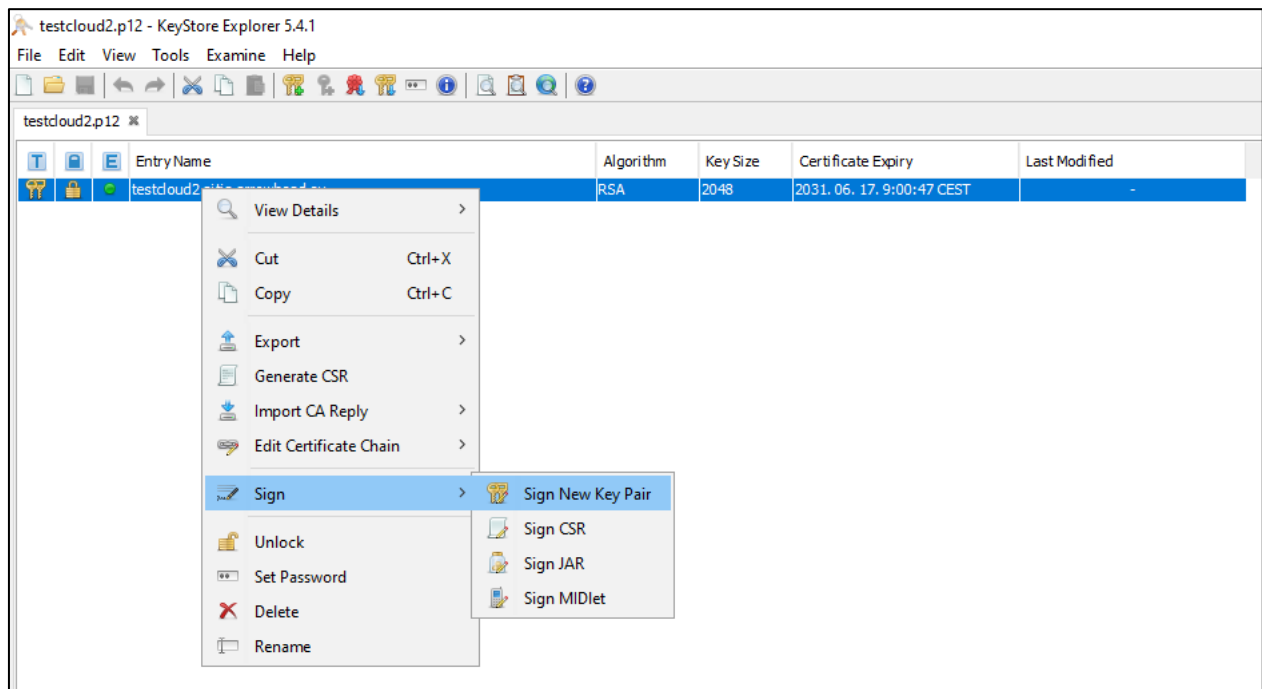
1st STEP:

Open your cloud **p12** certificate file.



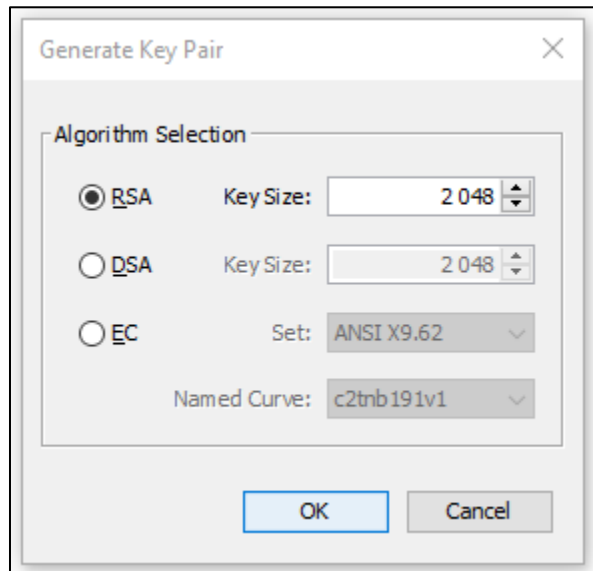
2nd STEP:

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 shows the "Algorithm Selection" section. The "RSA" radio button is selected. The "Key Size" is set to 2048. The "DSA" and "EC" options are unselected. The "Set" dropdown is set to "ANSI X9.62" and the "Named Curve" dropdown is set to "c2tnb191v1".

Generate Key Pair

Algorithm Selection

☒ RSA Key Size: 2 048

☐ DSA Key Size: 2 048

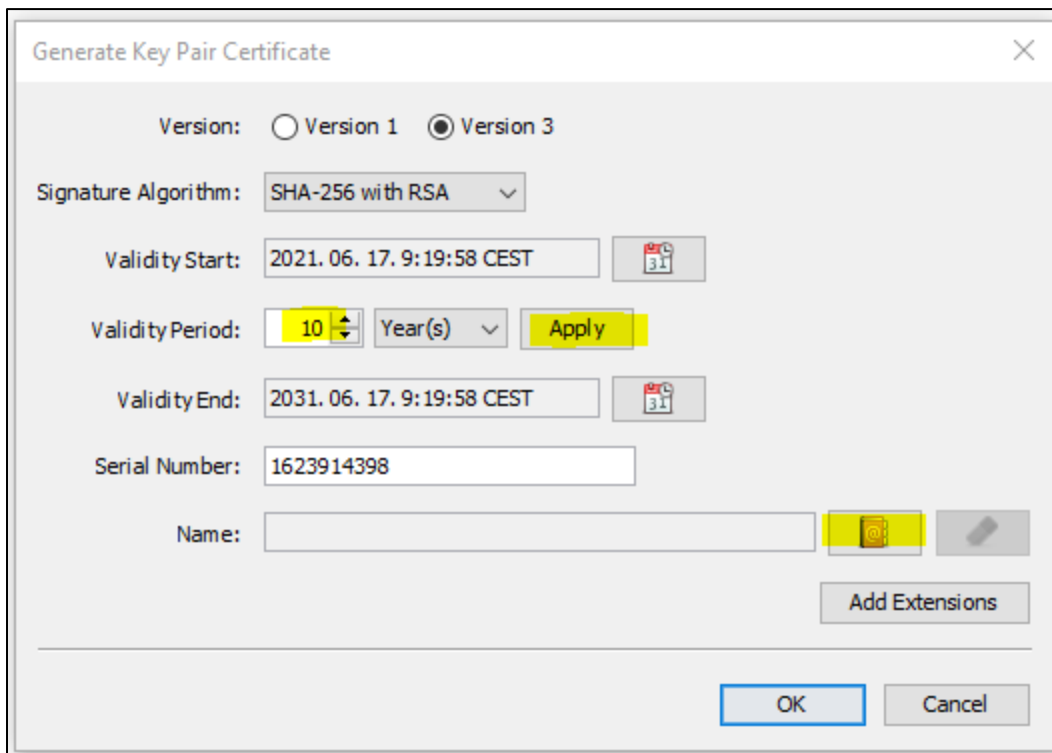
☐ EC Set: ANSI X9.62

Named Curve: c2tnb191v1

OK Cancel

4th STEP:

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



The "Generate Key Pair Certificate" dialog box shows the "Version" set to "Version 3". The "Signature Algorithm" is "SHA-256 with RSA". The "Validity Start" is "2021. 06. 17. 9:19:58 CEST". The "Validity Period" is "10" years. The "Validity End" is "2031. 06. 17. 9:19:58 CEST". The "Serial Number" is "1623914398". The "Name" field is empty. The "Apply" button is highlighted. The "Add Extensions" button is also visible.

Generate Key Pair Certificate

Version: ☐ Version 1 ☒ Version 3

Signature Algorithm: SHA-256 with RSA

Validity Start: 2021. 06. 17. 9:19:58 CEST

Validity Period: 10 Year(s) Apply

Validity End: 2031. 06. 17. 9:19:58 CEST

Serial Number: 1623914398

Name:

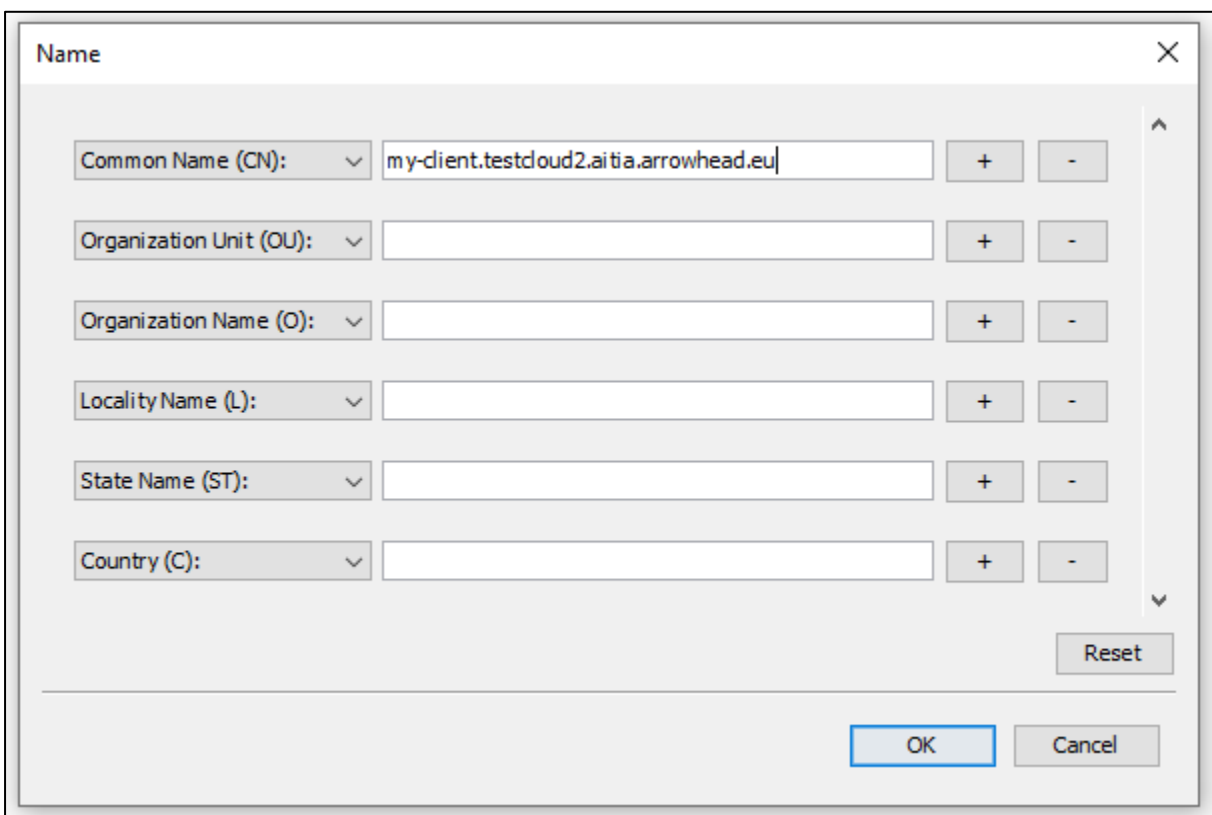
Add Extensions

OK Cancel

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

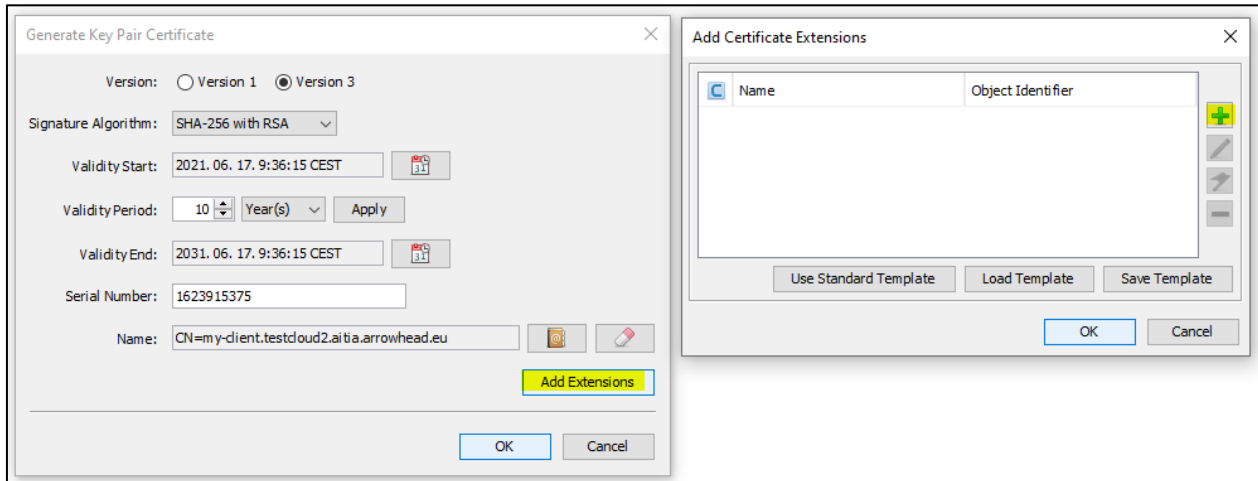


The screenshot shows a 'Name' dialog box with a close button (X) in the top right corner. It contains six rows of input fields, each with a dropdown menu on the left and '+' and '-' buttons on the right. The first row, 'Common Name (CN):', has the text 'my-client.testcloud2.aitia.arrowhead.eu' entered. 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.testcloud2.aitia.arrowhead.eu
Organization Unit (OU):	
Organization Name (O):	
Locality Name (L):	
State Name (ST):	
Country (C):	

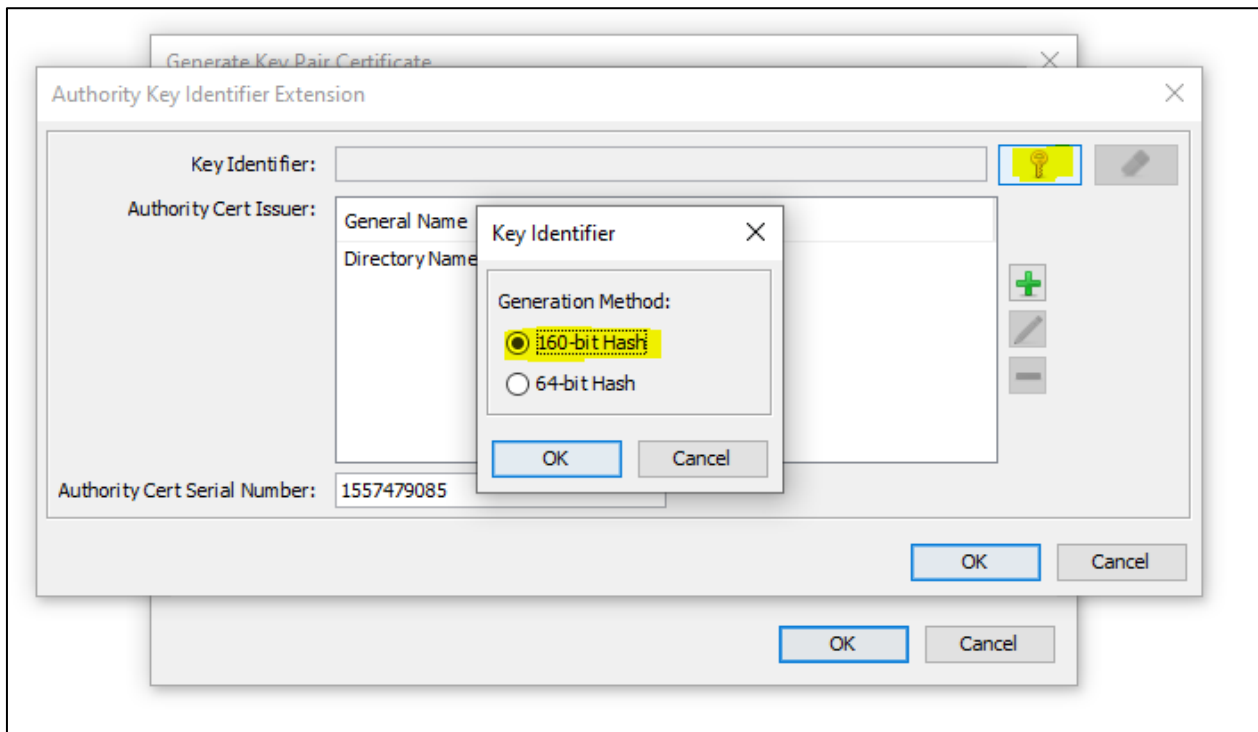
6th STEP:

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



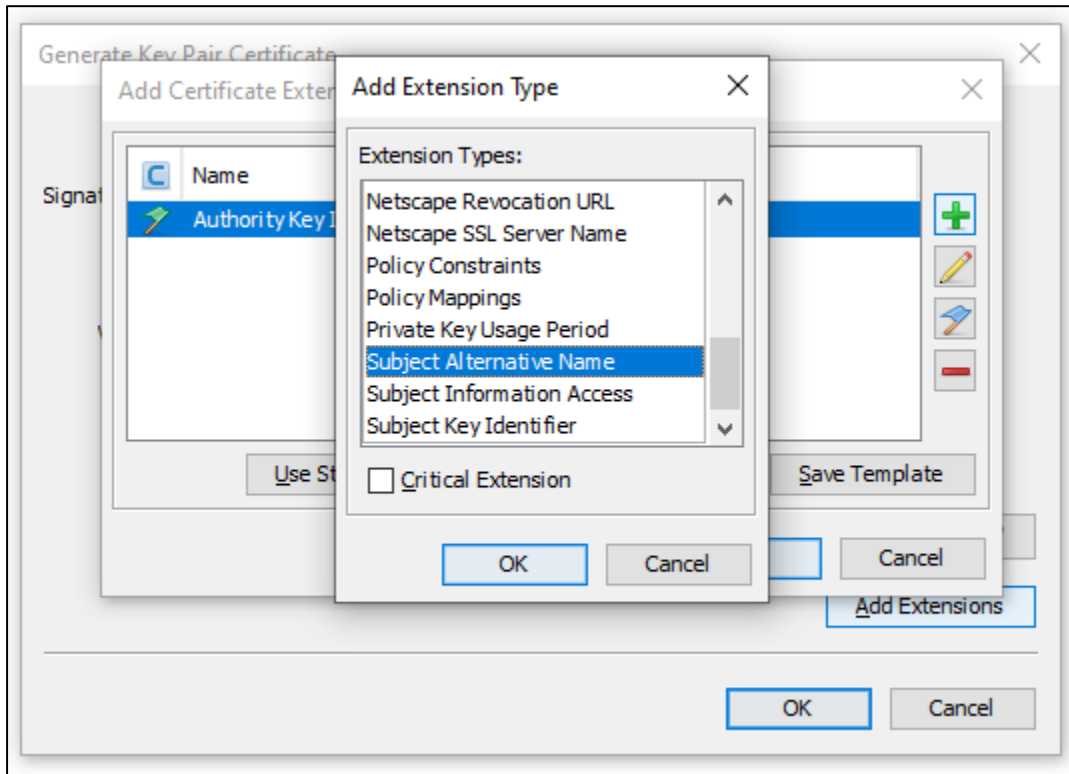
7th STEP:

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



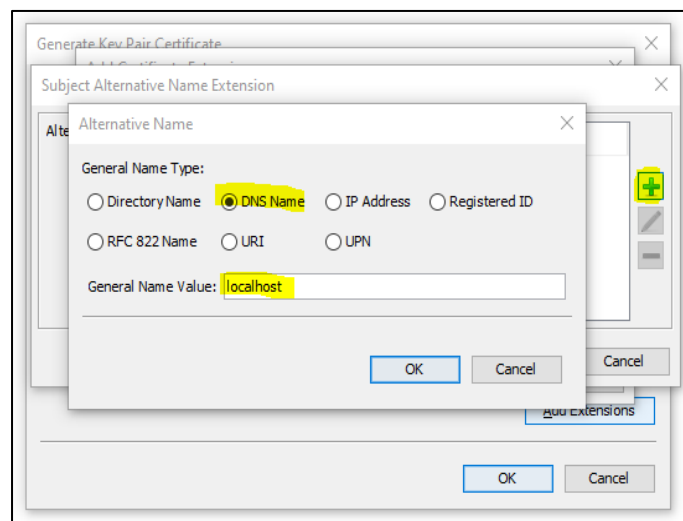
8th STEP:

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



9th STEP:

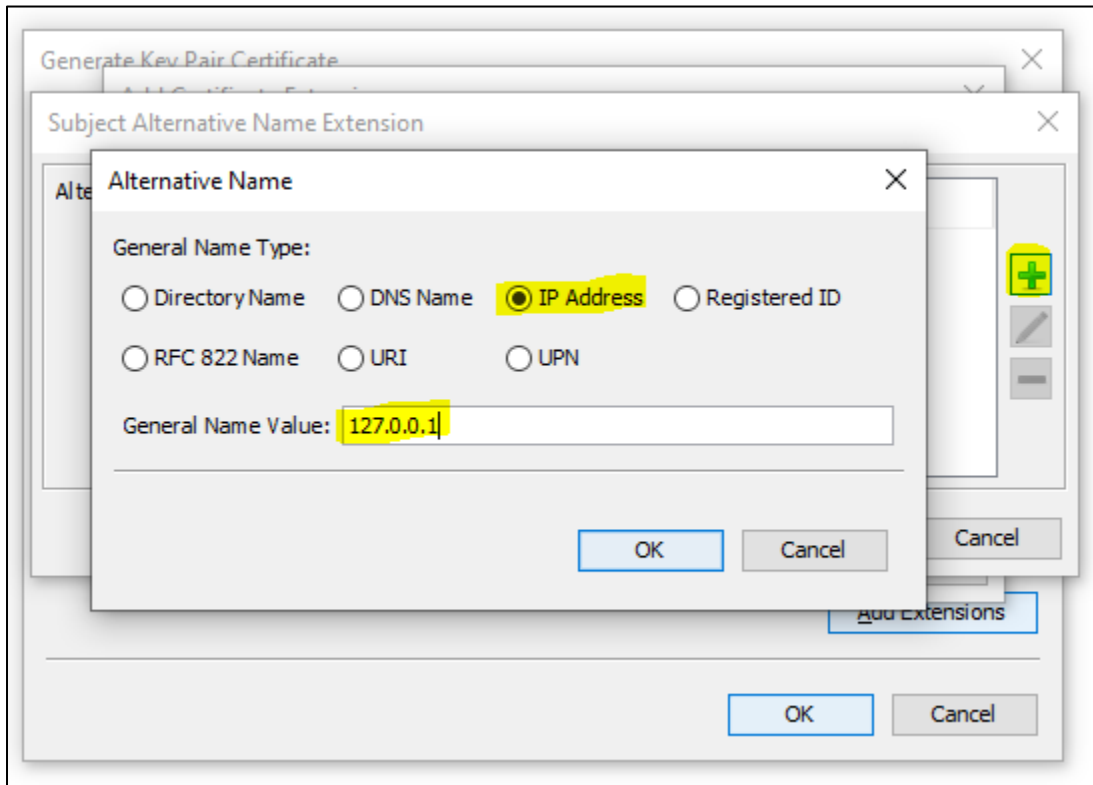
Click on green “+” button, select “DNS Name” and fill the “General Name Value” with “localhost” and press “OK”:



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

10th STEP:

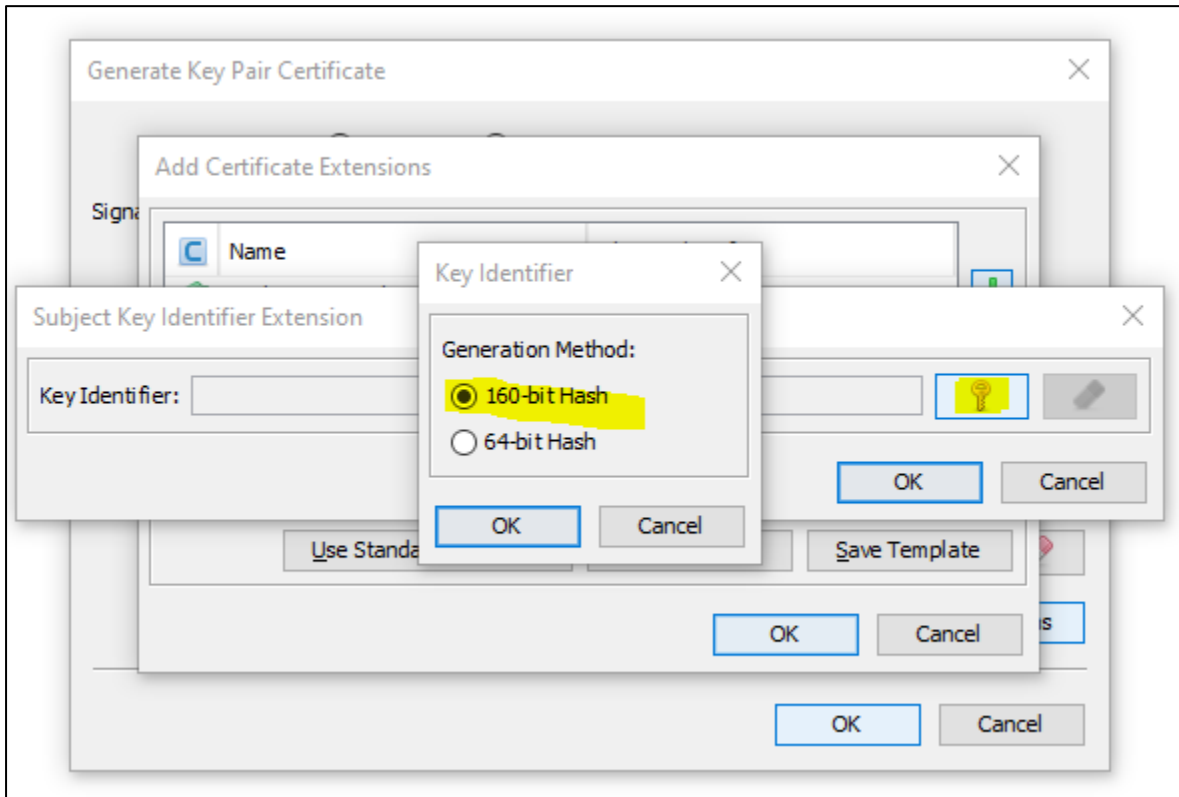
Click on green “+” button again, select “IP Address” and fill the “General Name Value” with “127.0.0.1” and press “OK”:



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

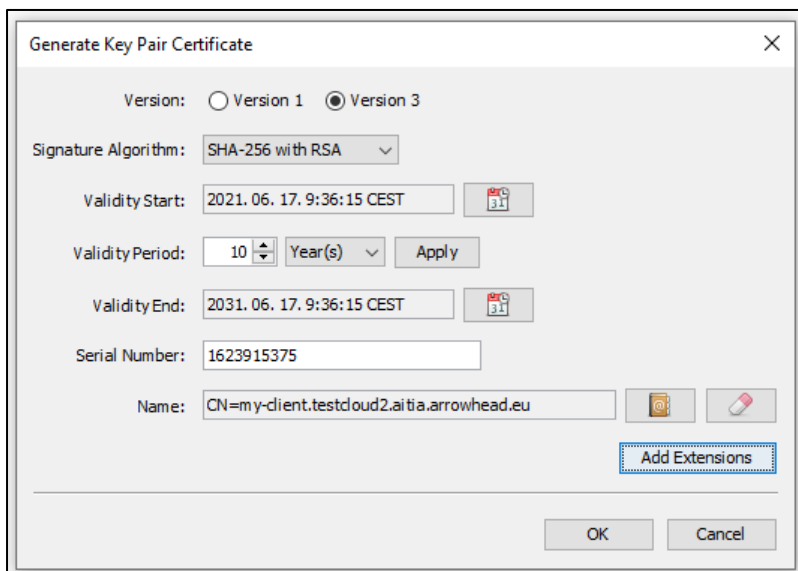
11th STEP:

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”:



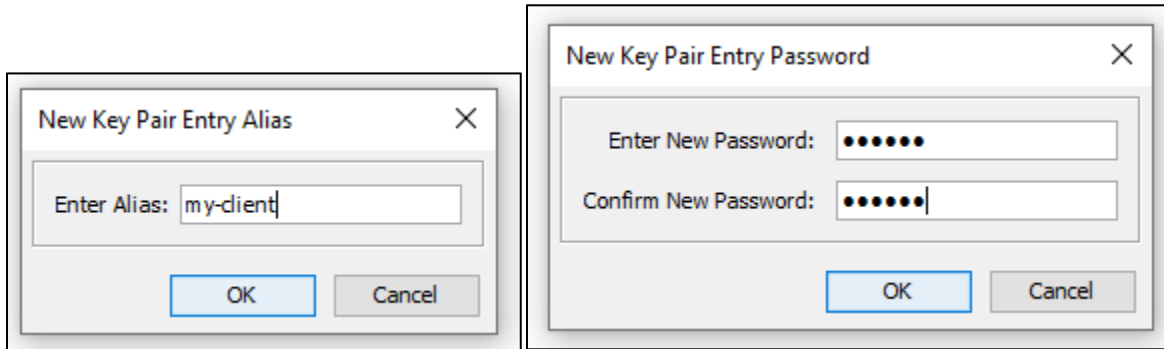
12th STEP:

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



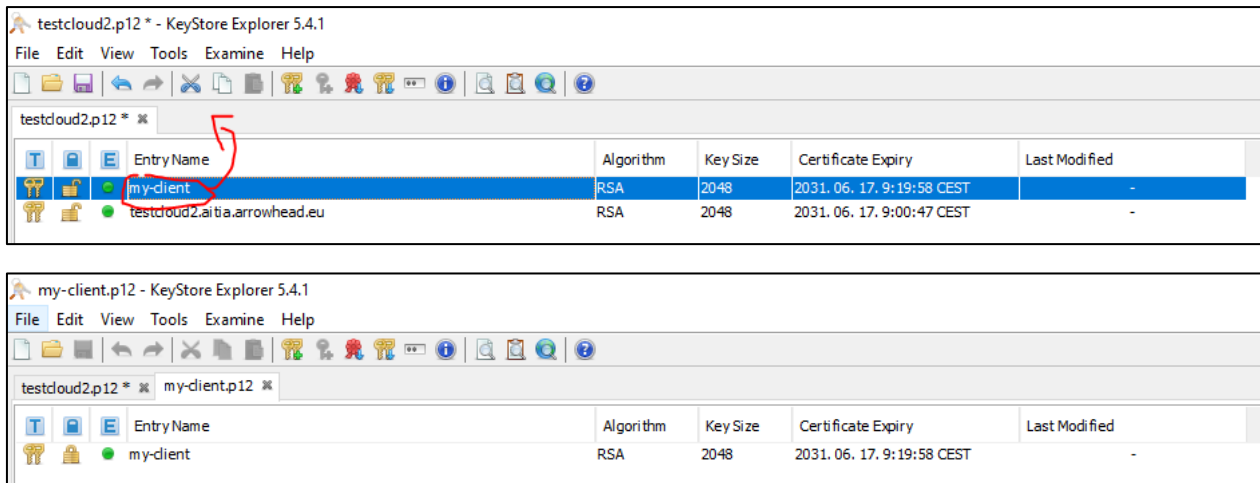
13th STEP:

Set alias (eg.: “my-client”), then give a password.



14th STEP:

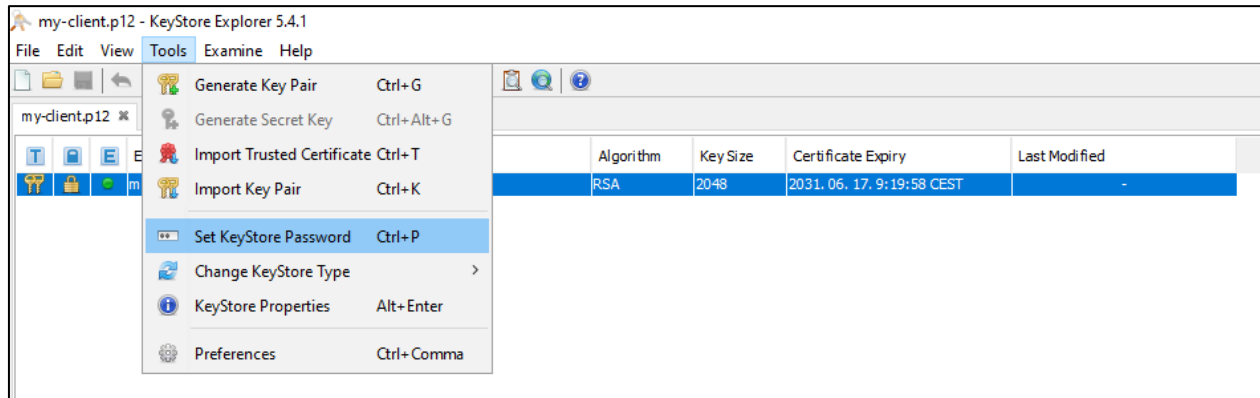
Drag & Drop your newly created key-pair entry to a new tab (It will ask for the password given in the step before.):



Close the “testcloud2.p12” and DO NOT SAVE THE CHANGES!

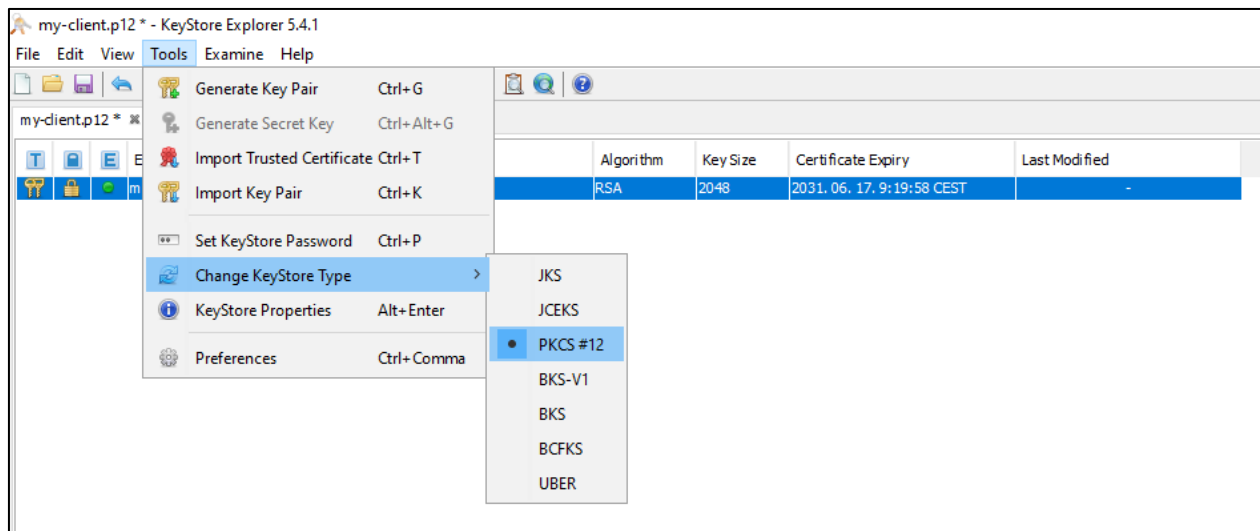
15th STEP:

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-client.**p12**.

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

