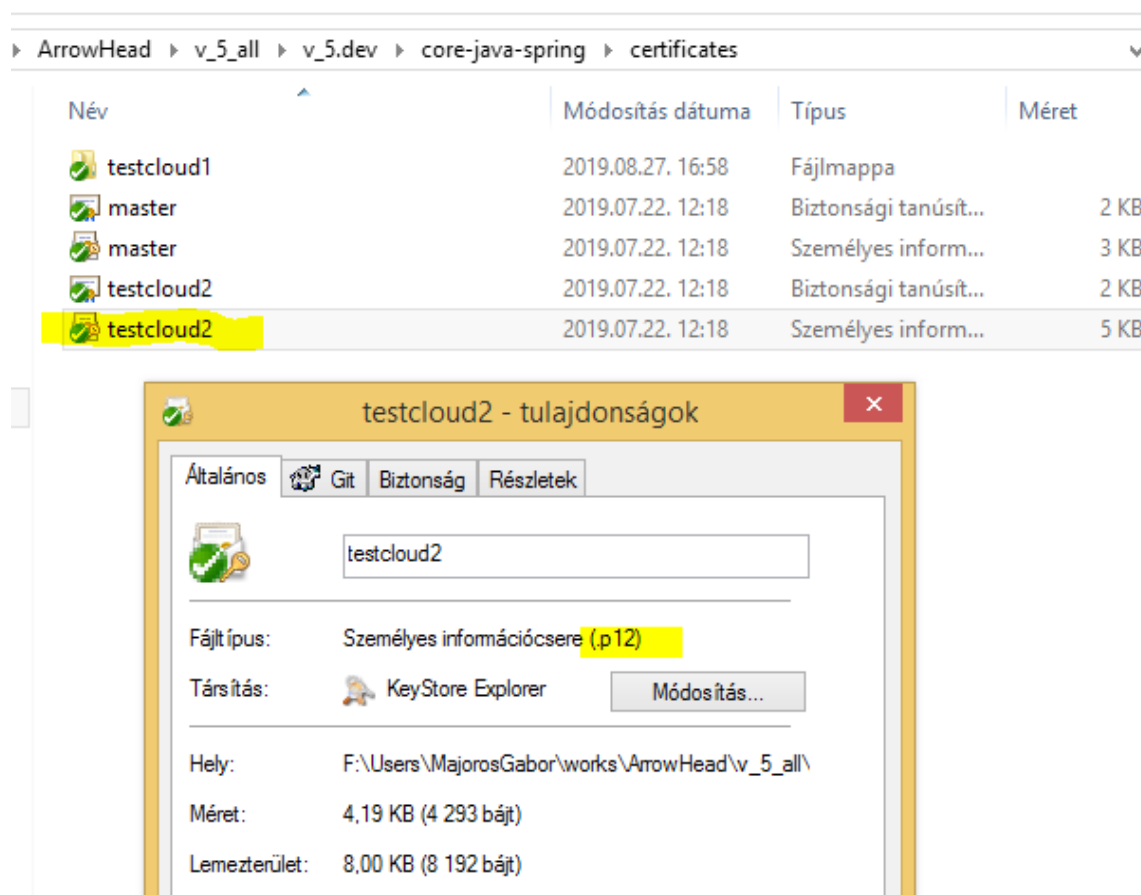
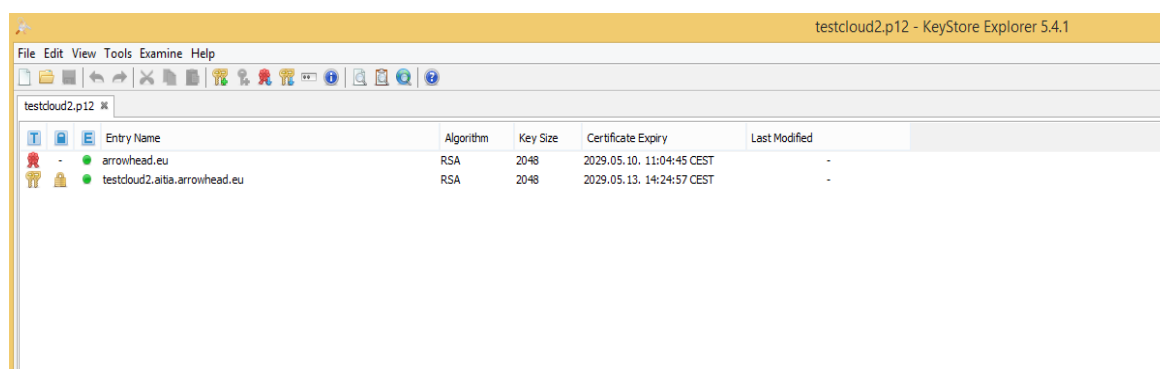


Sample Client System Certificate Generation _ With KeyStoreExplorer 5.4.1

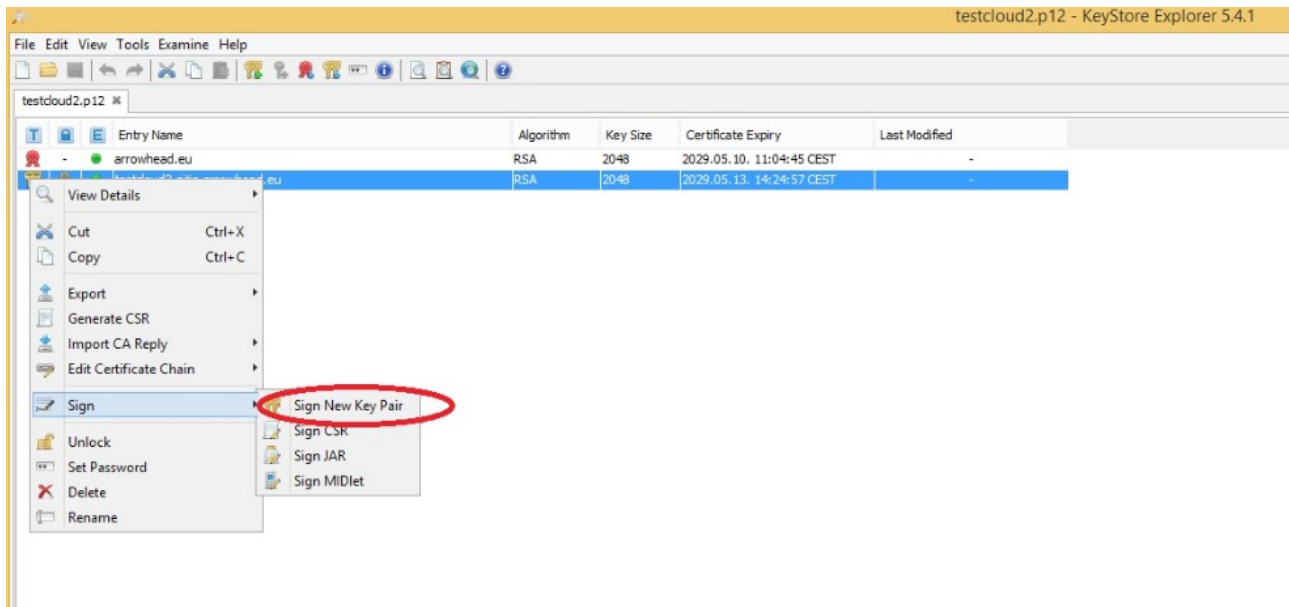
Start with cloud certificate:



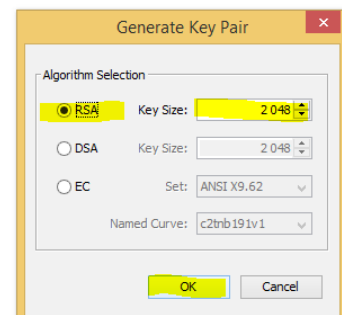
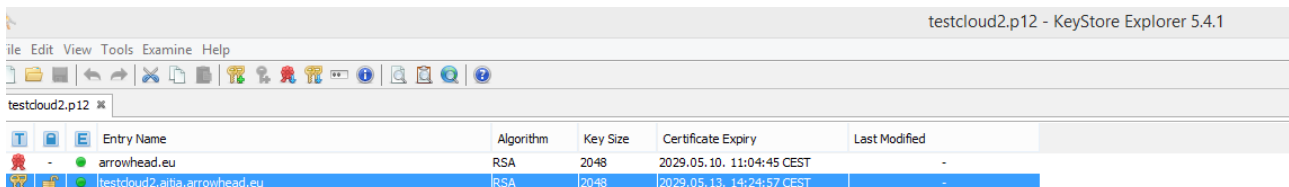
Open it with KeyStoreExplorer:



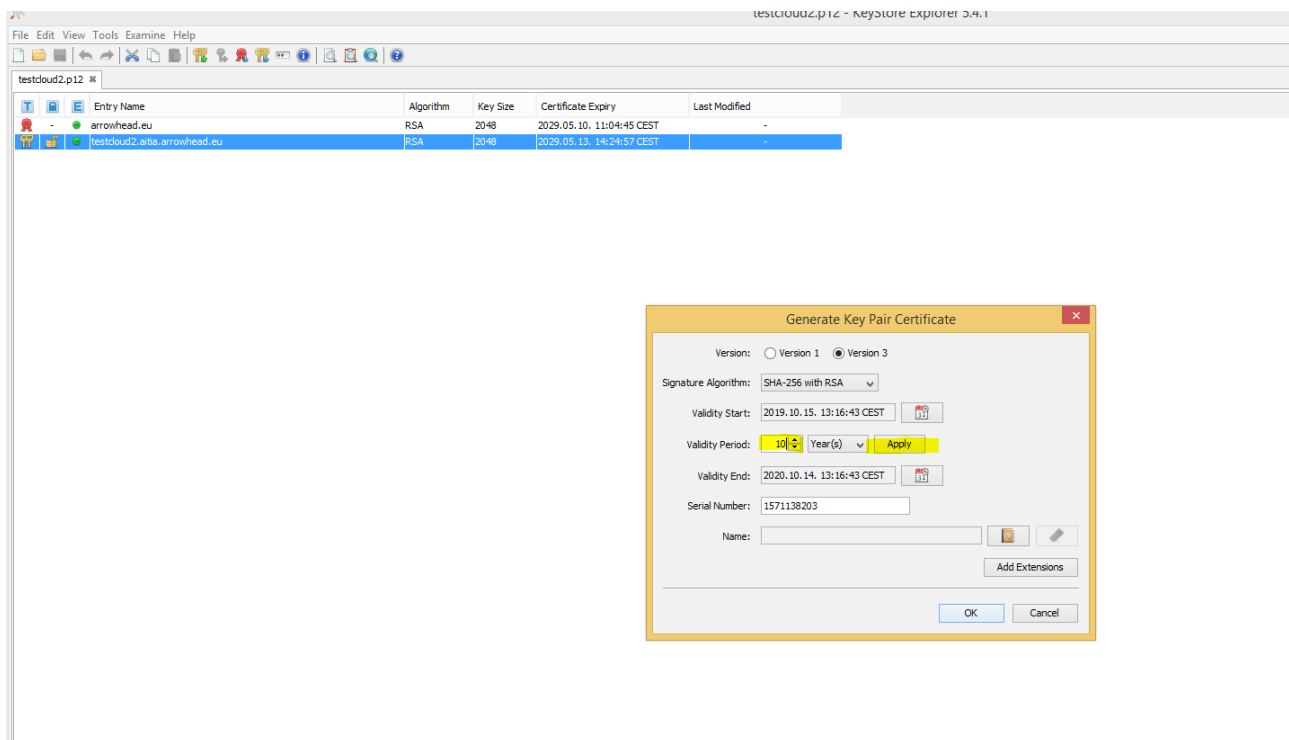
Right-click on keyPair and select SignNewKeyPair:



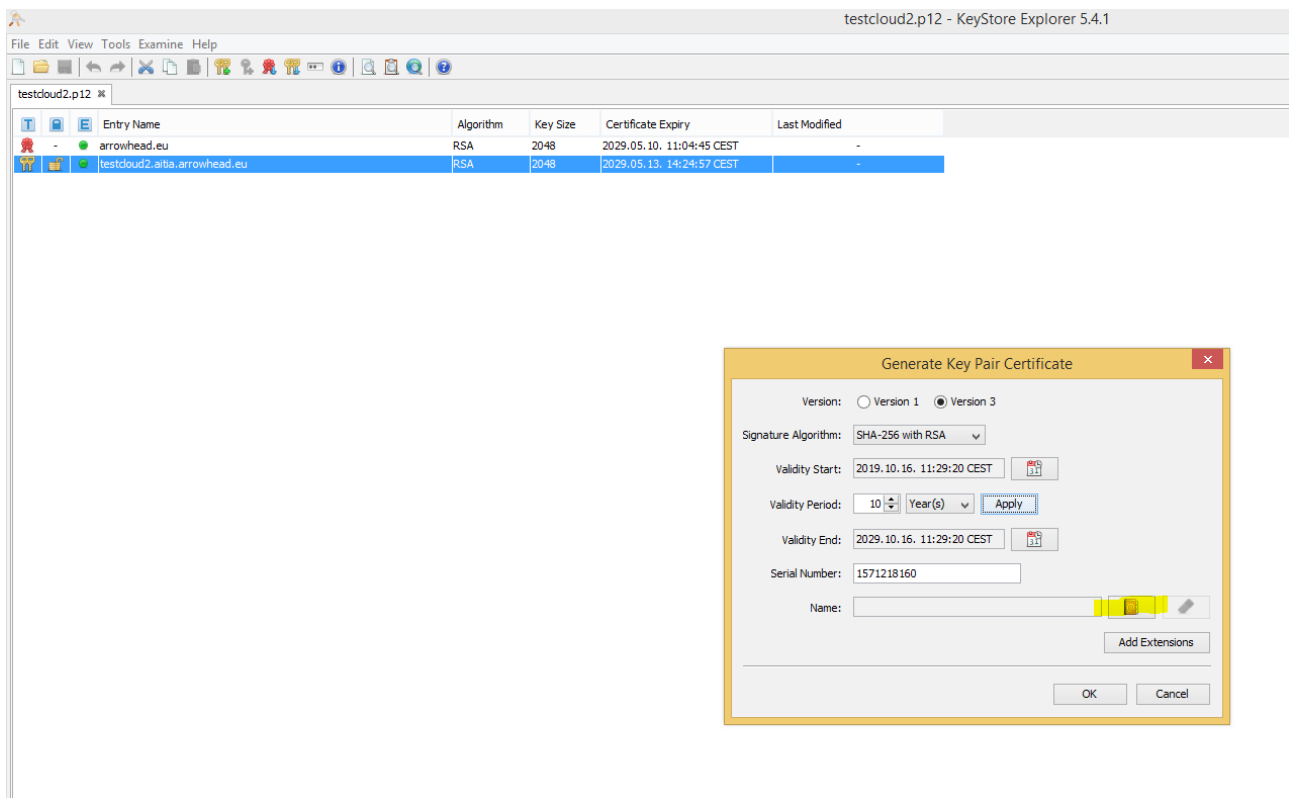
Select RSA.
Set Key Size to 2048.
Then click Ok on Generate Key Pair popup window.



Set validity Period to 10 year.
Click Apply !



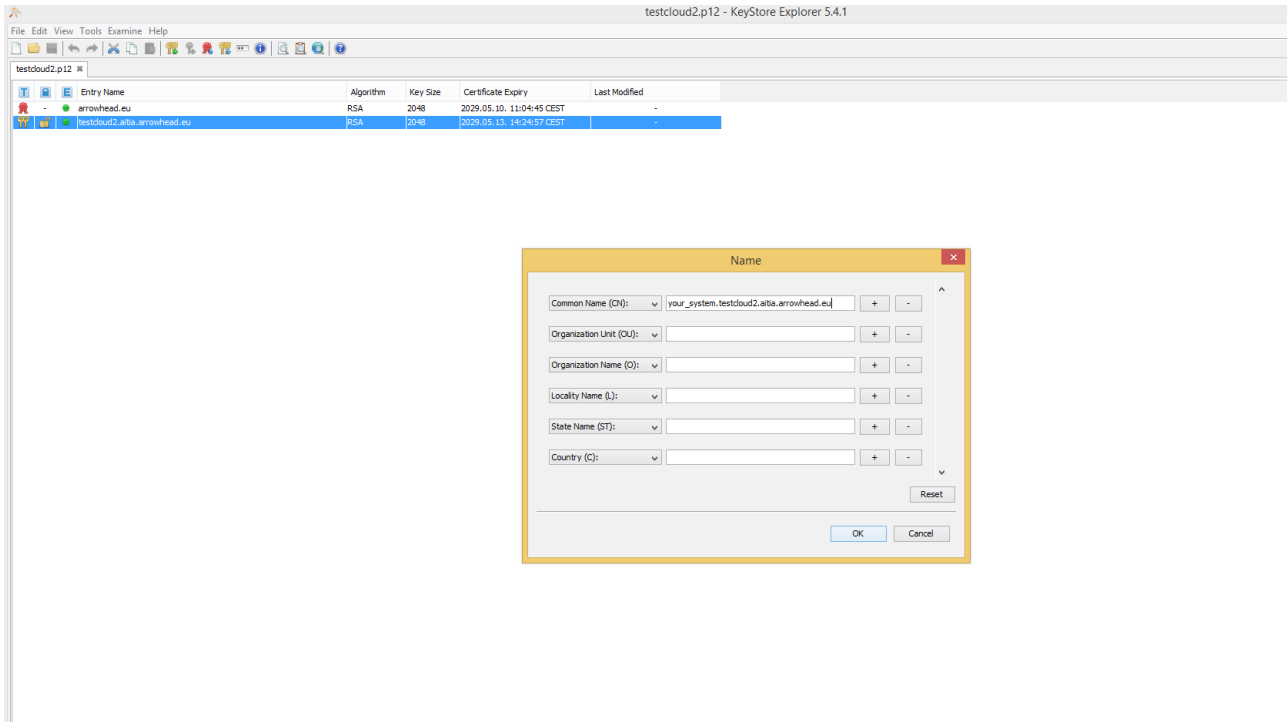
Click on Edit name (Symbol of a book with @ sign).



Set Common Name (CN).

Example: your_system.testcloud2.aitia.arrowhead.eu

Then click Ok on Name popup window.



Click Add Extensions

testcloud2.p12 - KeyStore Explorer 5.4.1

File Edit View Tools Examine Help

testcloud2.p12

Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
- arrowhead.eu	RSA	2048	2029.05.10. 11:04:45 CEST	-
testcloud2.altia.arrowhead.eu	RSA	2048	2029.05.13. 14:24:57 CEST	-

Generate Key Pair Certificate

Version: ☐ Version 1 ☒ Version 3

Signature Algorithm: SHA-256 with RSA

Validity Start: 2019.10.16. 11:32:21 CEST

Validity Period: 10 Year(s) Apply

Validity End: 2029.10.16. 11:32:21 CEST

Serial Number: 1571218341

Name: CN=your_system.testcloud2.altia.arrowhead.eu

Add Extensions

OK Cancel

Click green +.

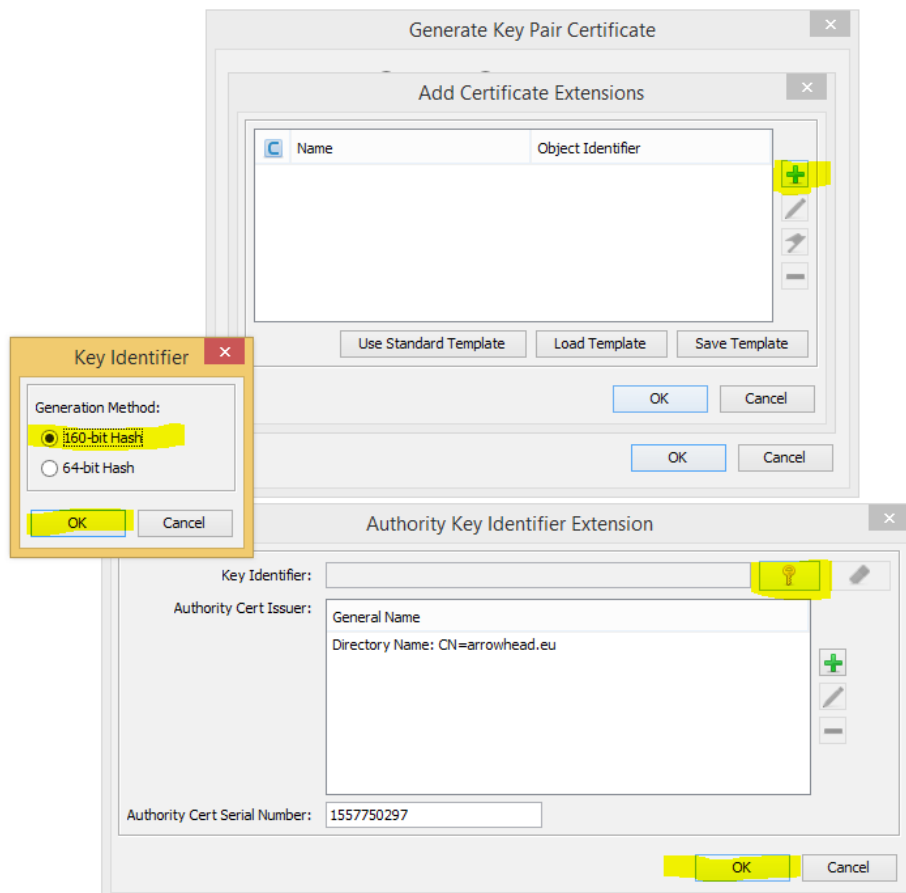
Select Add Authority Key Identifier.

Click key symbol.

Select the 160-bit Hash.

Click Ok on Key Identifier popup window.

Then click Ok on Authority Key Identifier Extension popup window.



Click green +.

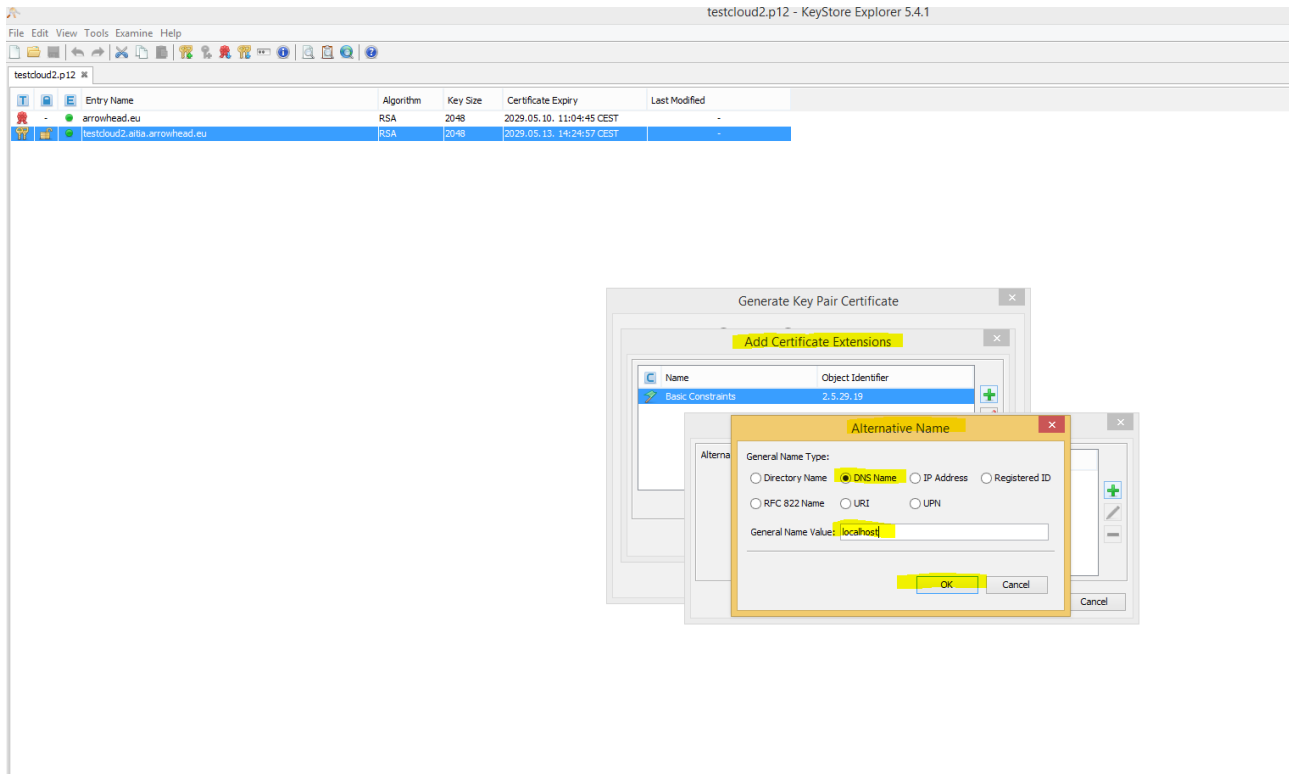
Select Add Subject Alternative Name.

Select DNS Name

Set General Name Value: localhost

Then click ok on the Alternative Name popup window.

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



Click green +.

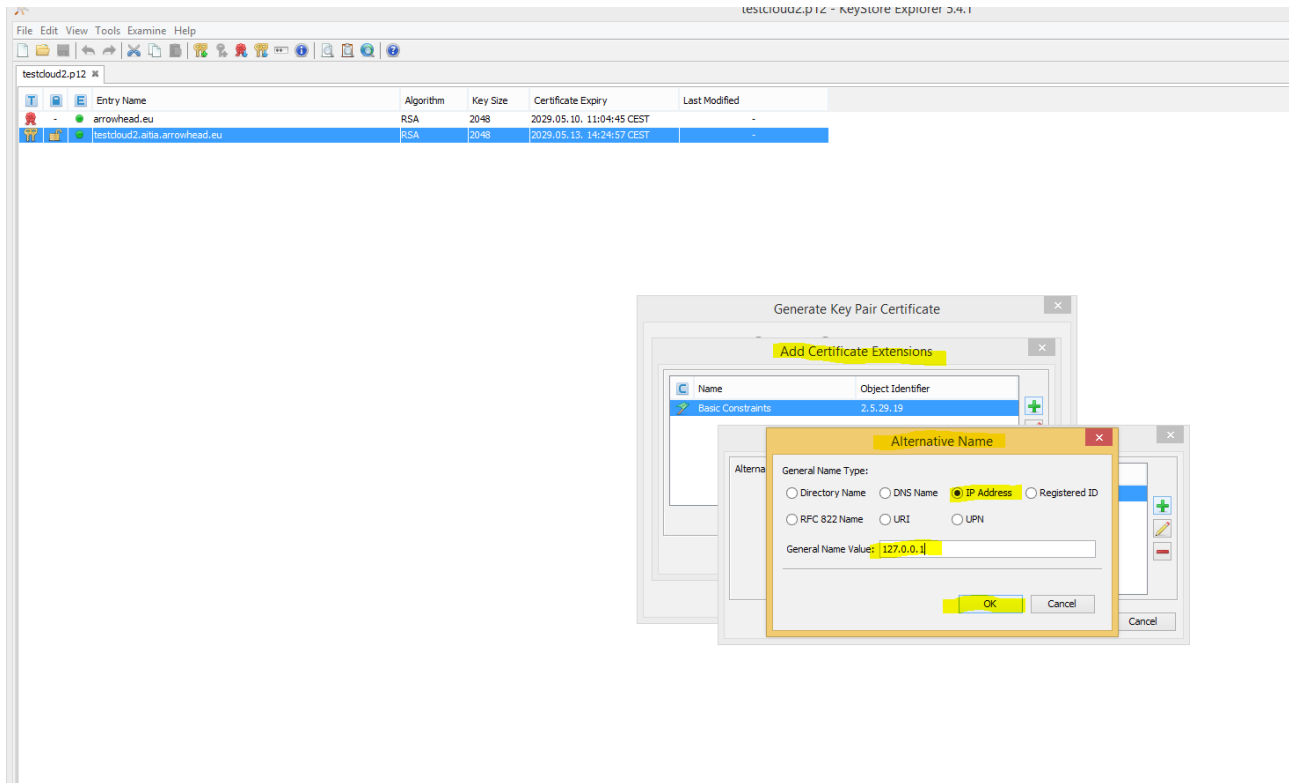
Select IP Address

Set General Name Value: 127.0.0.1

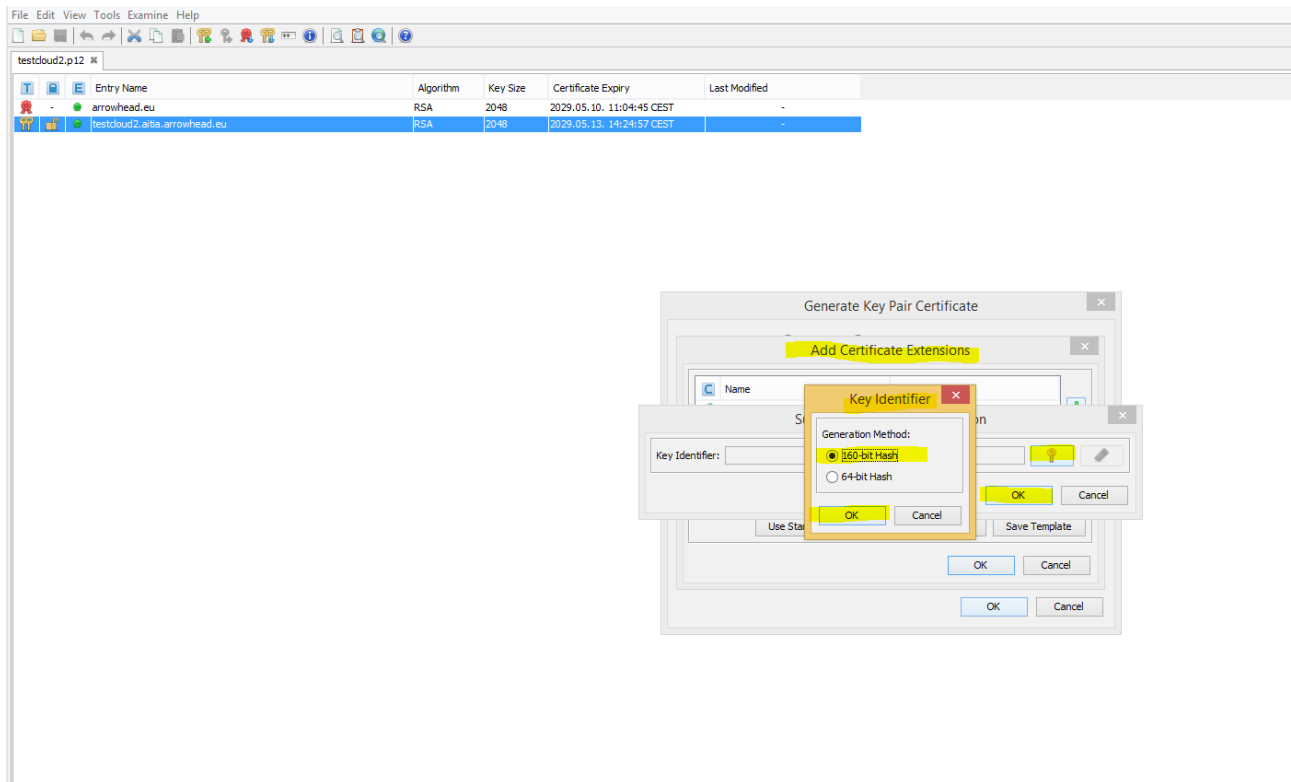
Then click ok on the Alternative Name popup window.

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

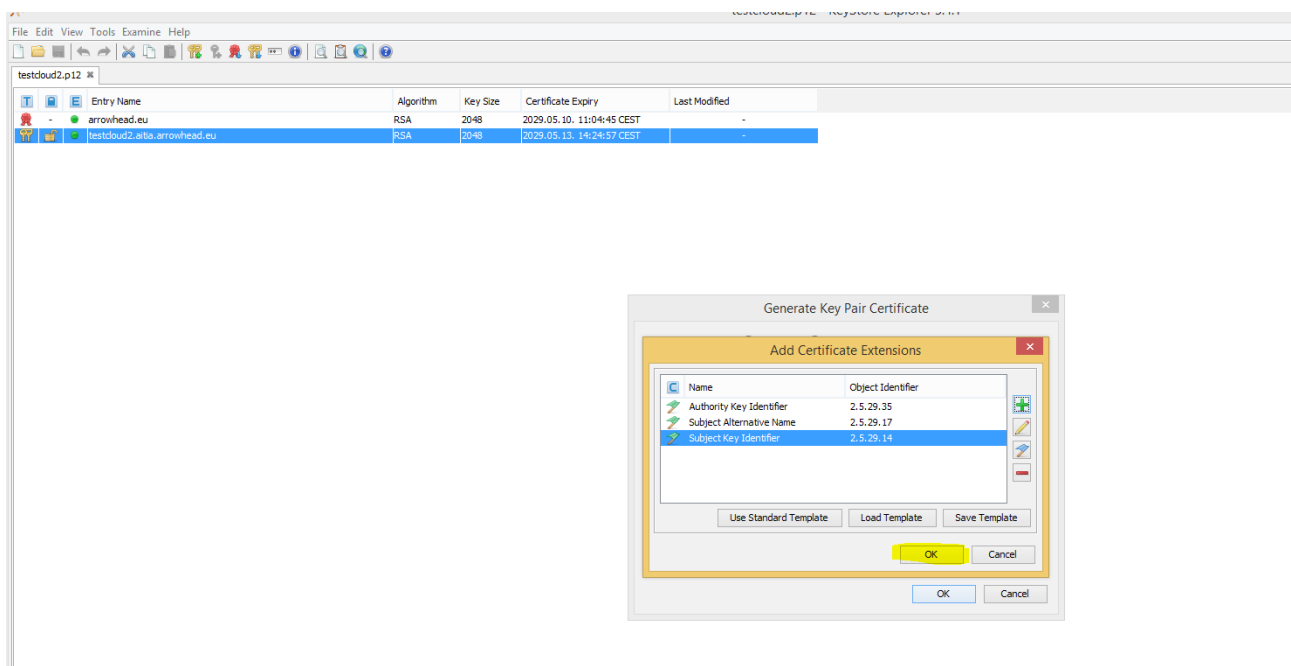
Then click ok on Subject Alternative Name Extension popup window.



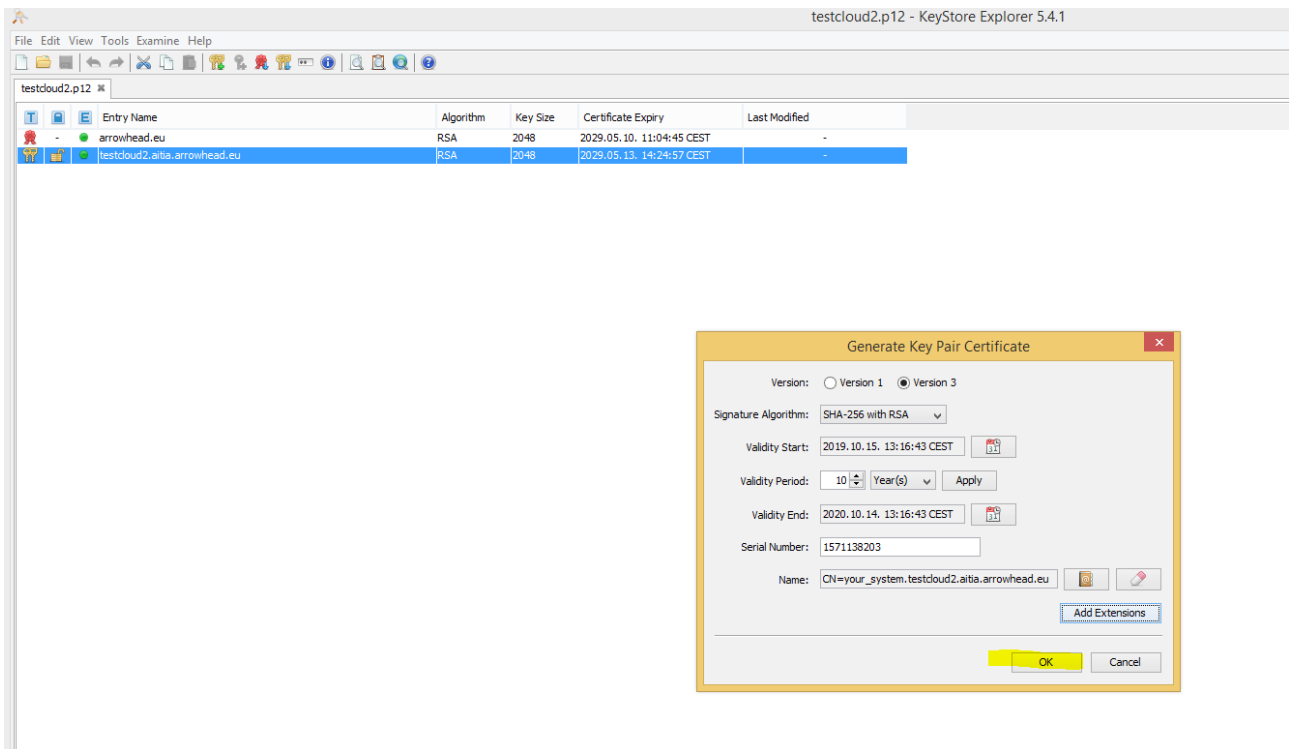
Click green +.
 Select Subject Key Identifier
 Click Ok on Add Extension Type popup window.
 Click on the key symbol.
 Select a 160-bit Hash.
 Click Ok on Key Identifier popup window.
 Click Ok on Subject Key Identifier popup window.



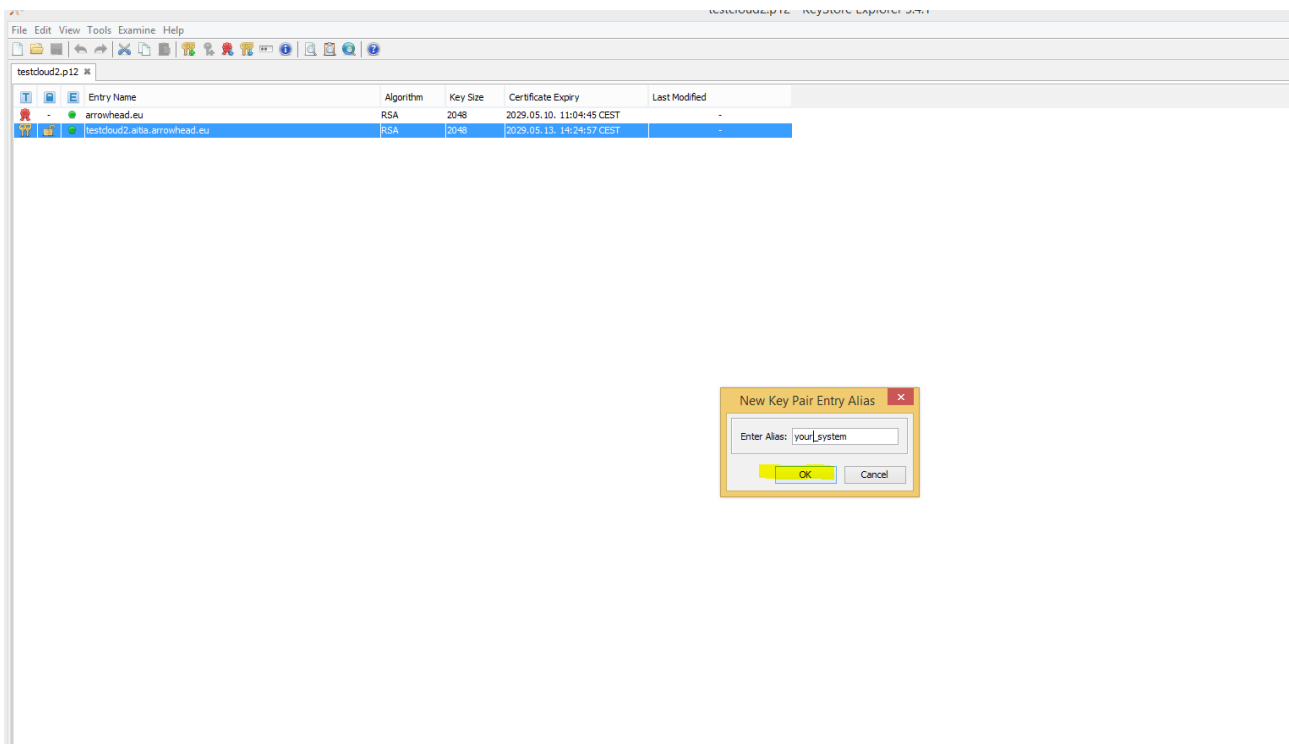
Finished adding extensions - Click Ok on Add Certificate Extensions popup window.



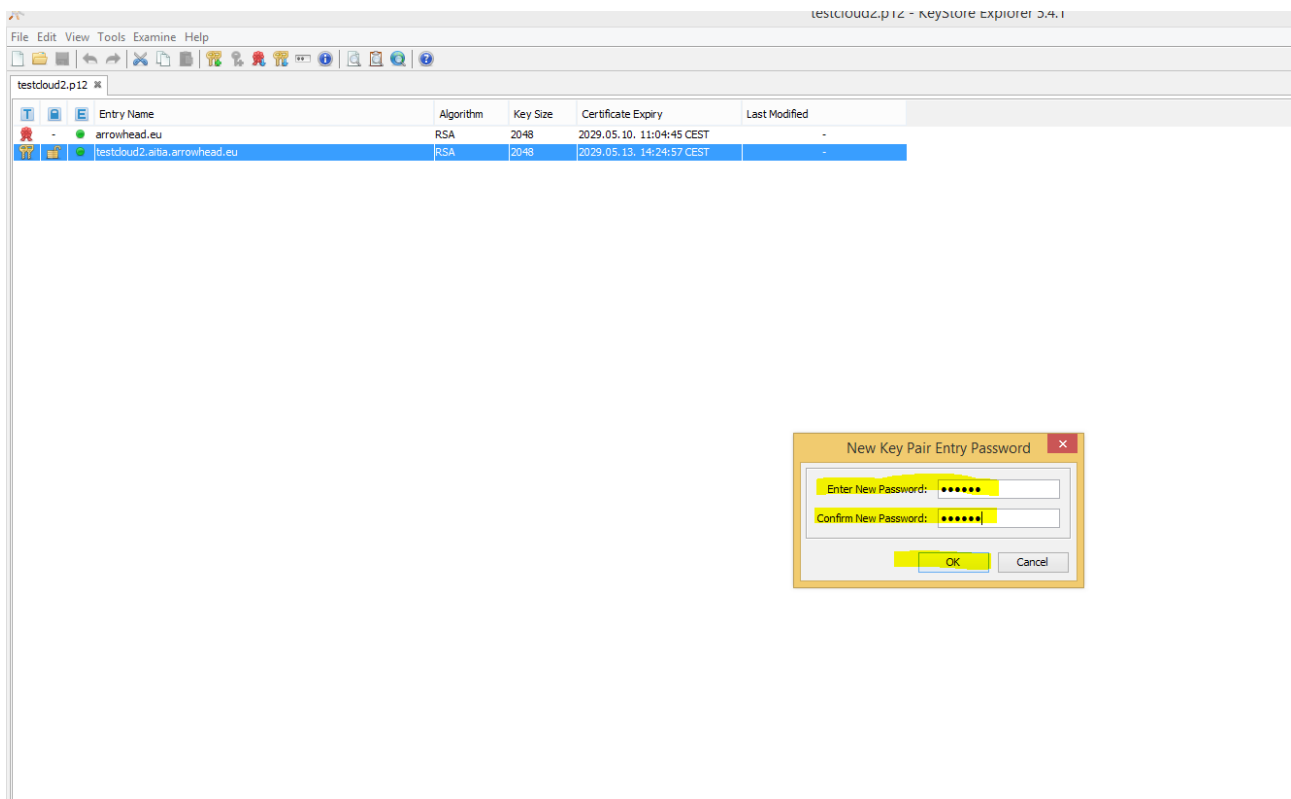
Click Ok on Generate Key Pair Certificate popup window.



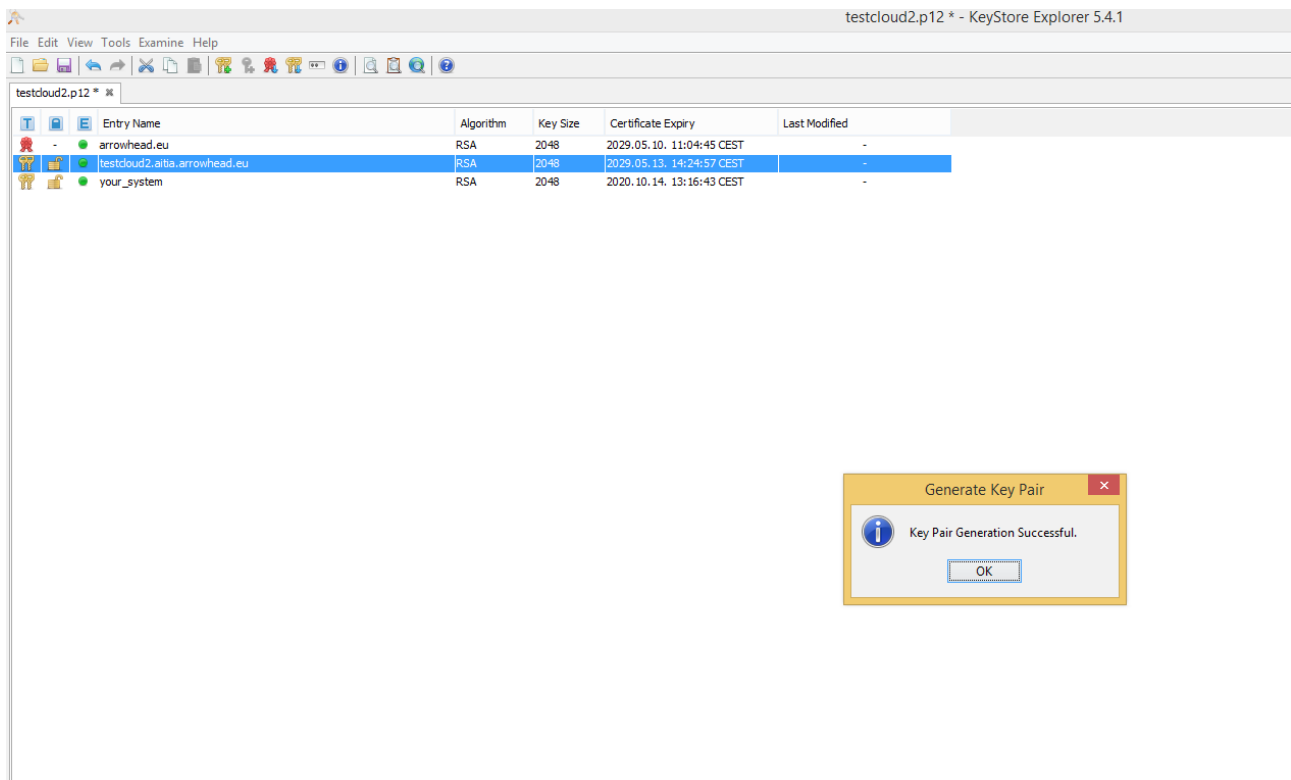
Edit alias of your new keypair – for example : your_system.
Click Ok.



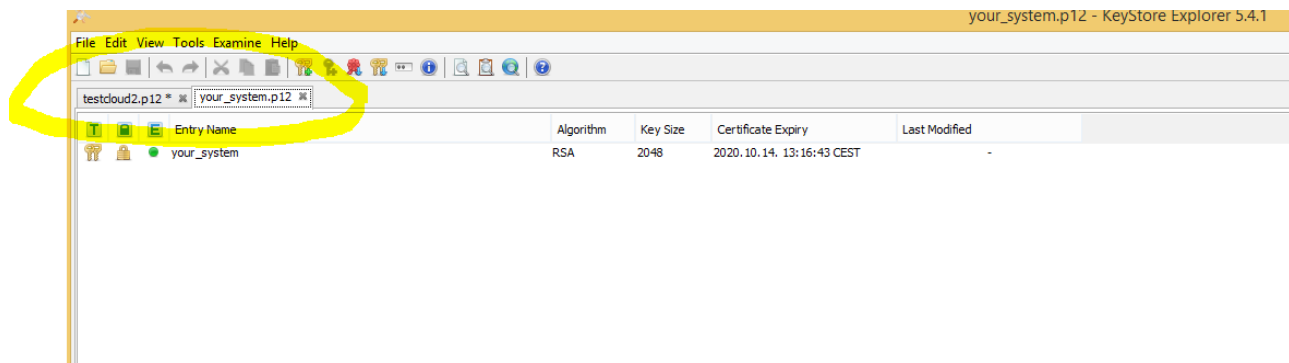
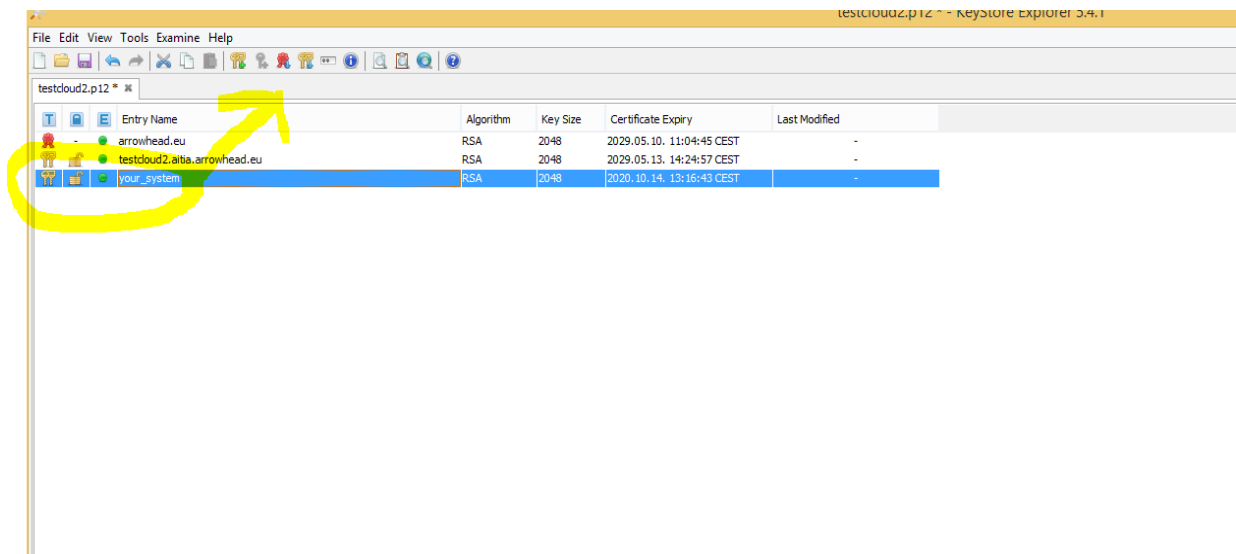
Enter Password for your new keyPair



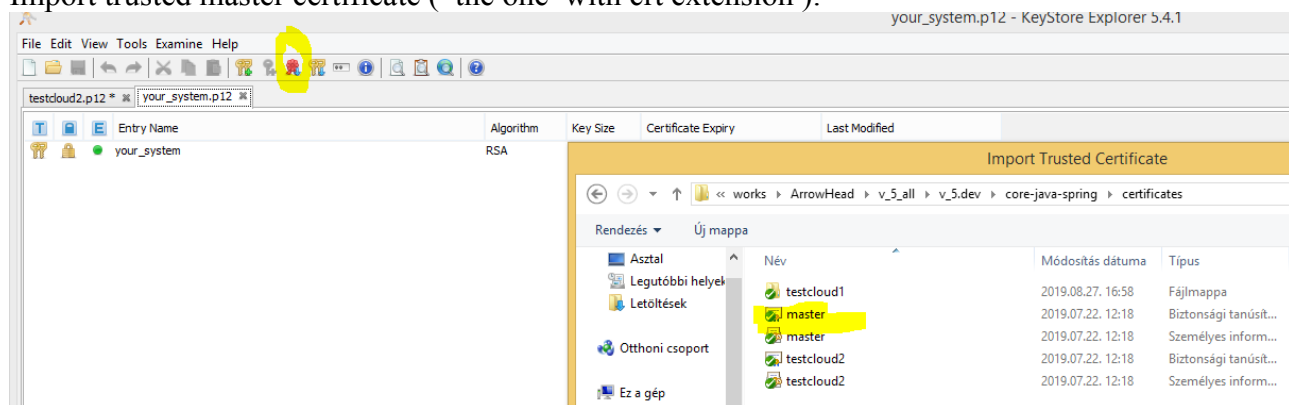
You should see a similar popup window:



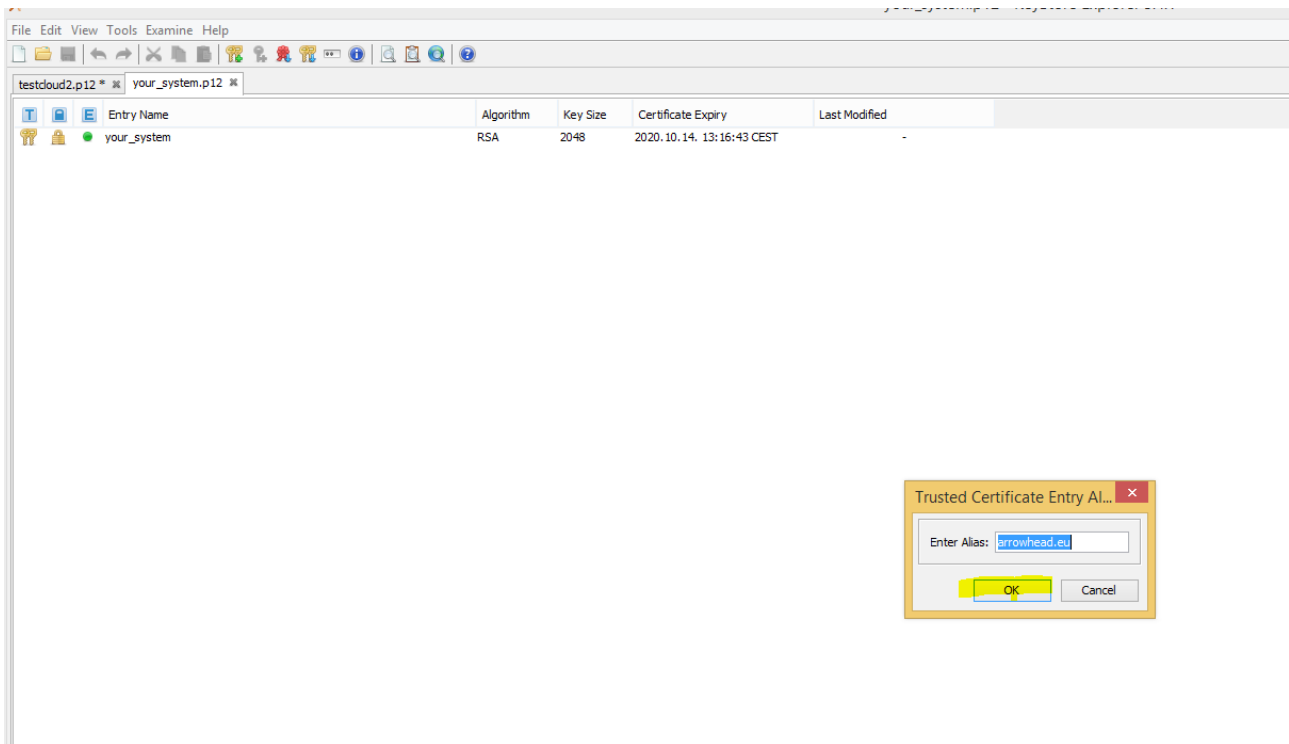
Click and drop the newly generated keypair to a new tab.



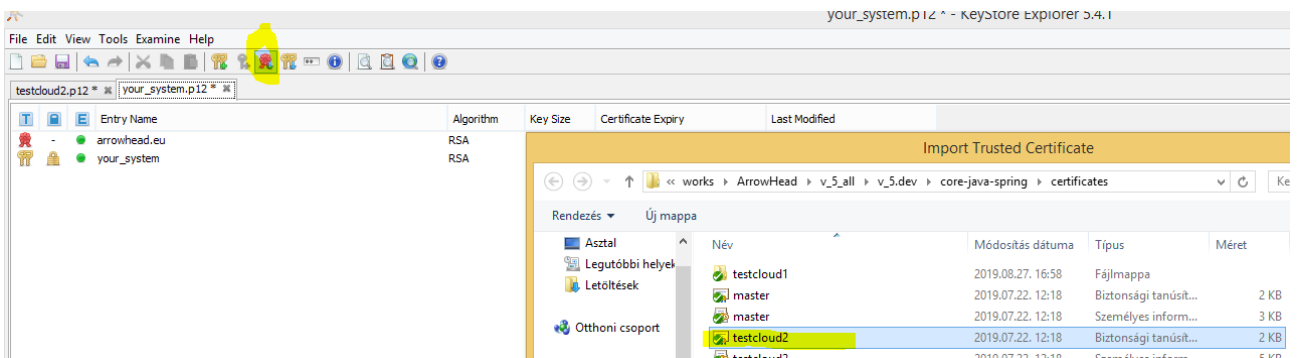
Import trusted master certificate (the one with crt extension):



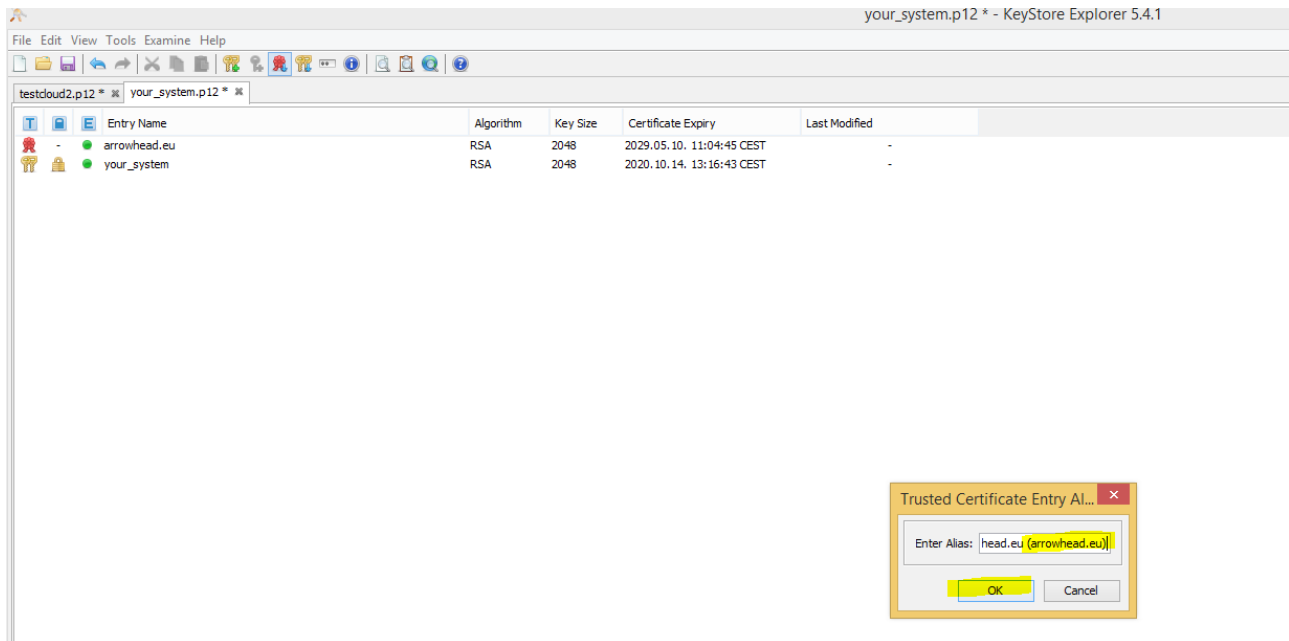
Edit imported master certificate alias – for example: arrowhead.eu
Click ok.



Import trusted cloud certificate (the one with crt extension):

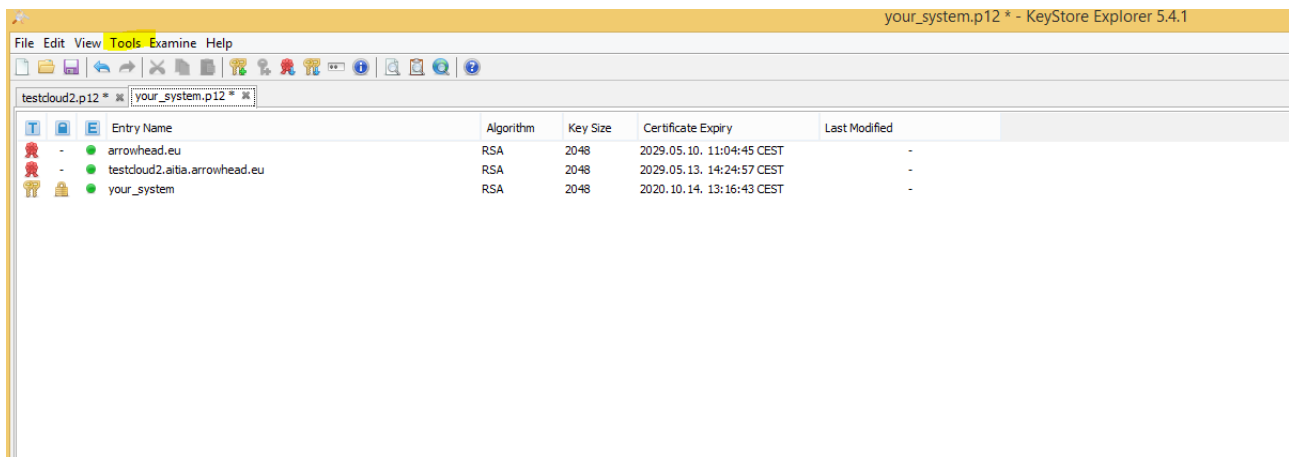


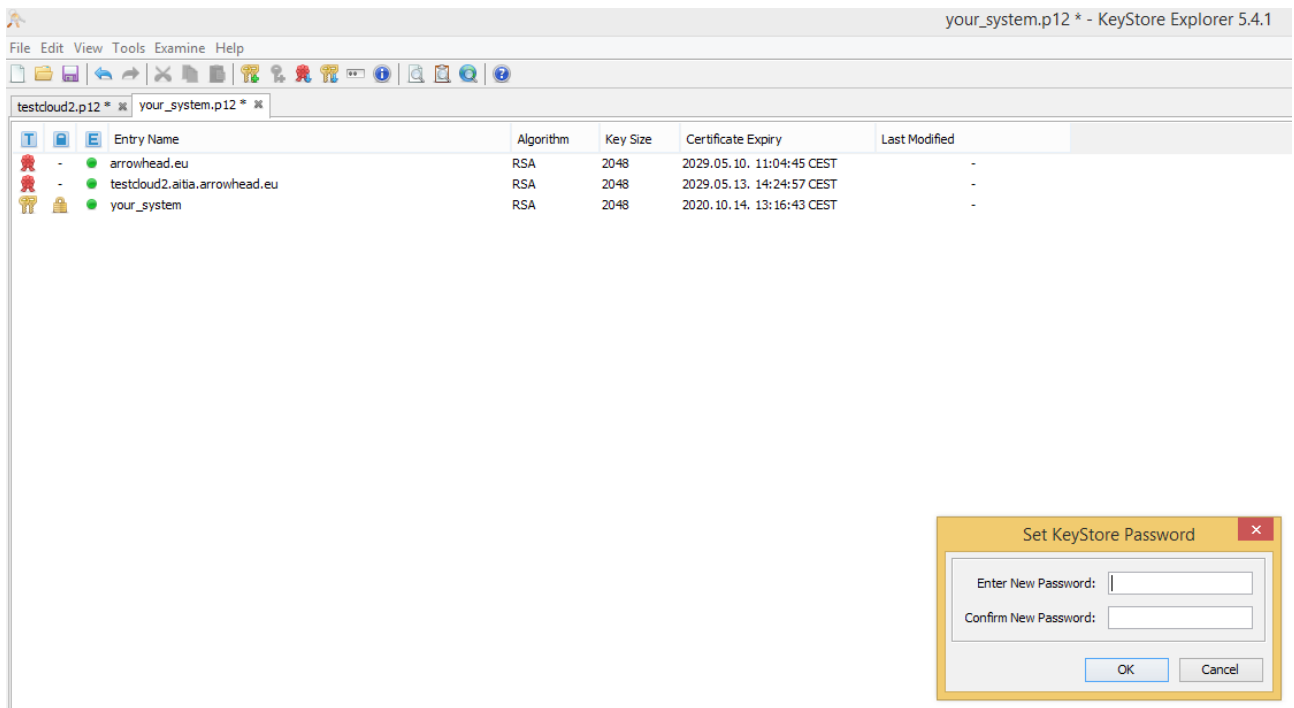
Edit trusted cloud certificate alias – for example : testcloud2.aitia.arrowhead.eu
Click Ok.



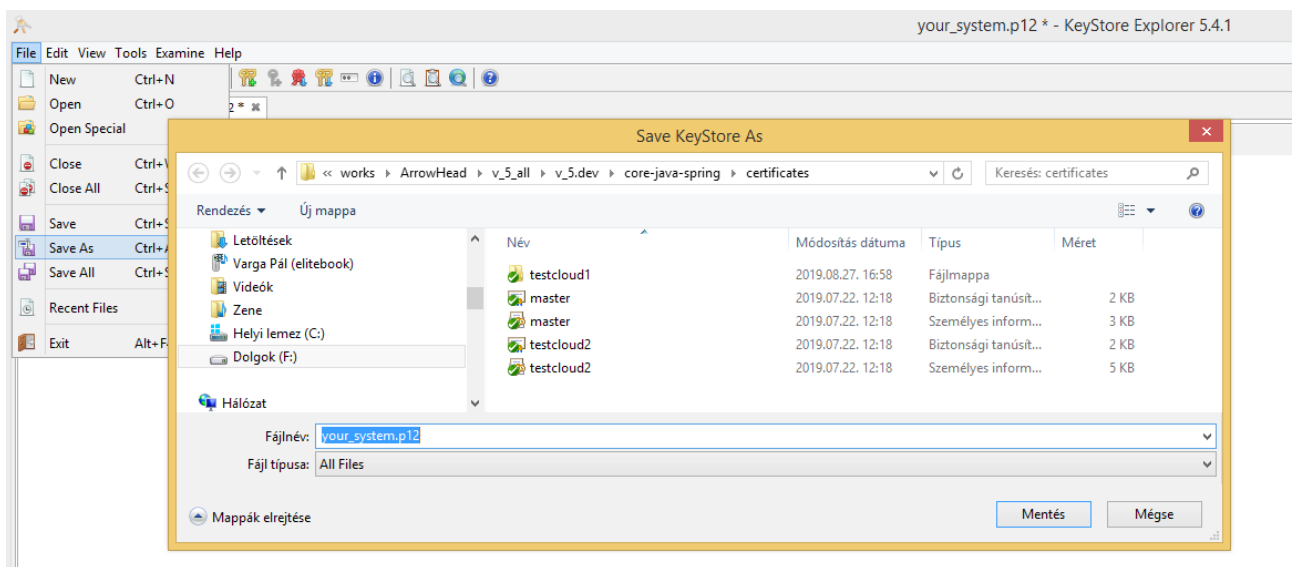
Set Keystore Password:

Click Tools.
Click Set Key Store Password.
Enter Password for KeyStore.
Click Ok.





Save As new keyPair as a p12 file – for example: you_system.p12



DO NOT SAVE THE CHANGES TO THE ORIGINAL CERTIFICATE!!!

