Client Certificate Guide

This is a step-by-step introduction in how to create a client-certificate keystore in Java environment. In this document we use KeyStore explorer software that is free and available for download for several operating systems.

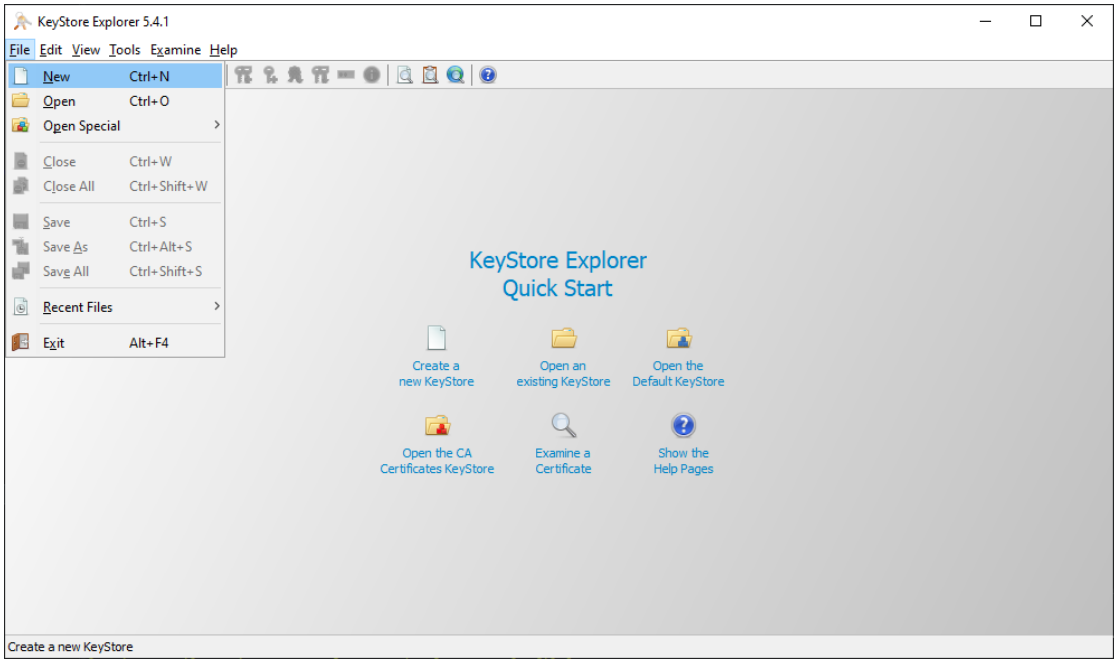
1 Basic Setup

Download and install free KeyStore Explorer software from
https://keystore-explorer.org/

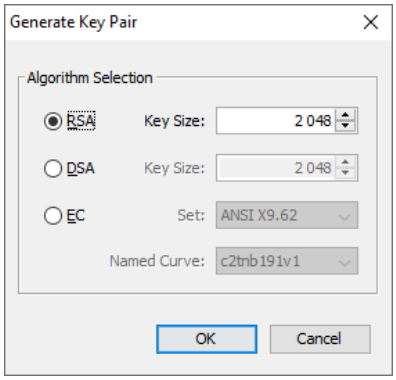
KeyStore Explorer is far more user-friendly that Java's command line Keytool.

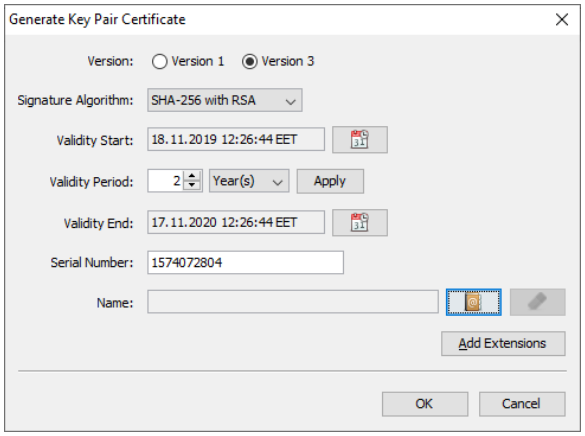
2 Generating Private Key and Keystore

Open KeyStore Explorer and select "Create a new KeyStore" (or File->New).
New KeyStore Type should be **JKS**.



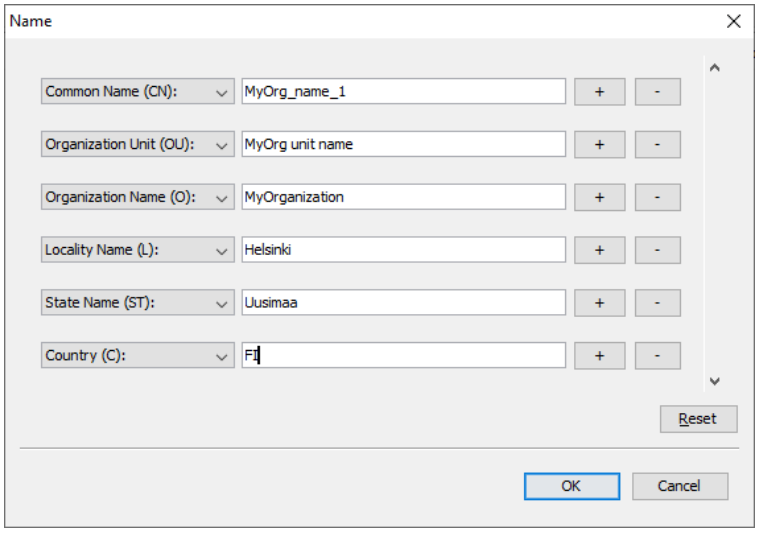
Generate a new key pair. This selection is available if you right-click the window or from the Tools menu (in version 5.4). Use the default values (Algorithm: RSA, Key Size: 2048).





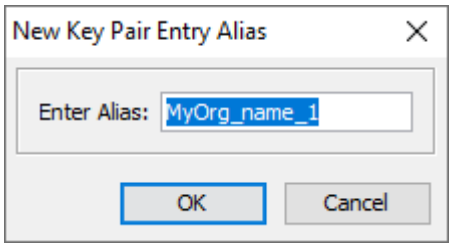
Select the following values from the next dialog:

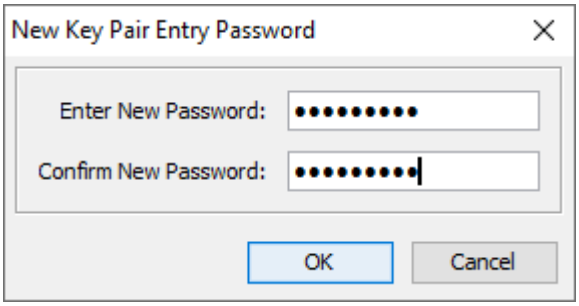
- Version: Version 3
- Signature Algorithm: SHA-256 with RSA
- Validity Period: 2
- Click the button next to Name to open another dialog.



Fill in the details. Common Name (CN) should be distinguishable among all other certificates (in Finland). Use only ASCII characters in all fields.

Click OK, then OK again.
KeyStore Explorer suggests an alias for the key pair, leave it unmodified.

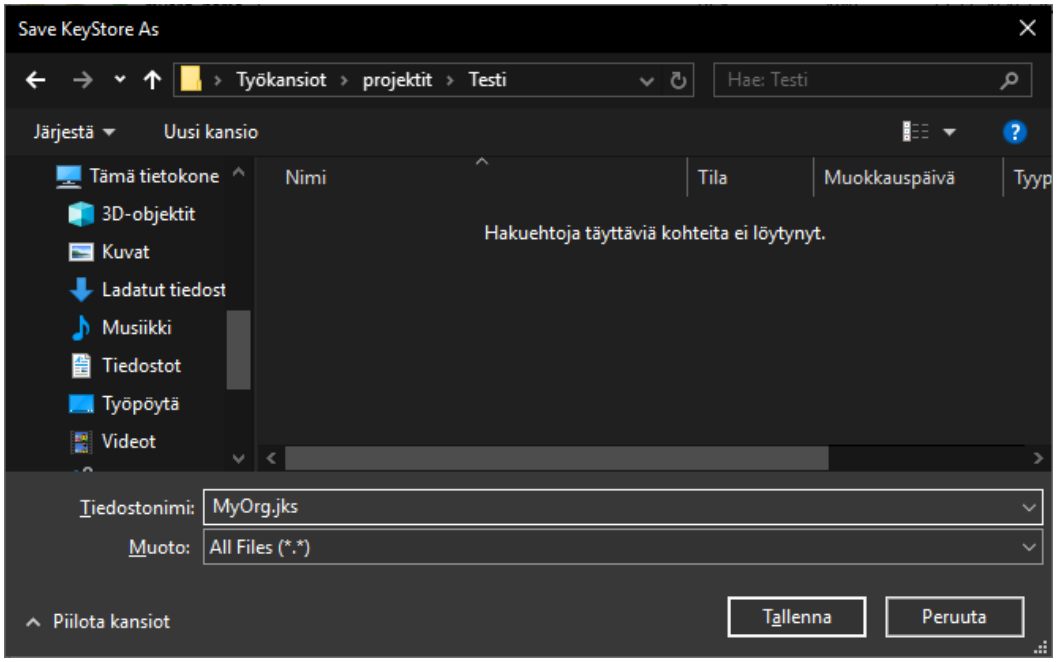




Enter password for private key and store it in a safe place! You will need this password later and if you lose it, your private key is unusable. This password protects your private key and you must not give it or send it to any outside partner in any case.

Save your Keystore using File->Save. You'll be asked for password for keystore file itself. This password should be the same as your key pair's password from last step. It can also be different, but to make sure that your Java implementation is able to use keystore file and key pair properly, use same password. Store password in safe place!

Enter a name for your keystore and use file extension .jks

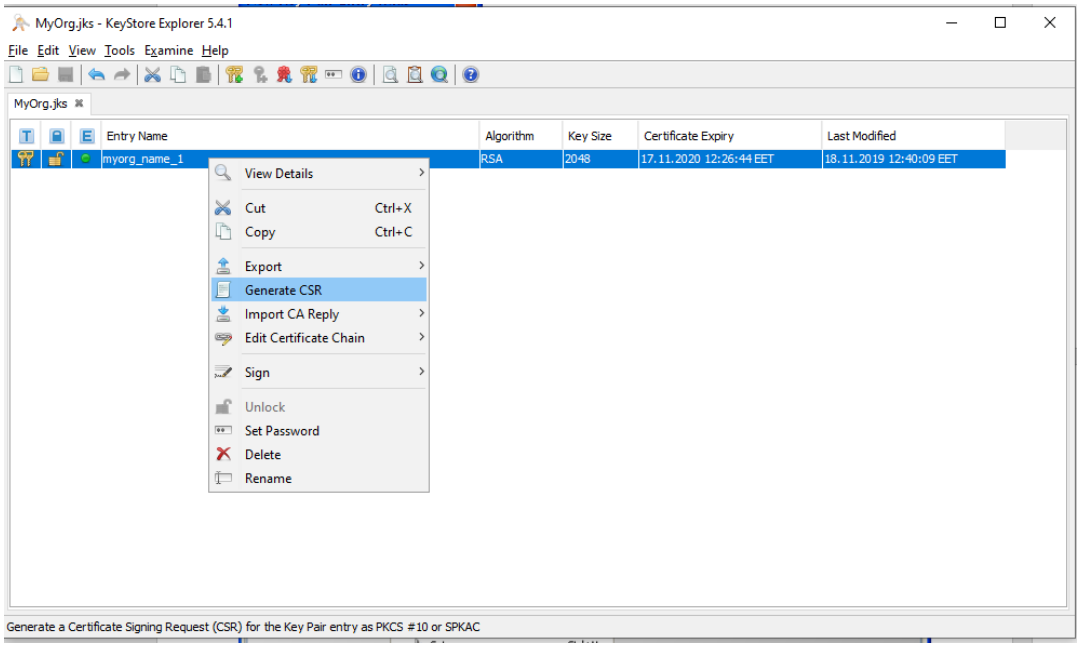


Now you have a Java Keystore containing a private key. Next we need to acquire a signed certificate.

3 Certificate Signing Request

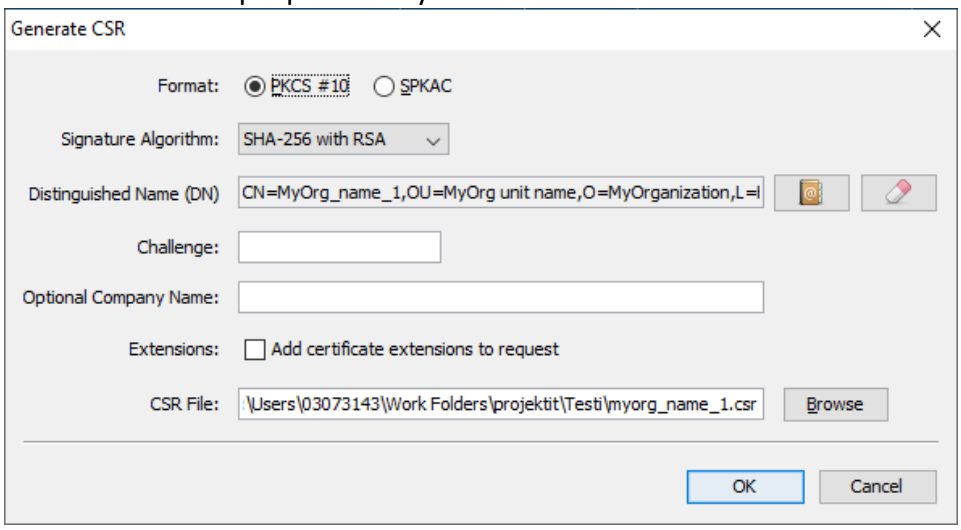
Next thing we need is a signed client certificate. We start by creating a certificate request using your private key. This will be then signed by the certificate authority.

Right-click your private key and select -Generate CSR' from the context menu.



Use the following values:

- PKSC #10
- Signature Algorithm: SHA-256 with RSA
- Challenge: empty
- CSR File: name ending in _request followed by a number if you're creating multiple requests from multiple private keys. File extension .csr

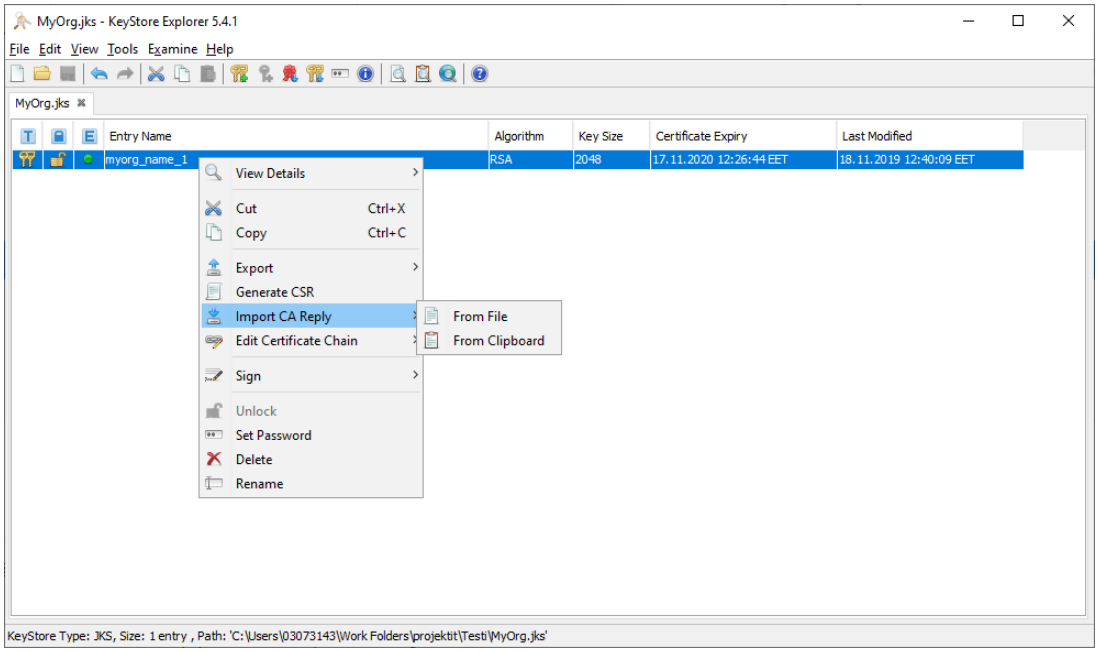


Now you have created the certificate signing request using your private key. Send the file (myorg_name_1_request.csr) to the designated contact person along with user rights application. **Never send your keystore file or any password to anyone!**

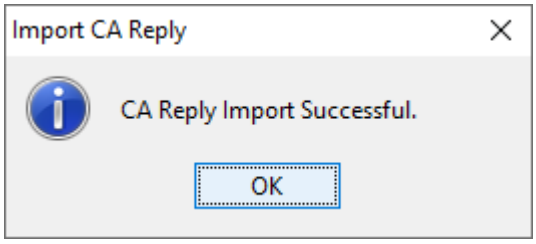
4 Combining Signed Certificate with Private Key

After receiving the signed certificate from the certificate authority you must combine it with your private key. The certificate may have one of several file extensions, for example: .cer, .p7r, .pem or .der. The Finnish Food Authority supplies a .cer file along with two CA certificates.

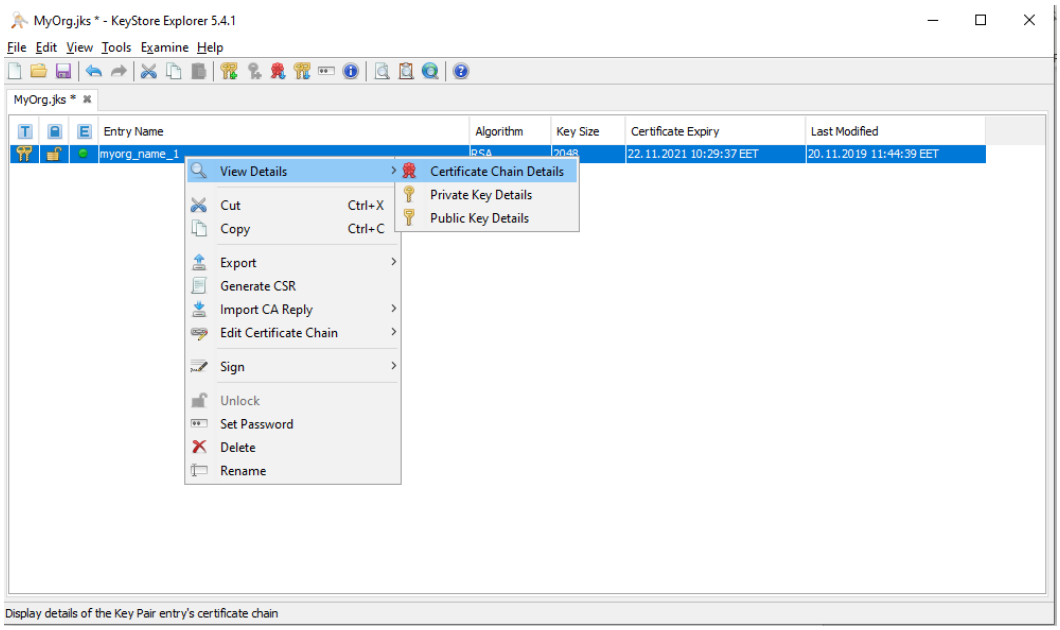
Open the Keystore, right-click the private key and select 'Import CA Reply' from the context menu.



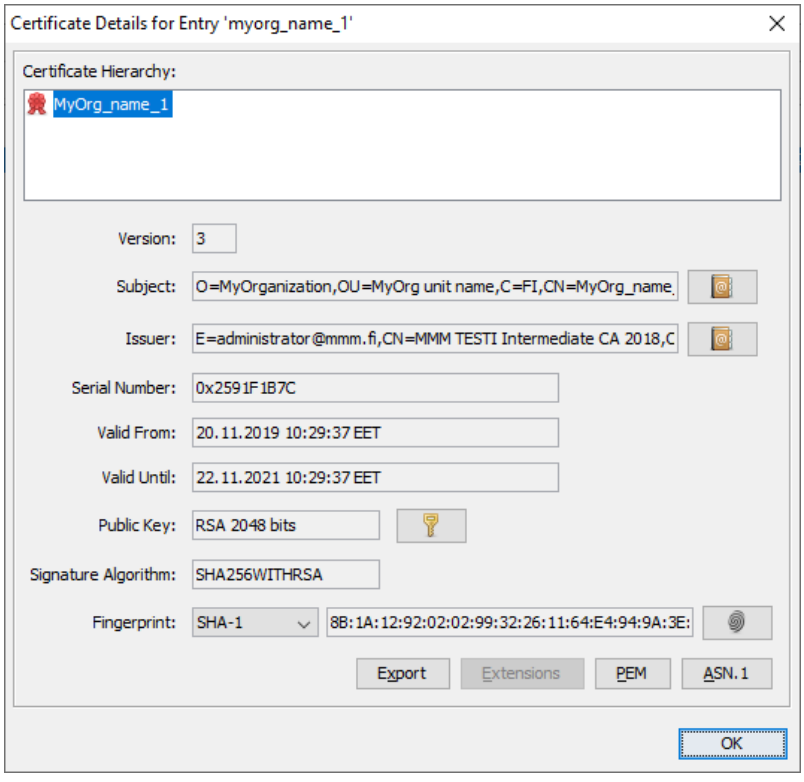
Select the signed certificate (myorg_name_1_request.cer) and click ok.
KeyStore Explorer will confirm that the import was successful. This does not indicate that the certificate chain is in order and it should be checked.



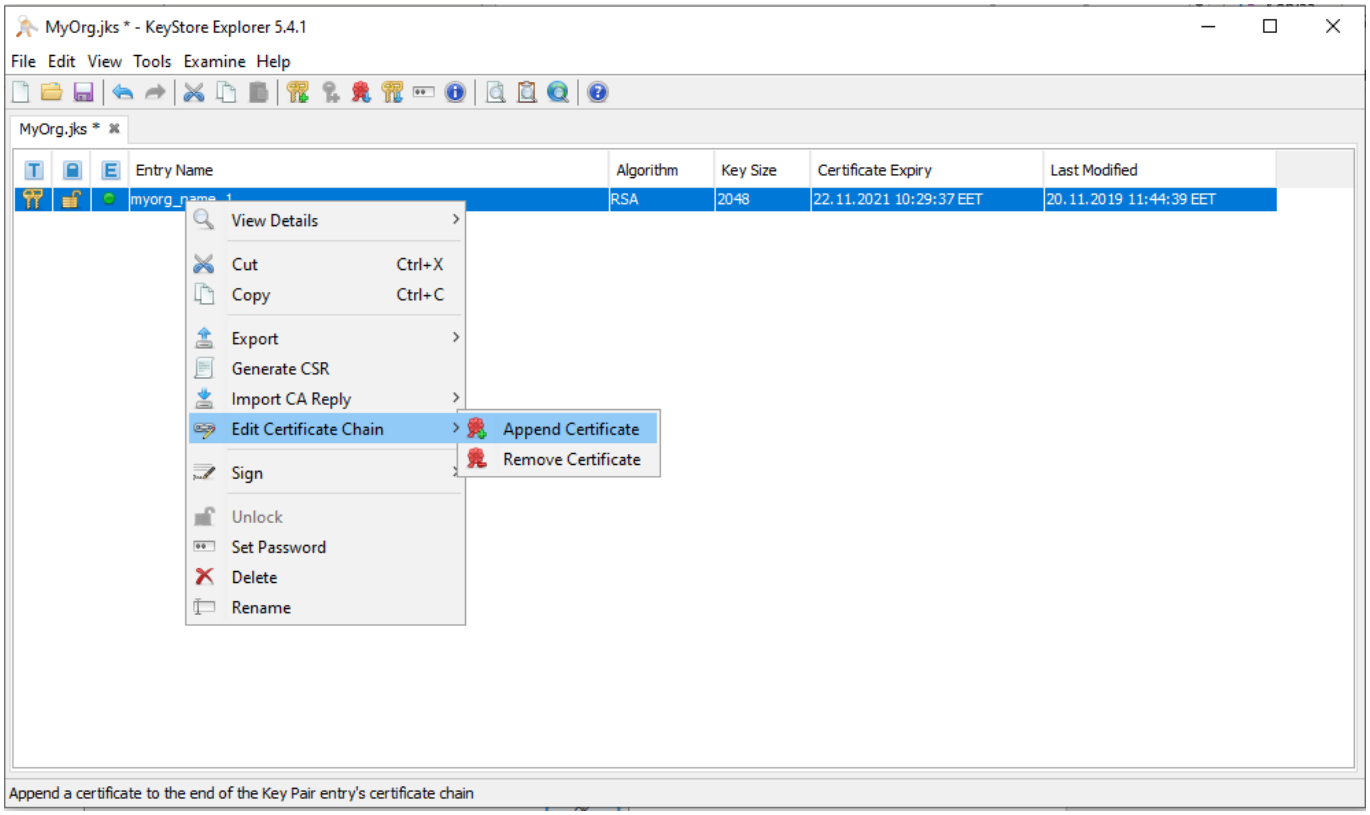
Open the context menu once again by right-clicking the key. Select View Details -> Certificate Chain Details.



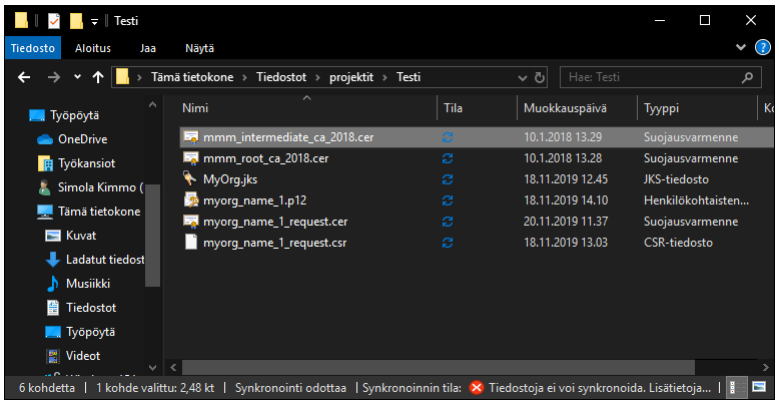
If the Certificate Hierarchy tree contains only the newly acquired certificate, you need to construct the certificate chain by hand.

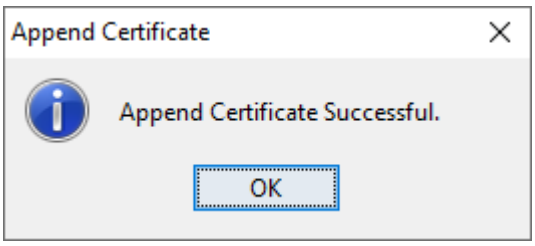


From the context menu, select Edit Certificate Chain -> Append Certificate.

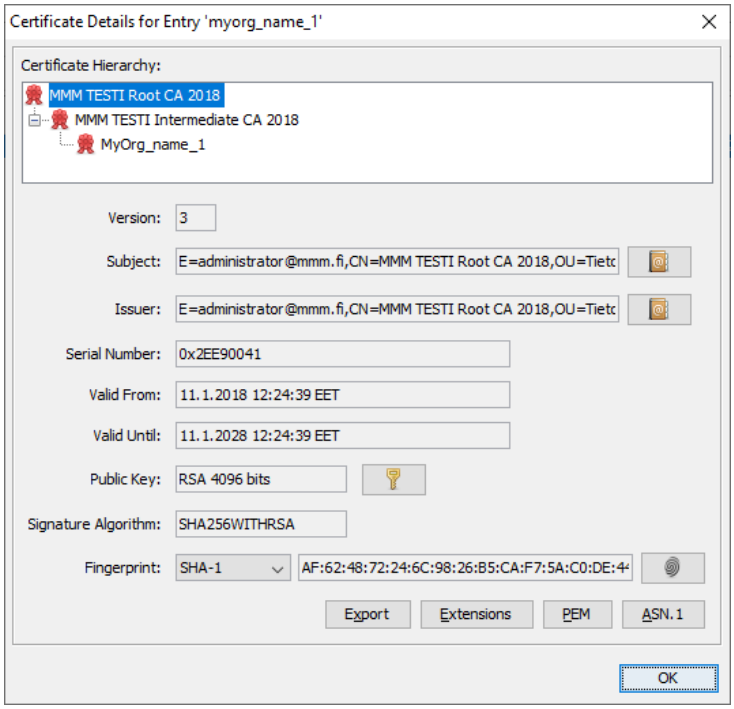


Choose the intermediate certificate (mmm_intermediate_ca_2018.cer) first. Confirmation will be displayed. Then repeat the procedure for the root certificate (mmm_root_ca_2018.cer).





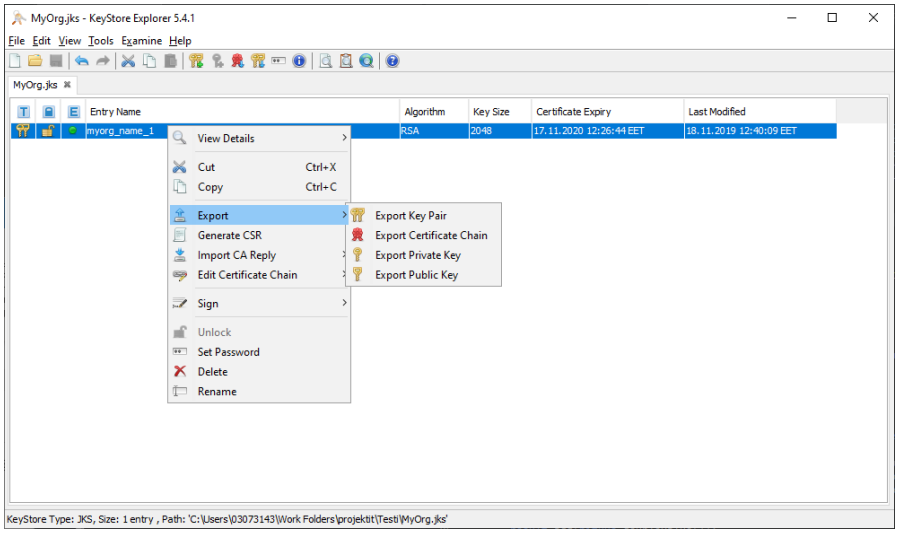
Now the Certificate Hierarchy should display two parent certificates (test certificates shown). This does not guarantee that any software using the keystore trusts the issuer certificates. You may need to add these certificates to a separate trust store. In any case our keystore now contains information about the certificate's issuers.



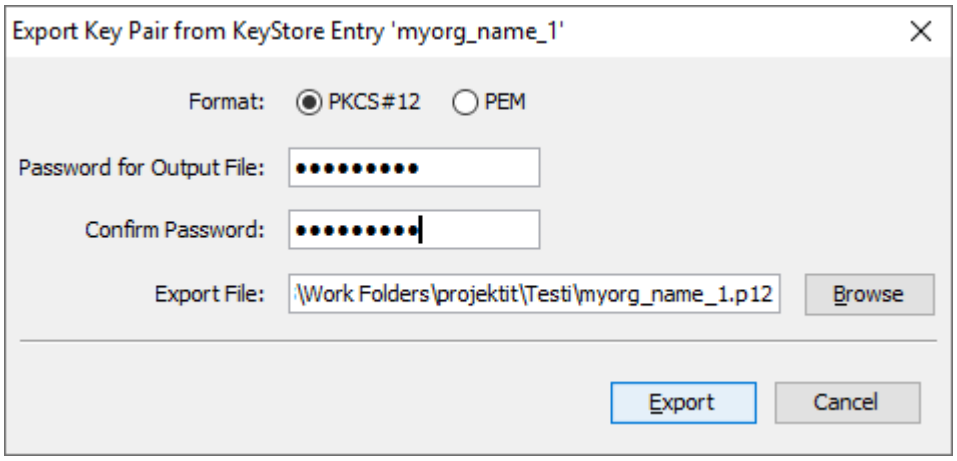
5 Exporting key pair to PKCS12 (.p12) format

If you need to have the key pair (private key and signed certificate) as Windows friendly pkcs12-format, it can be done with Keystore Explorer by following steps

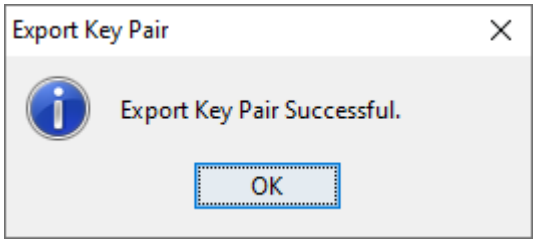
Right click key entry in Keystore Explorer. Choose Export -> Export Key pair. Enter password for private key from earlier.



Enter new passwords for pkcs12 file. Filename extension is p12.



You'll be notified if exporting was successful.



Now you have a file named myorg_name_1.p12. It contains key pair in pkcs12-format. It can be installed to Windows' certificate management by opening the file and following the instructions.