Contents

[Siebel certificates 2](#_Toc133495050)

[1. Create keystore 2](#_Toc133495051)

[NOTE 2](#_Toc133495052)

[example 2](#_Toc133495053)

[2. Generate CSR 2](#_Toc133495054)

[example 2](#_Toc133495055)

[3. Forward CSR to digicert 2](#_Toc133495056)

[4. Get certificate in return 3](#_Toc133495057)

[5. Get keytool-explorer 4](#_Toc133495058)

[6. Download the keystore from server if generated in server 7](#_Toc133495059)

[7. Inspect the certificate received from digicert 8](#_Toc133495060)

[8. Extract root certificate from CA cert chain 9](#_Toc133495061)

[9. Verify the extracted certificate 12](#_Toc133495062)

[10. Import server certificate 13](#_Toc133495063)

[11. Save the keystore before exiting or uploading to server 16](#_Toc133495064)

[12. Create Truststore and Import trust certificate 16](#_Toc133495065)

[12.1 Import root certificate 17](#_Toc133495066)

[12.2 Import intermediate certificate 19](#_Toc133495067)

[13. Save the keystore 21](#_Toc133495068)

[14. Import server certificate from all other servers to enable communication 22](#_Toc133495069)

[14.1 Do the same for all certificates 25](#_Toc133495070)

[**14.2** **Make sure you save the keystore** 25](#_Toc133495071)

[15. Upload the keystore and truststore 25](#_Toc133495072)

[16. Update server.xml to point to trust store and keystore 26](#_Toc133495073)

[17. Place the truststore in all servers and update server.xml 27](#_Toc133495074)

[18. Restart Siebel services 27](#_Toc133495075)

[19. Test 27](#_Toc133495076)

# Siebel certificates

## Create keystore

keytool -genkey -alias **<ALIAS NAME>** -keyalg RSA -keysize 2048 -keystore <KEYSTORE NAME> -sigalg SHA256withRSA

### NOTE

Make a note of the alias name, the server certificate when received from digicert needs to be imported into this alias

### example

keytool -genkey -alias ty-sebtst7-ma-s\_15-FEB-2023 -keyalg RSA -keysize 2048 -keystore siebelkeystore.jks -sigalg SHA256withRSA

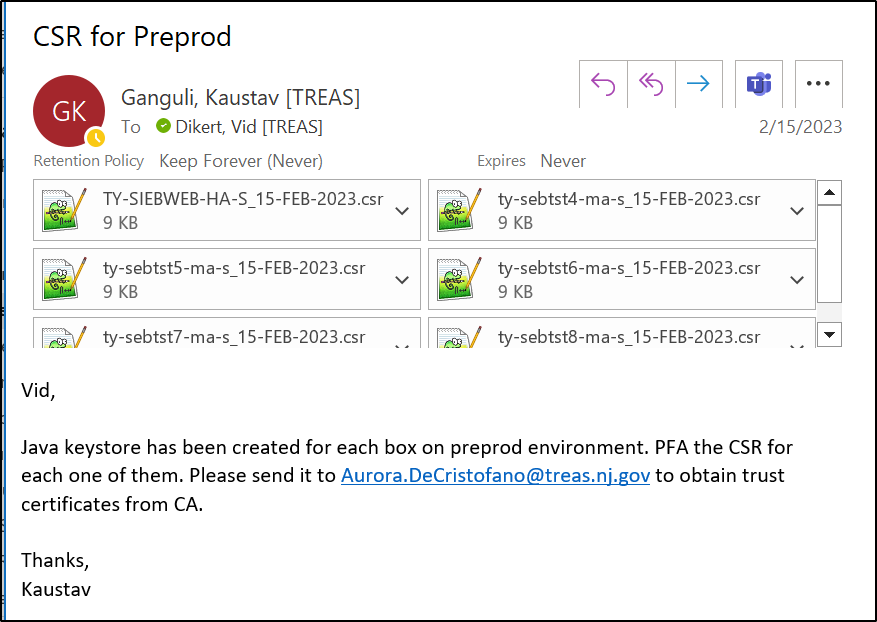
## Generate CSR

keytool -certreq -alias <ALIAS NAME> -keyalg RSA -file <CSR FILENAME> -keystore <KEYSTORE NAME>

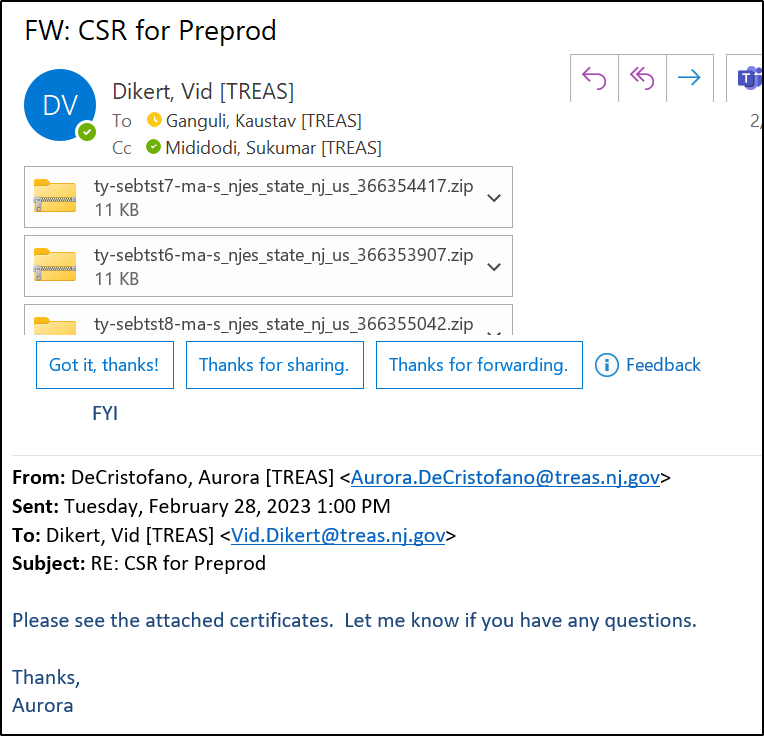
### example

keytool -certreq -alias ty-sebtst7-ma-s\_15-FEB-2023 -keyalg RSA -file ty-sebtst7-ma-s\_15-FEB-2023.csr -keystore siebelkeystore.jks

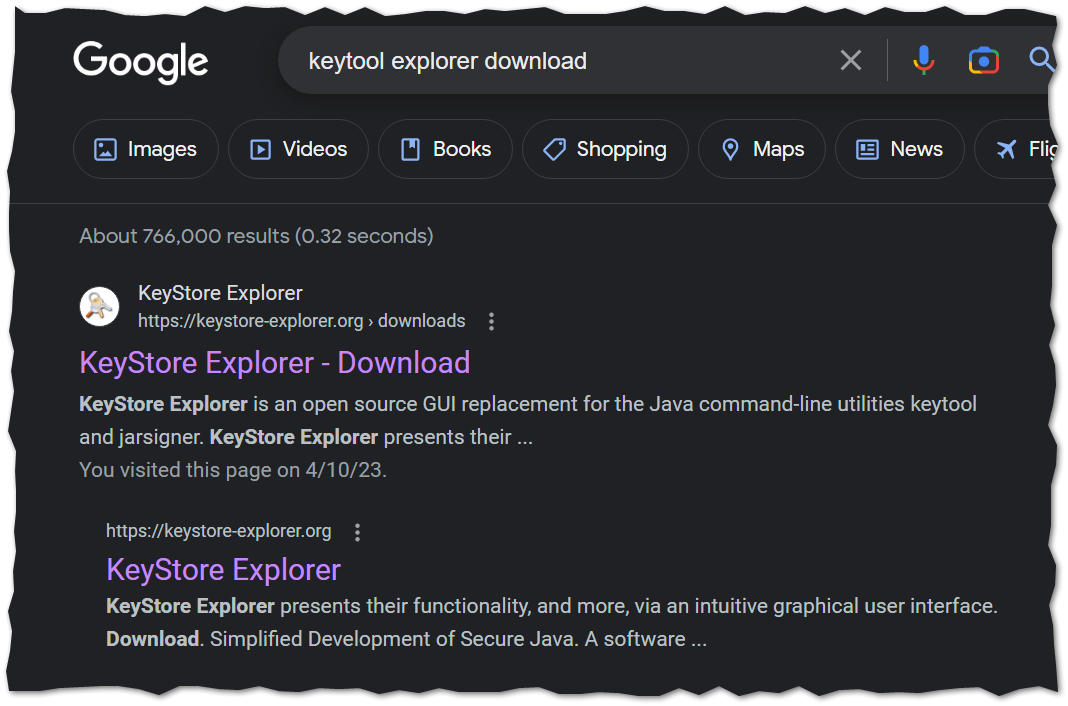
## Forward CSR to digicert

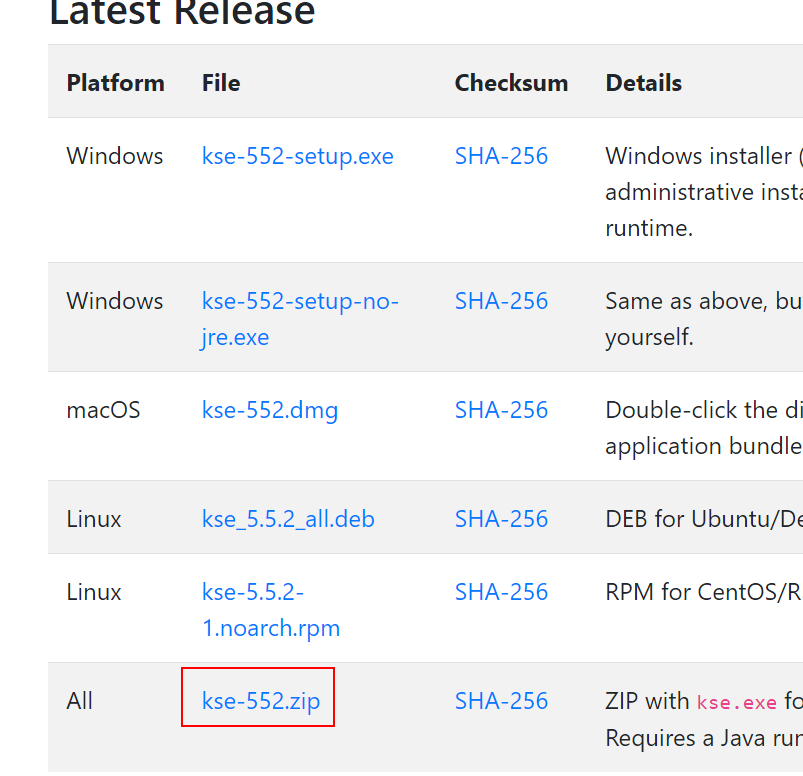


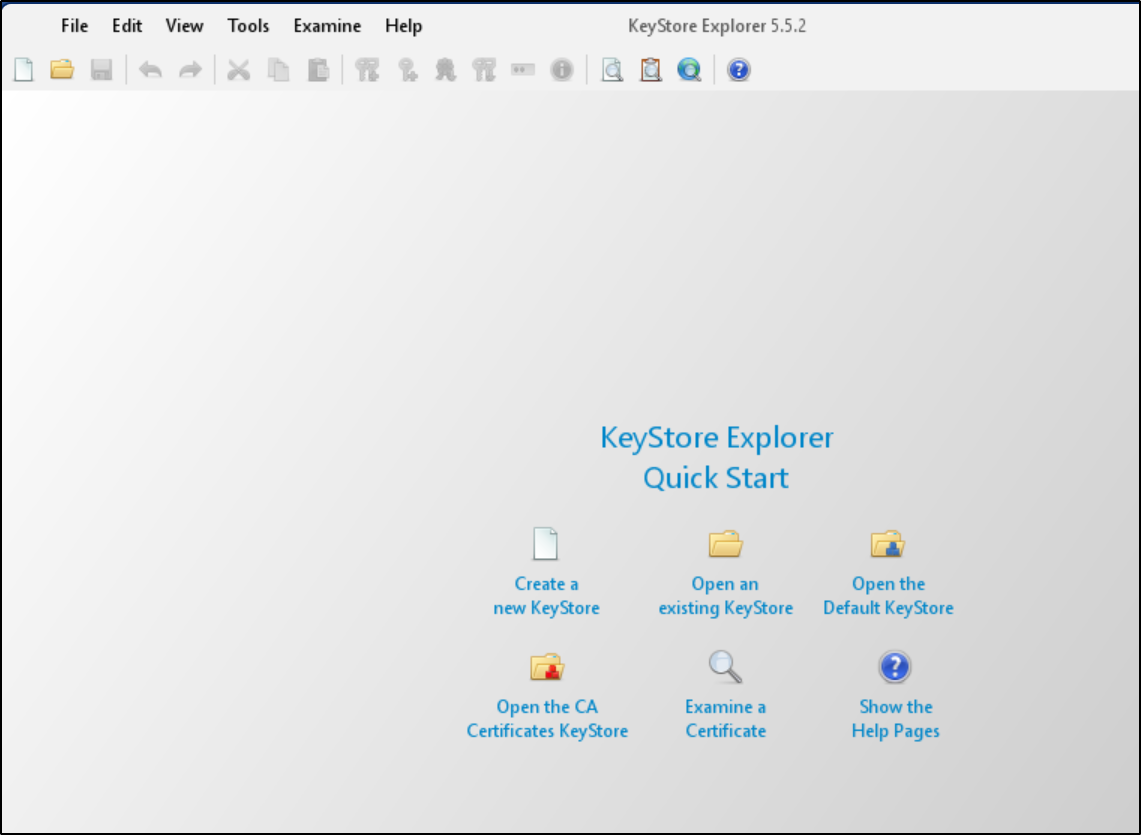
## Get certificate in return



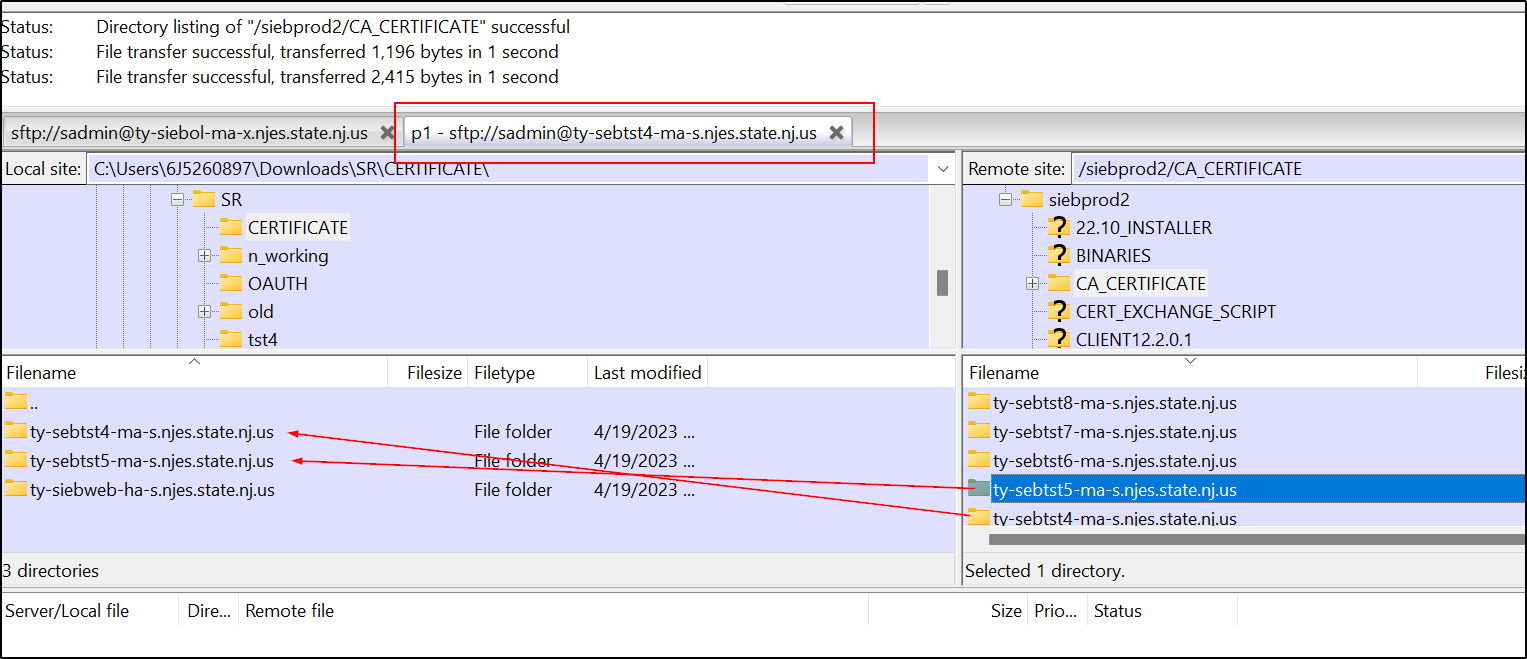
## Get keytool-explorer







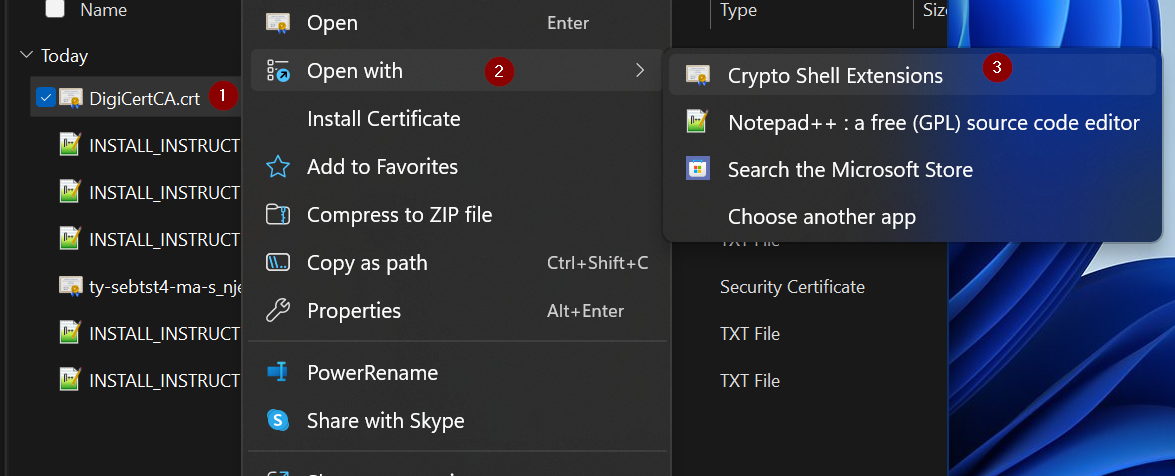
## Download the keystore from server if generated in server

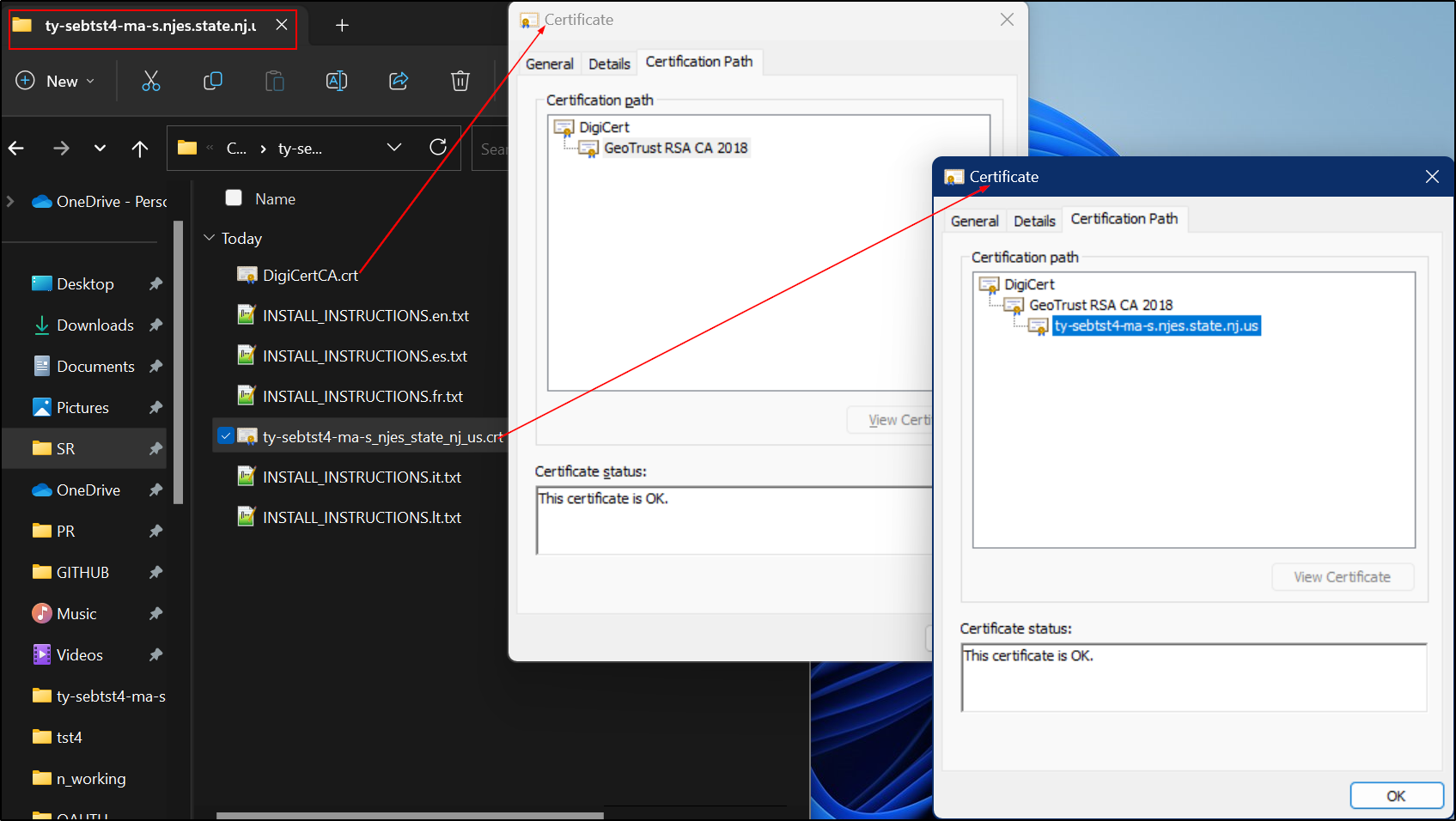


## Inspect the certificate received from digicert

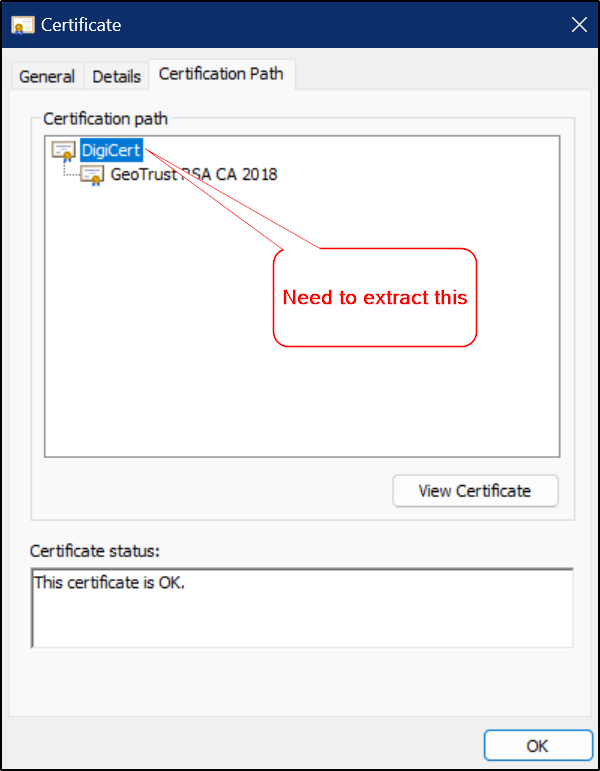
Digicert sends two files. One trust certificate that has root and intermediate certificate chained together, and a server certificate (for which it received the CSR for), that has all three certificates chained together –

Inspect the certificate with windows “Crypto Shell Extension” to see the certificate path –

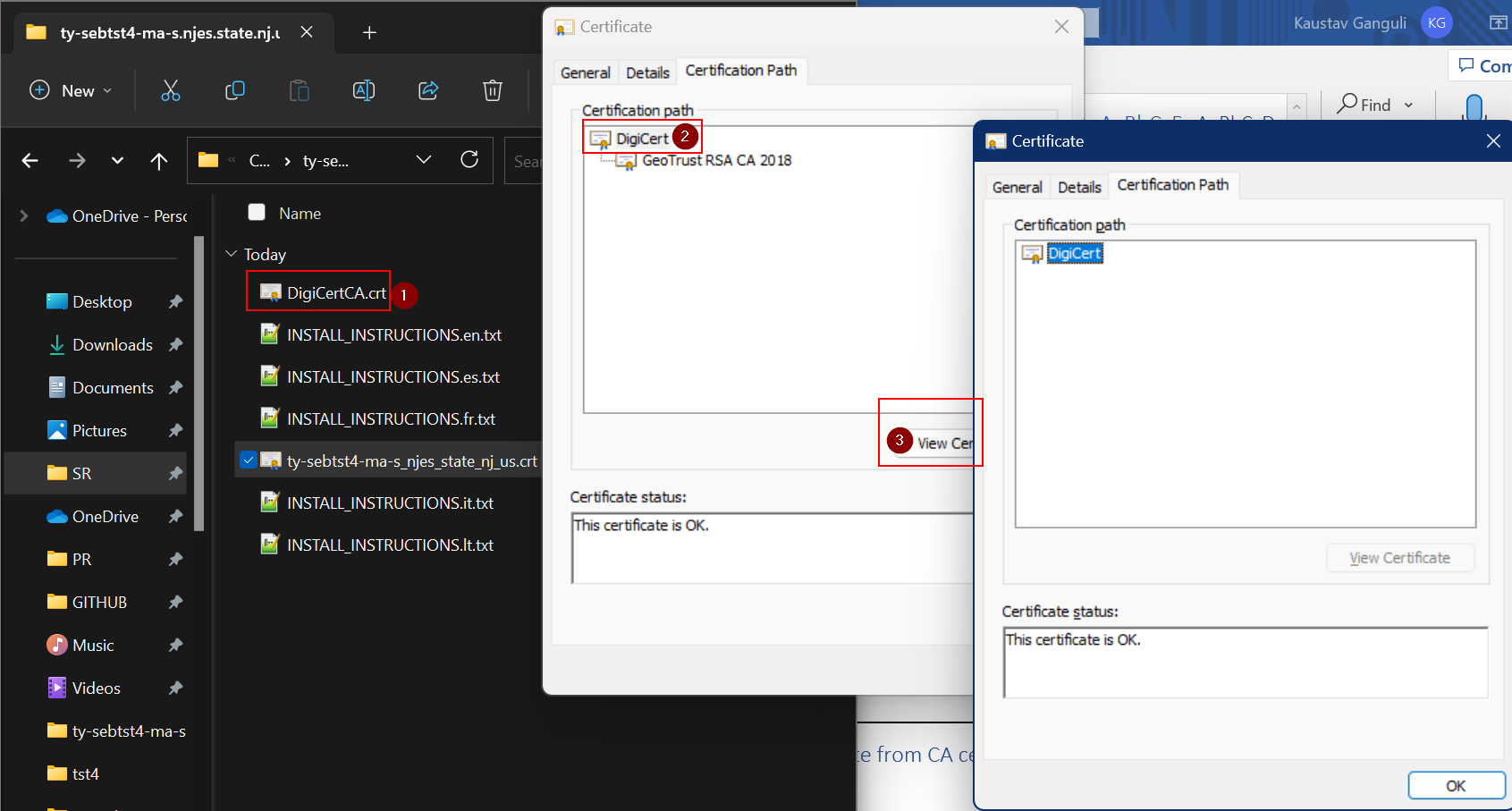


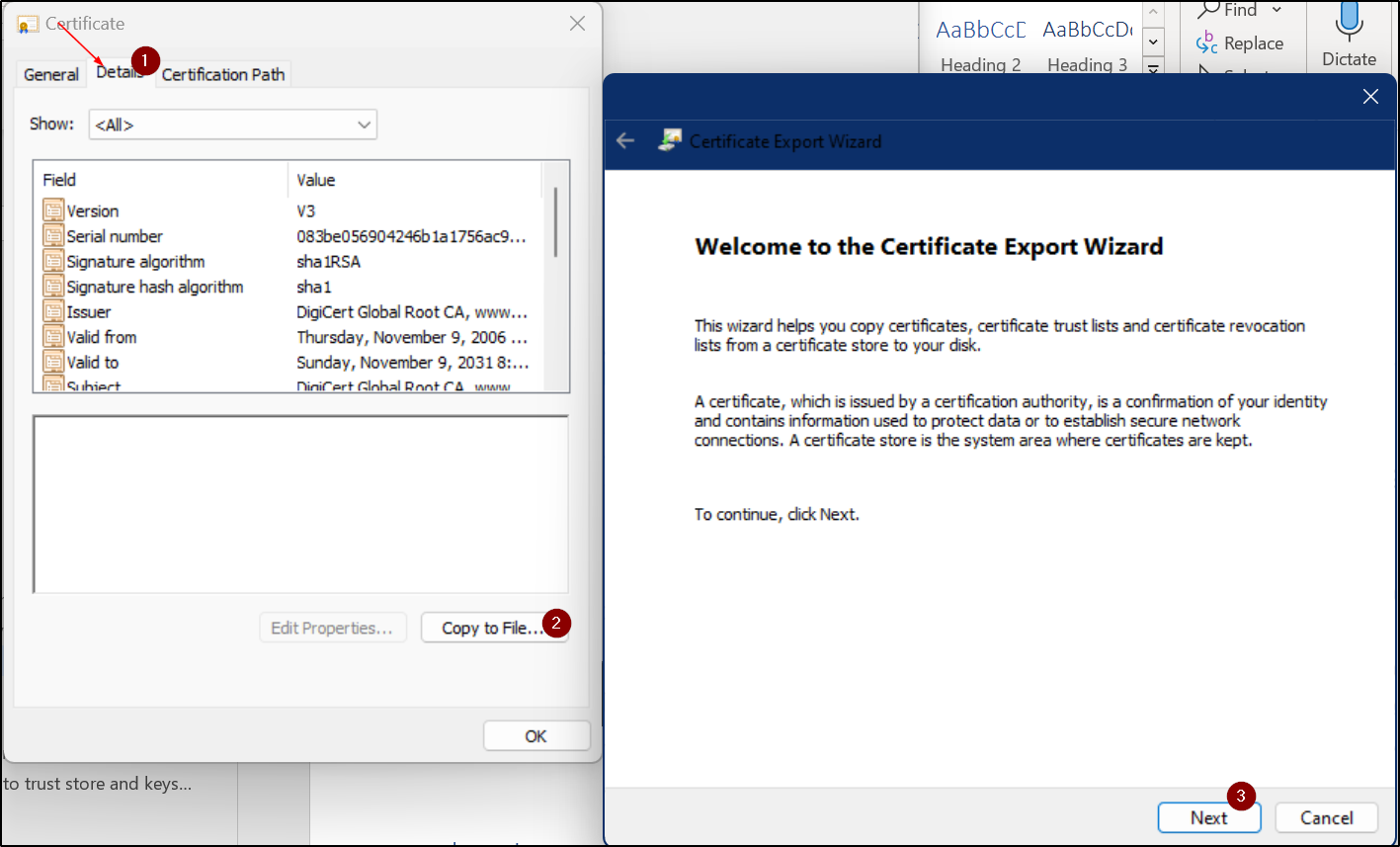


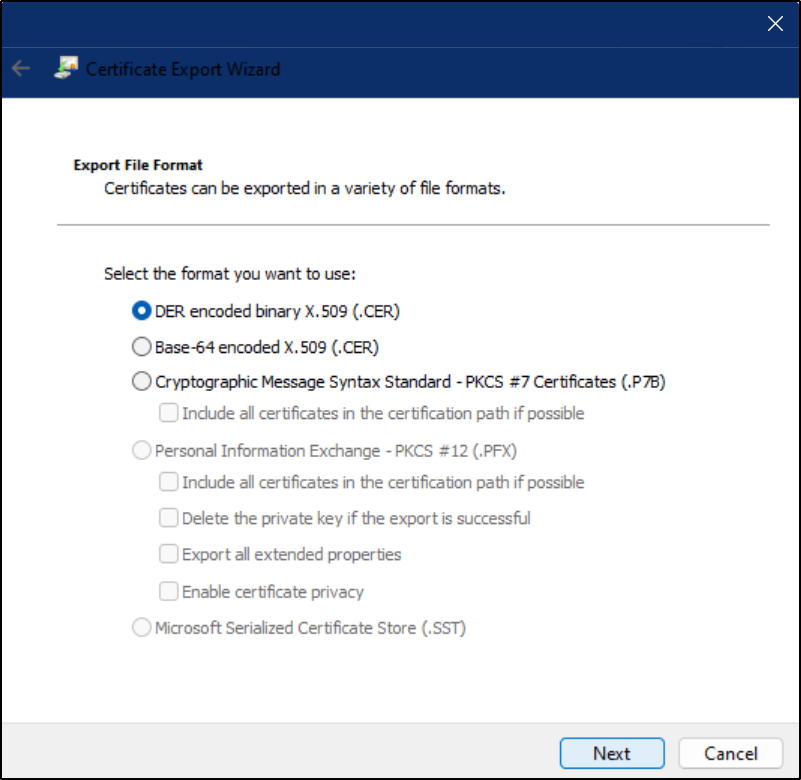
We would need the root certificate extracted in a separate file and then use keytool explorer to import. Without extracting the root certificate, keytool explorer only imports the intermediate certificate from “DigicertCA.crt” file

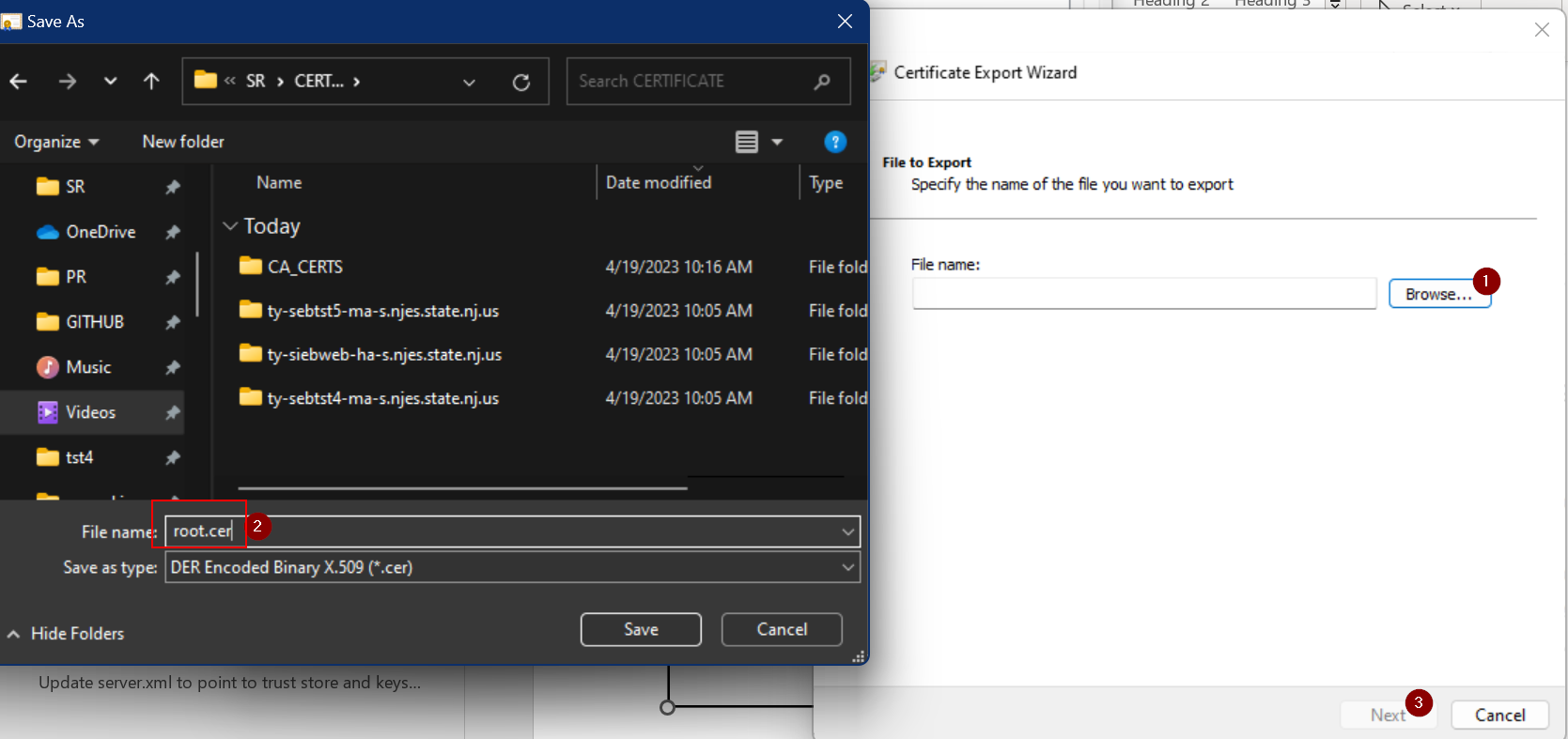


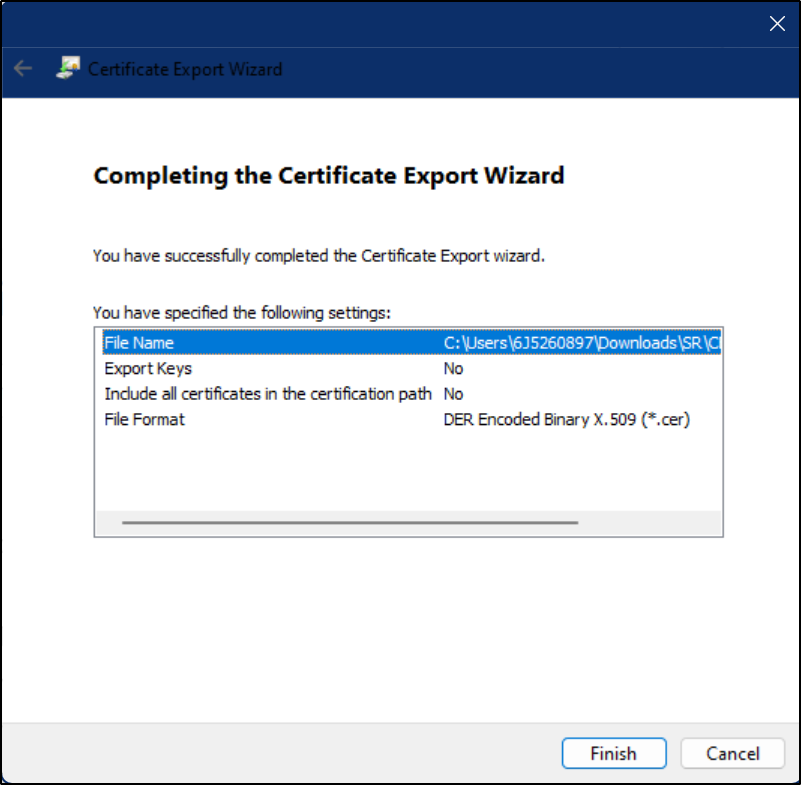
## Extract root certificate from CA cert chain



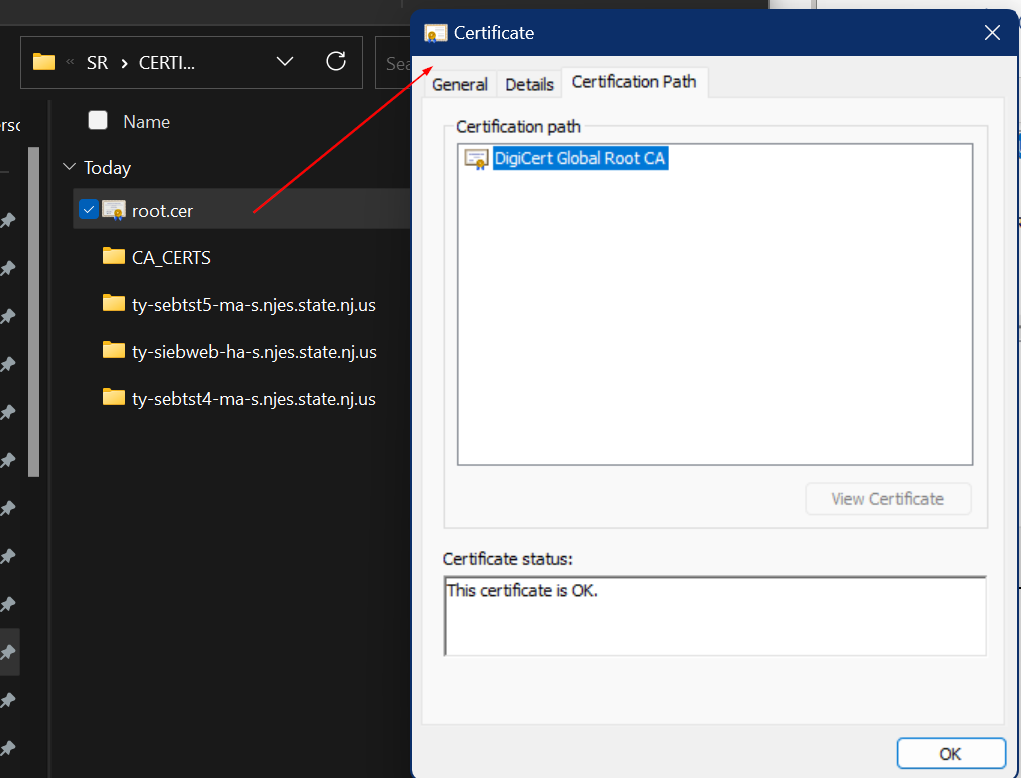






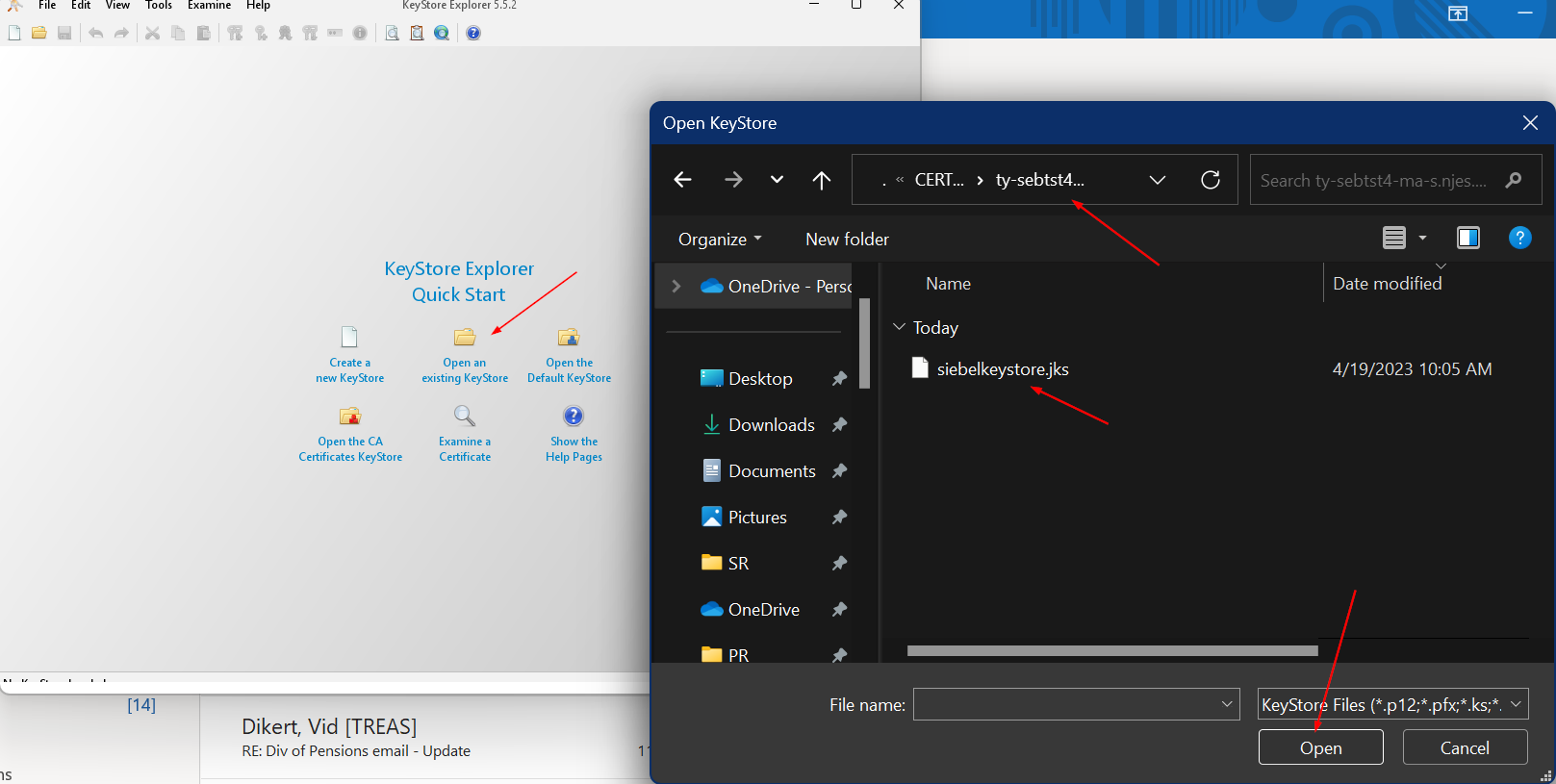


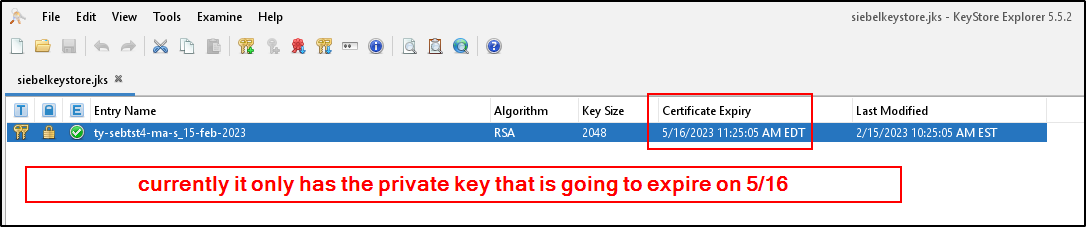
## Verify the extracted certificate

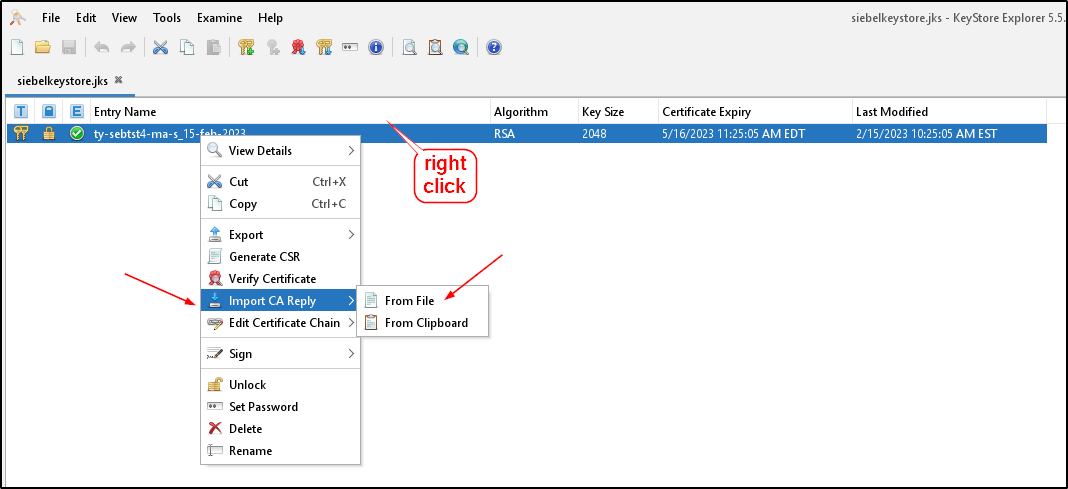


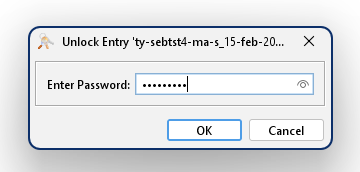
## Import server certificate

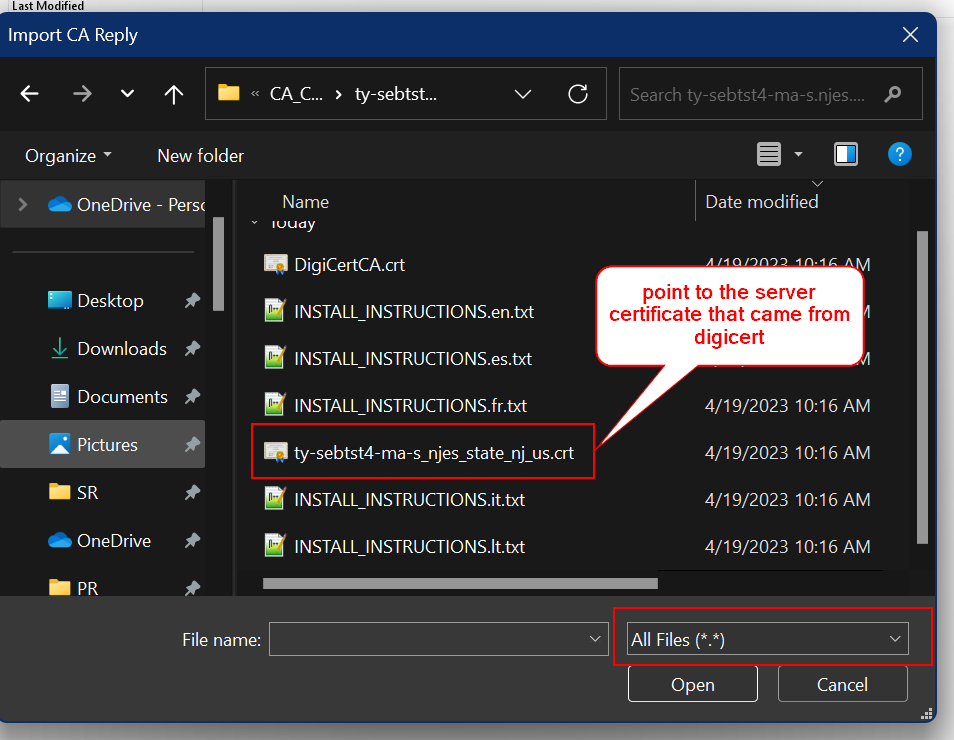
Open the keystore that was generated and downloaded

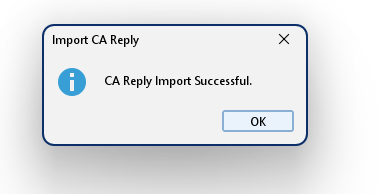


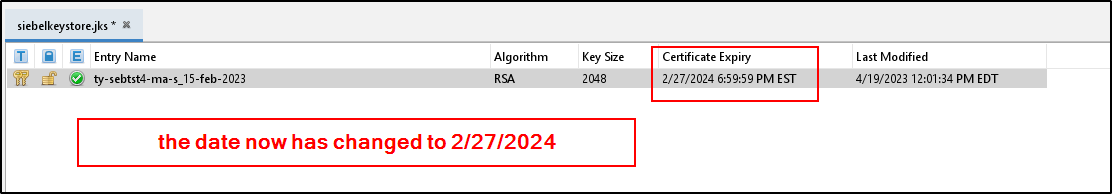


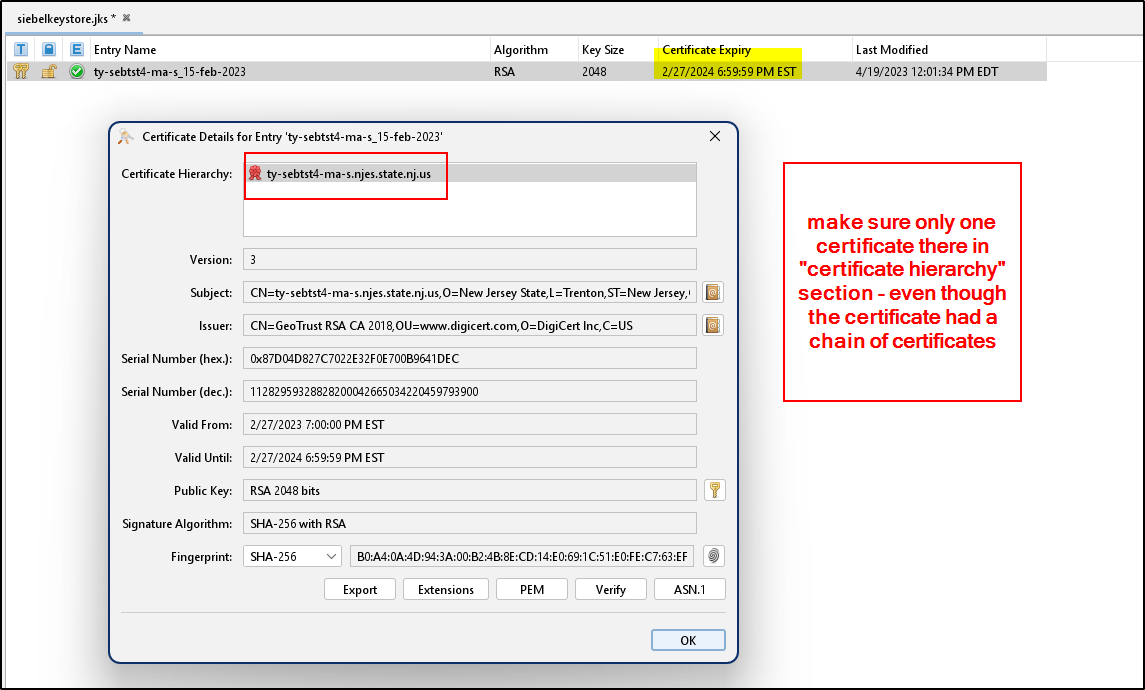




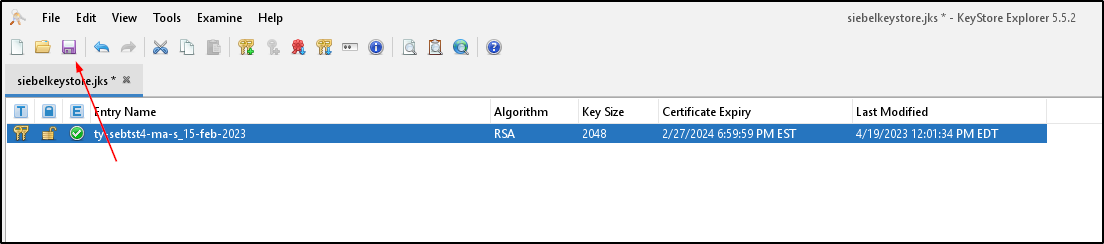




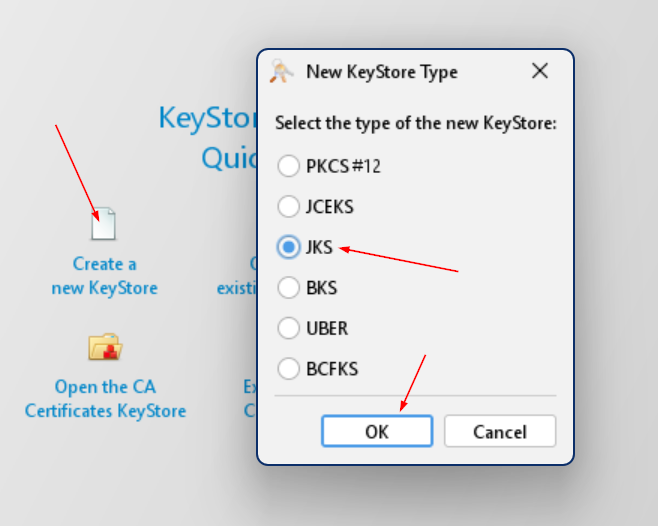


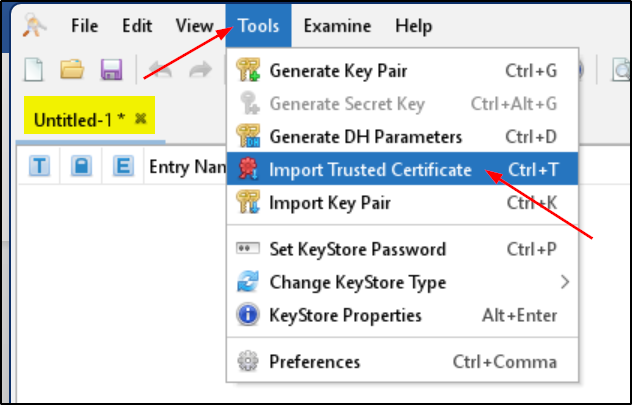


## Save the keystore before exiting or uploading to server

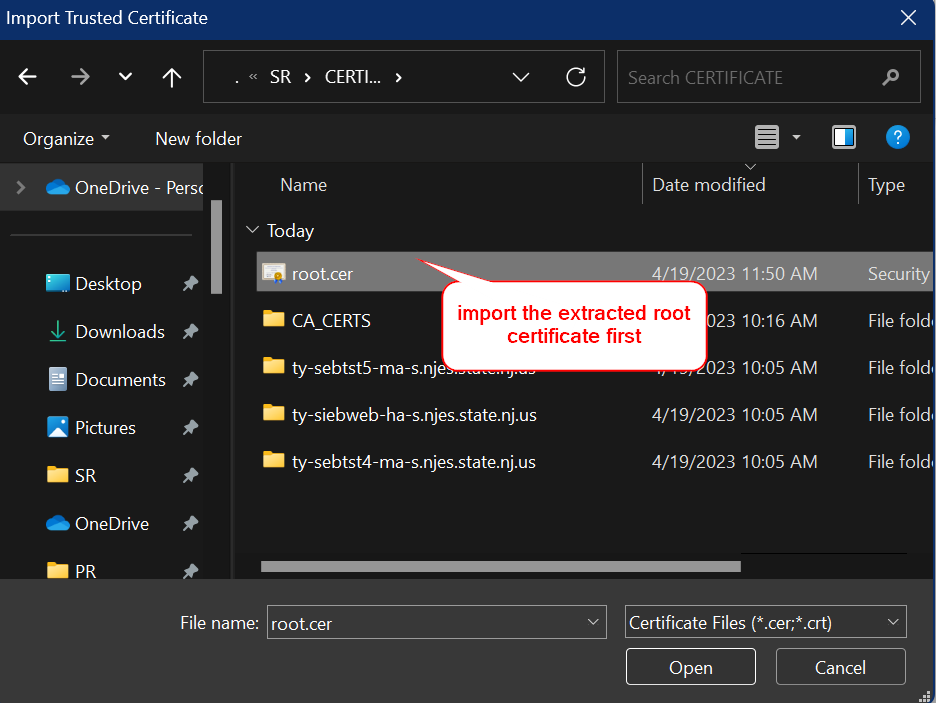


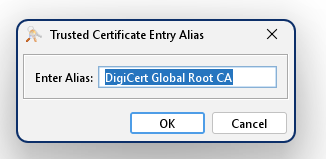
## Create Truststore and Import trust certificate

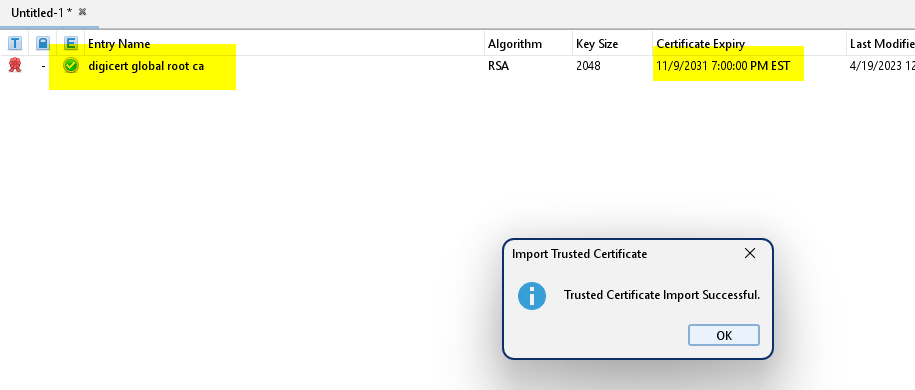




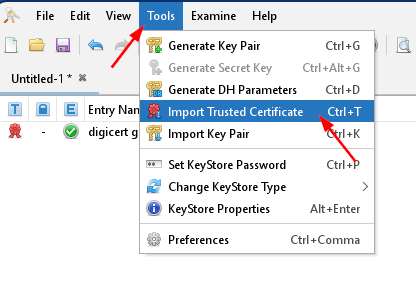
### 12.1 Import root certificate

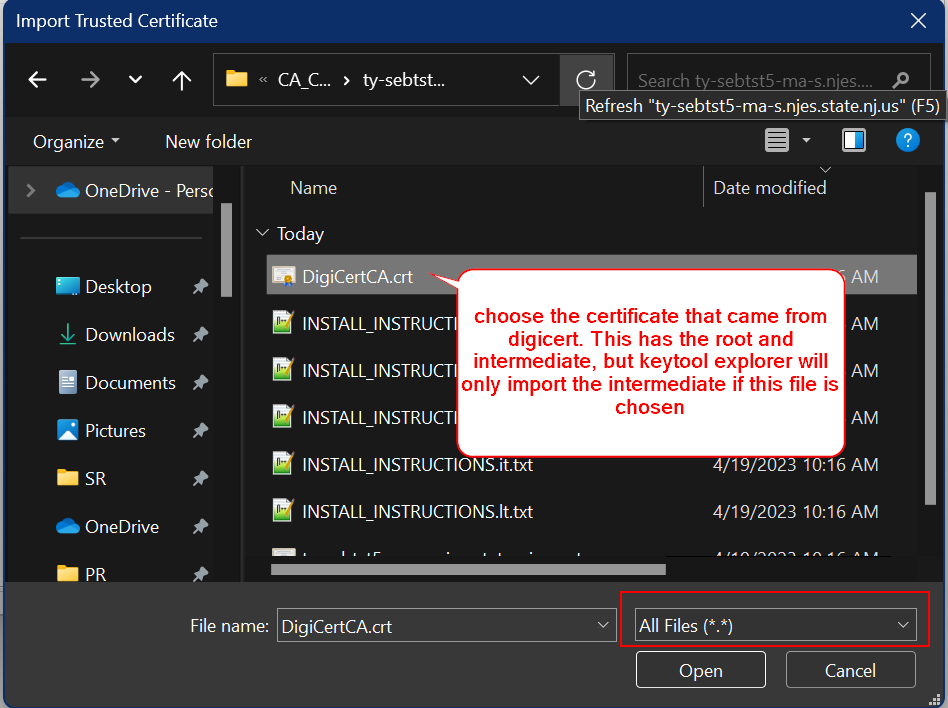


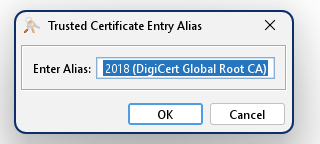


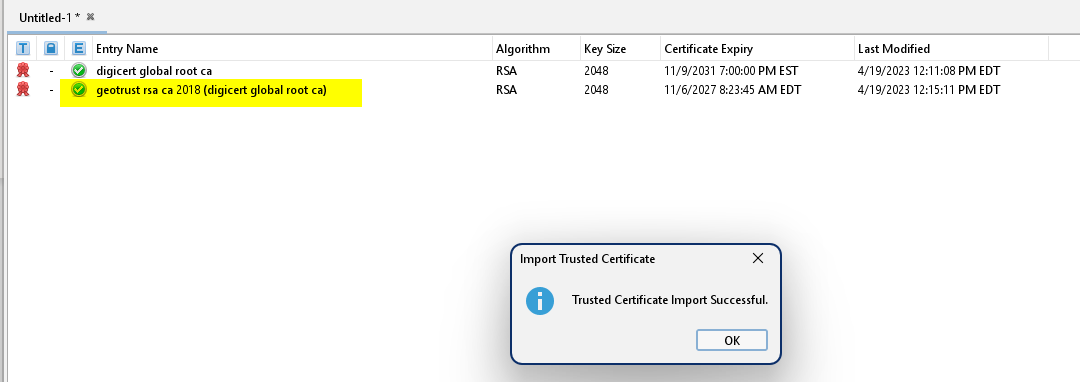


### 12.2 Import intermediate certificate

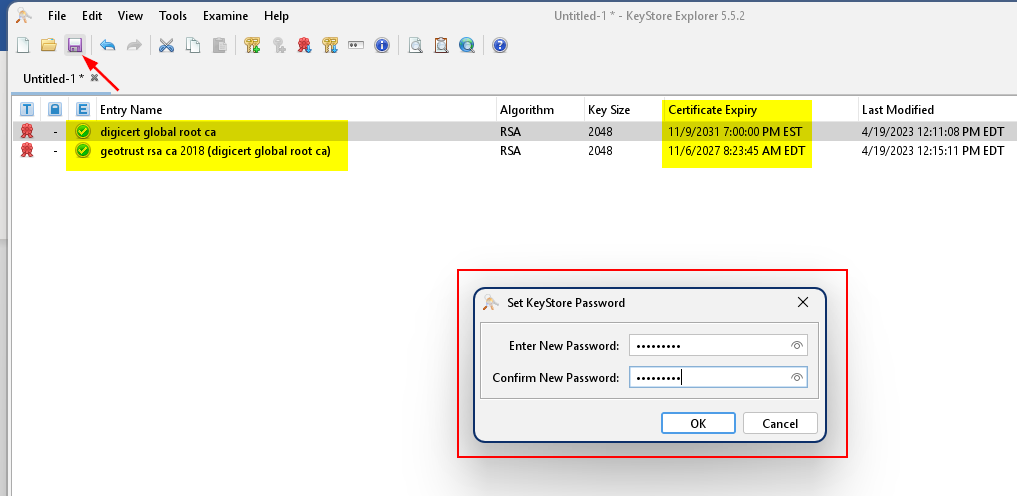


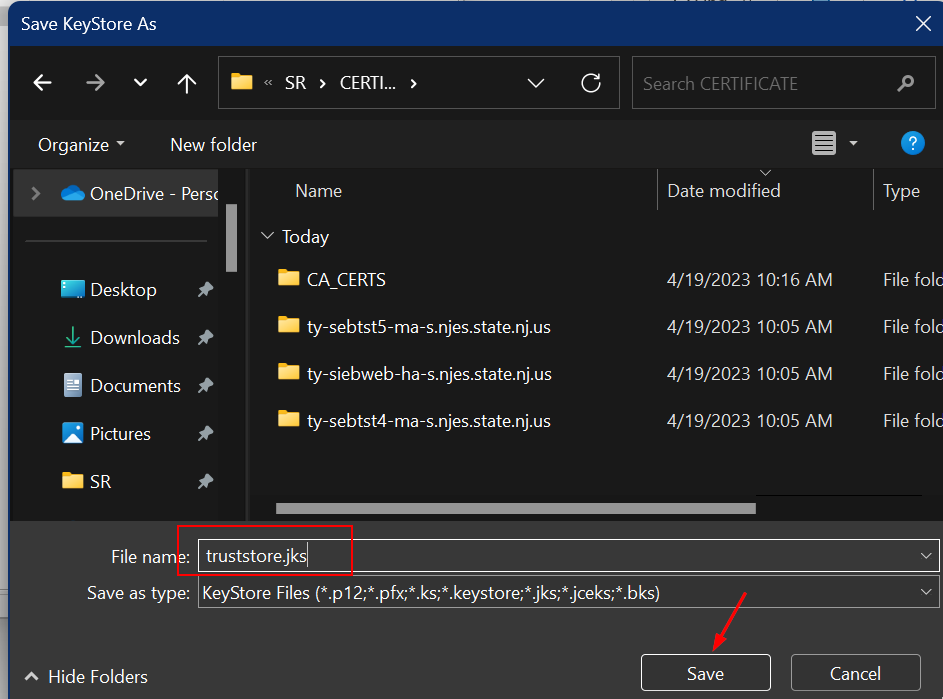


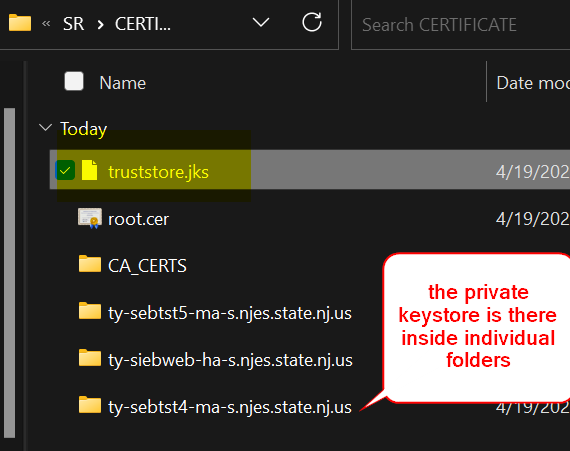




## Save the keystore

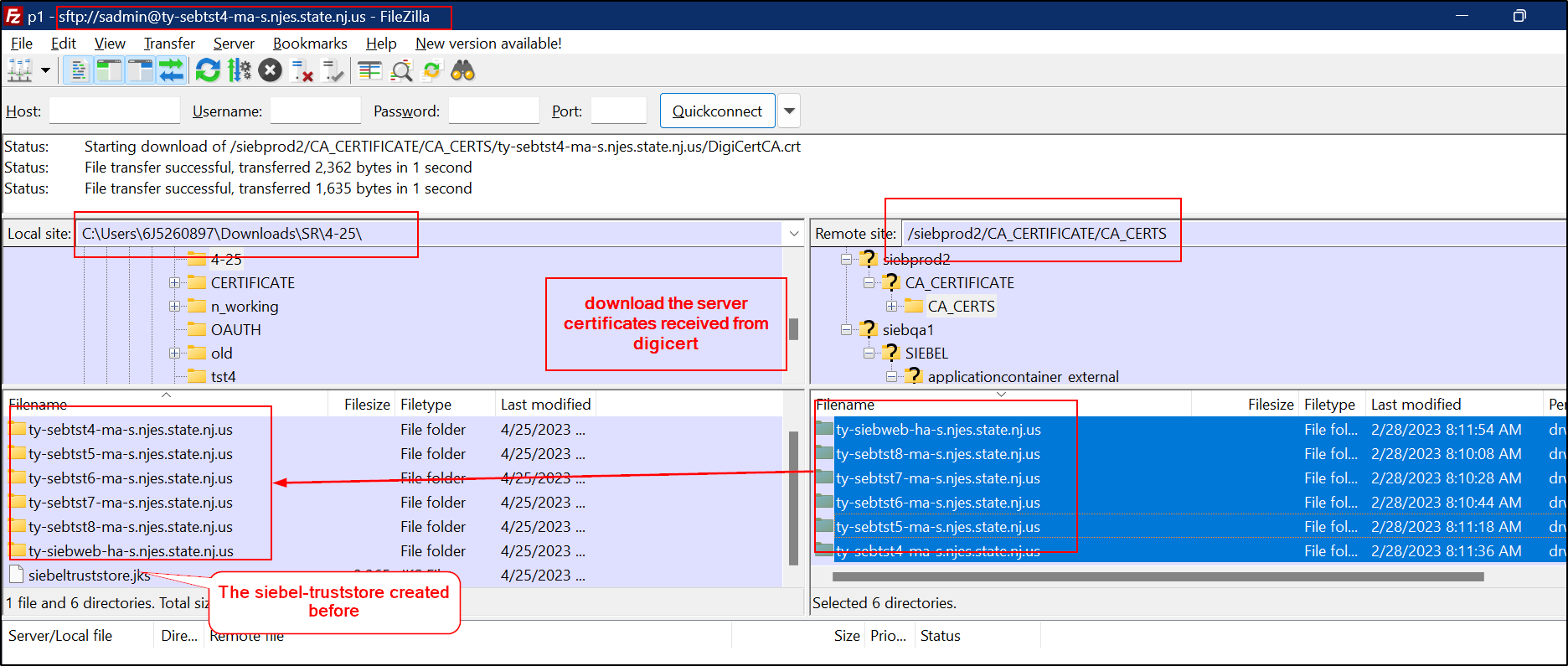


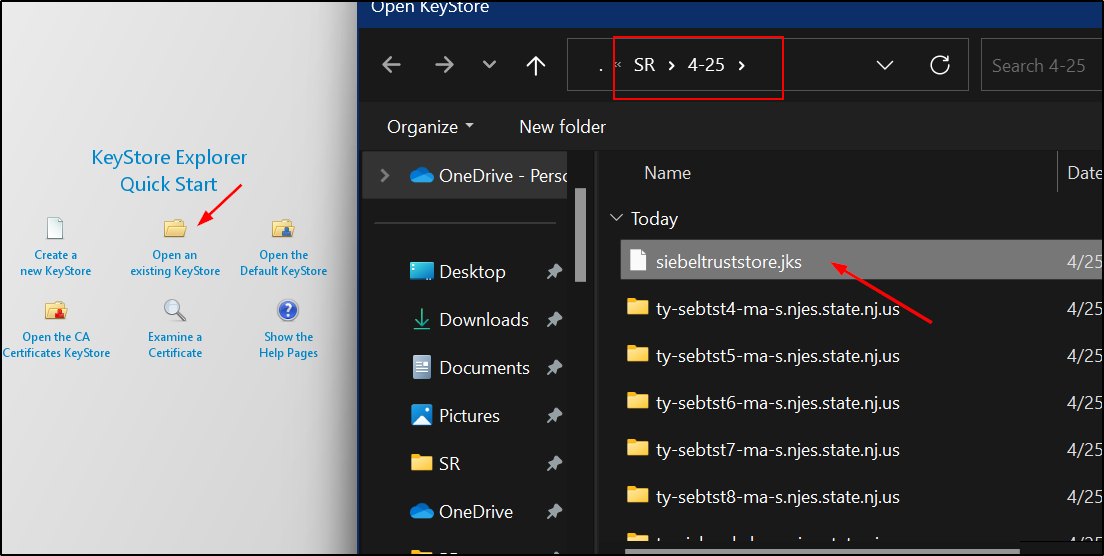


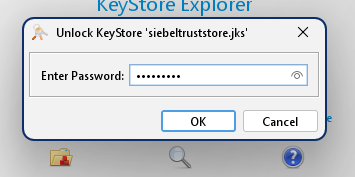


Renamed the “truststore.jks” to “siebeltruststore.jks” to match server configuration

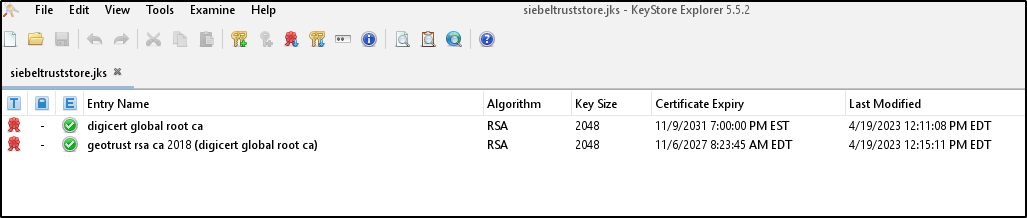
## Import server certificate from all other servers to enable communication



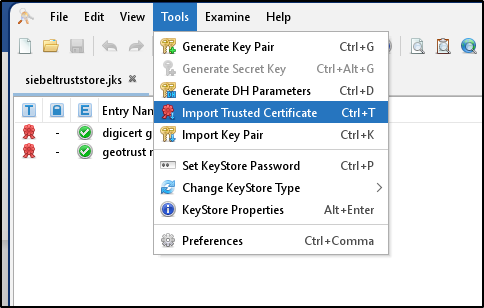


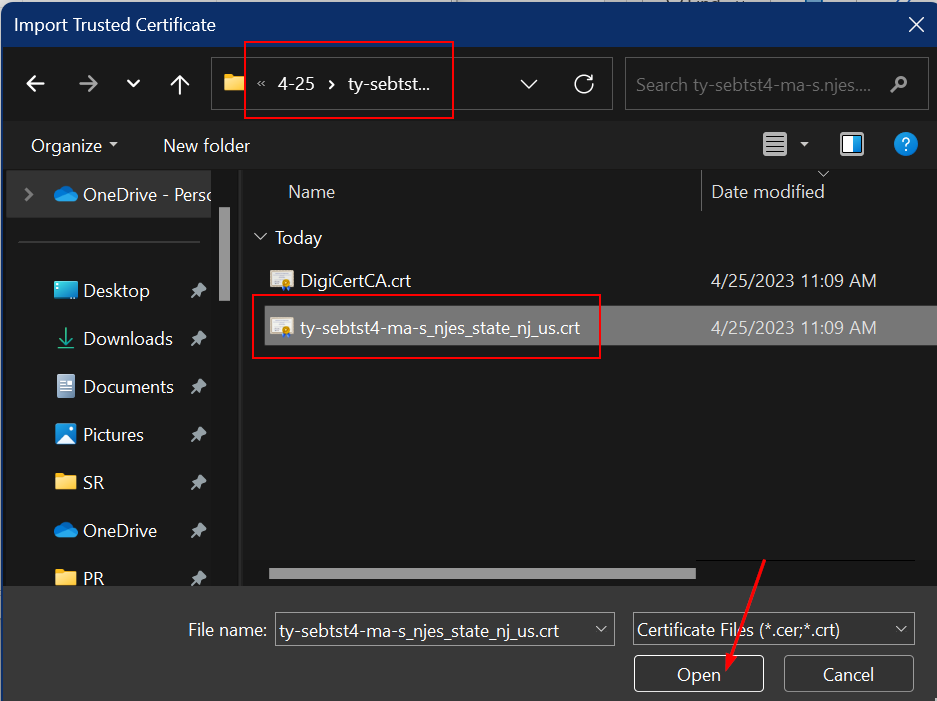


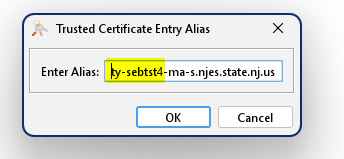
The truststore now has only the certificates imported from [step 12](#_Create_Truststore_and)

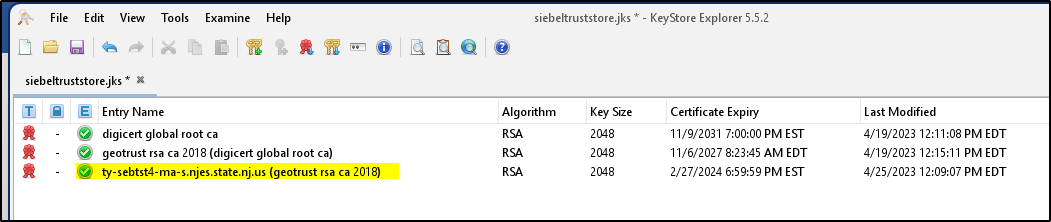


Add individual server certificates to this truststore to enable communication

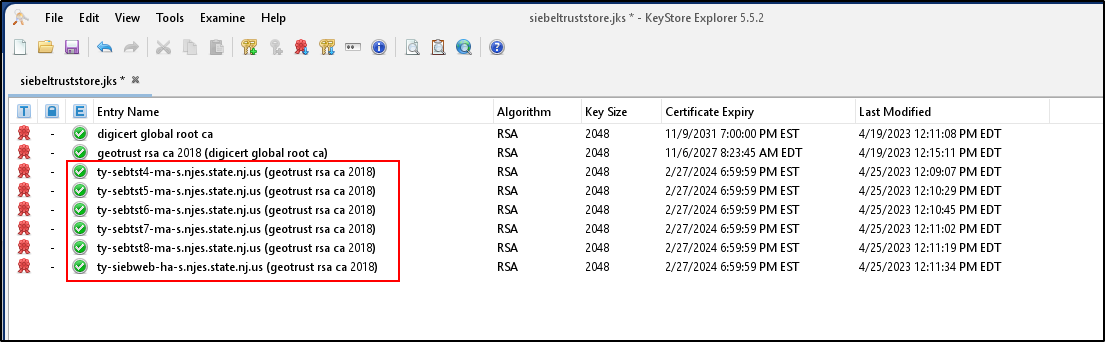






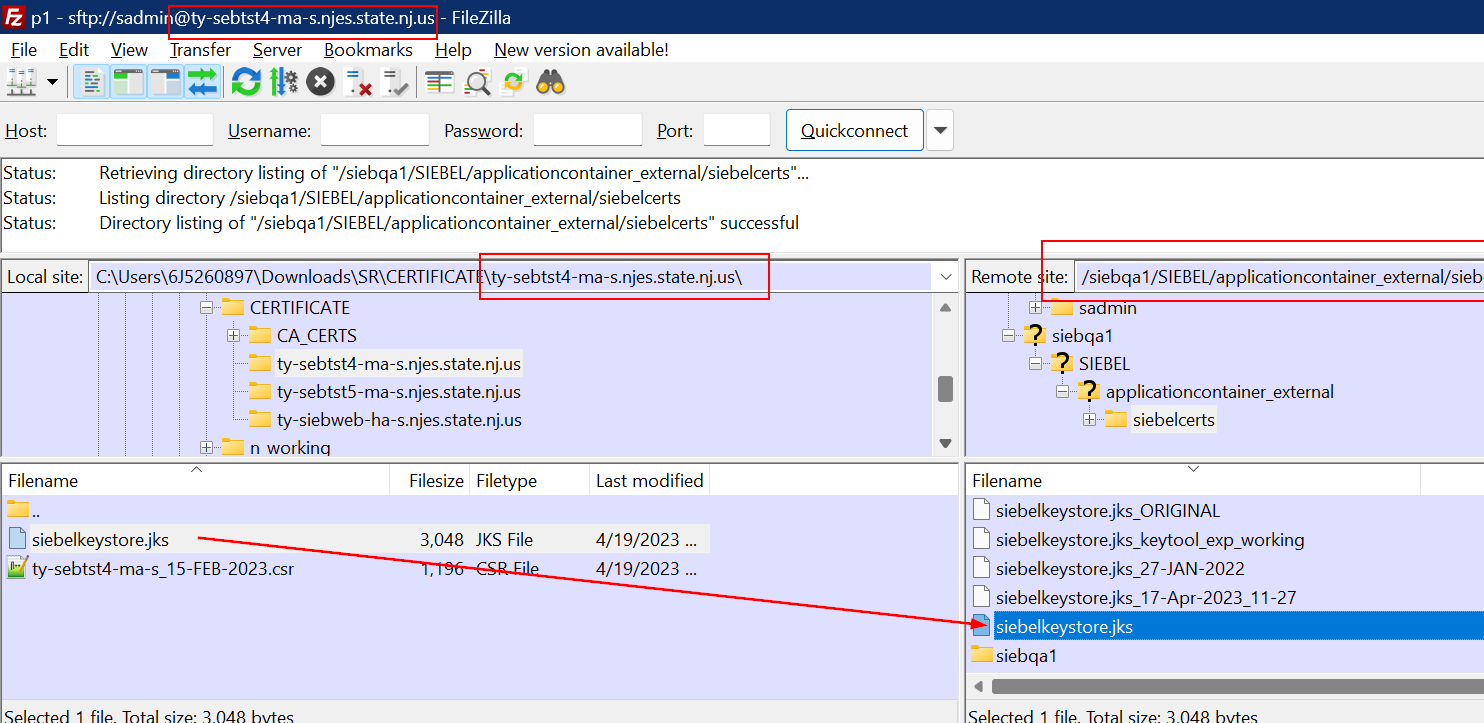


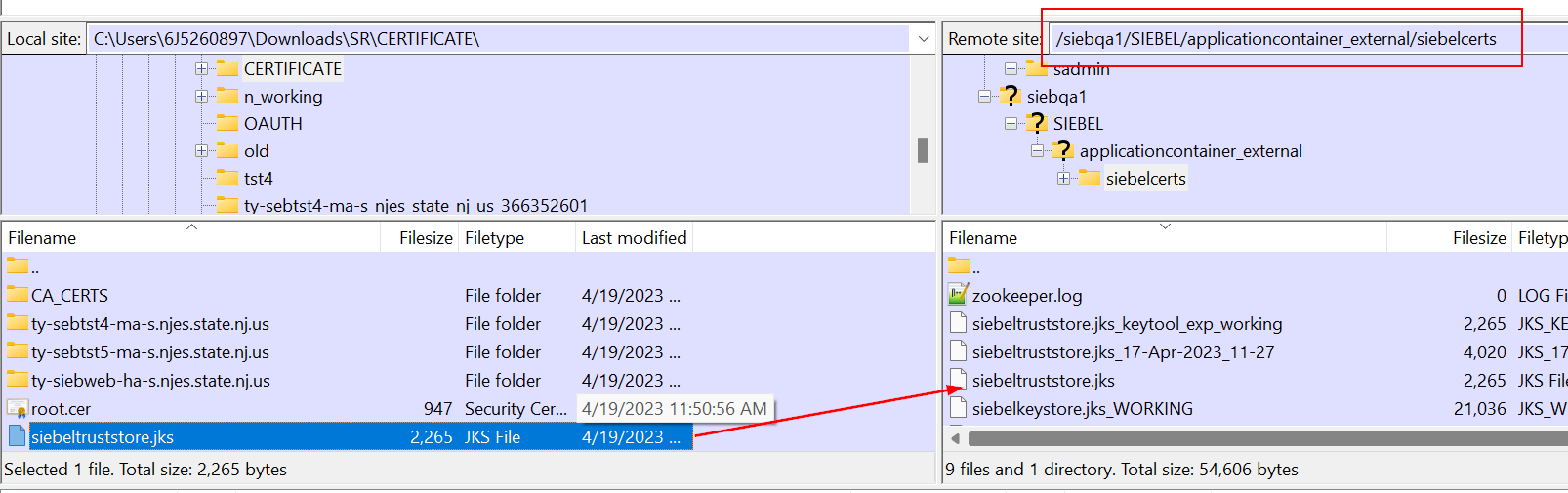
### Do the same for all certificates



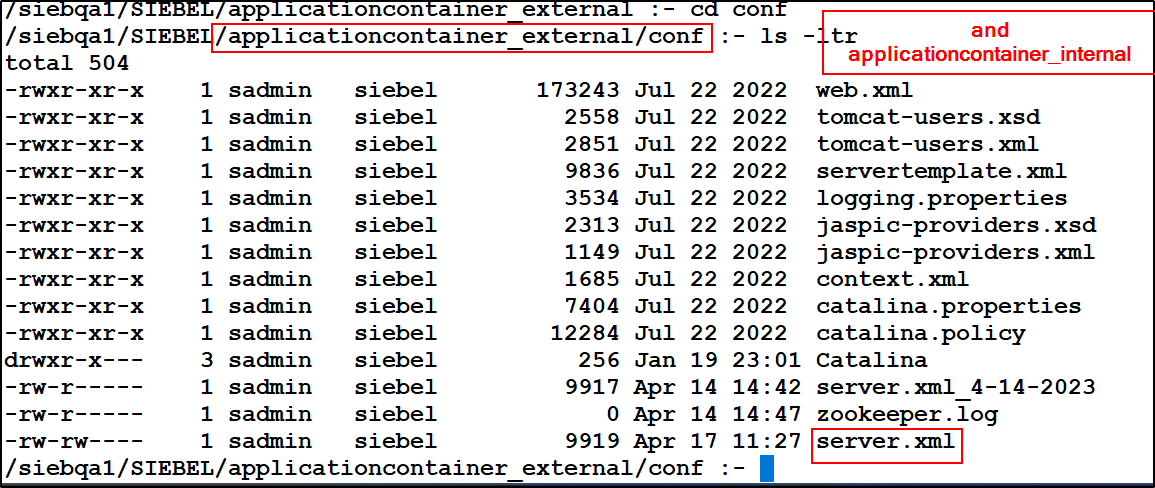
### **Make sure you save the keystore**

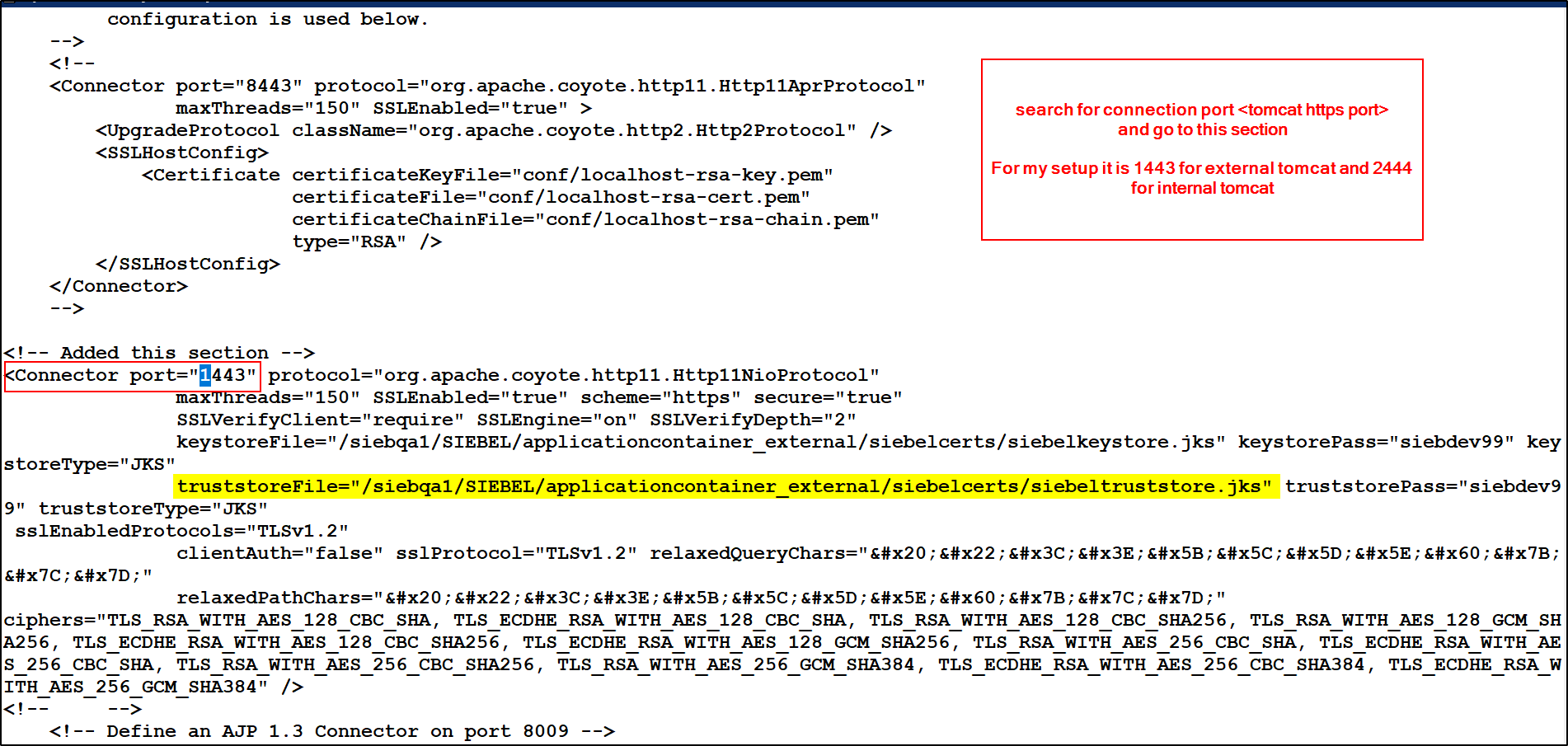
## Upload the keystore and truststore





## Update server.xml to point to trust store and keystore





## Place the truststore in all servers and update server.xml

## Restart Siebel services

## Test

