Contents

[Siebel certificates 1](#_Toc132799720)

[Create keystore 1](#_Toc132799721)

[NOTE 1](#_Toc132799722)

[example 1](#_Toc132799723)

[Generate CSR 1](#_Toc132799724)

[example 1](#_Toc132799725)

[Forward CSR to digicert 1](#_Toc132799726)

[Get certificate in return 2](#_Toc132799727)

[Get keytool-explorer 3](#_Toc132799728)

[Download the keystore from server if generated in server 6](#_Toc132799729)

[Inspect the certificate received from digicert 7](#_Toc132799730)

[Extract root certificate from CA cert chain 8](#_Toc132799731)

[Verify the extracted certificate 11](#_Toc132799732)

[Import server certificate 12](#_Toc132799733)

[Save the keystore before exiting or uploading to server 15](#_Toc132799734)

[Create Truststore and Import trust certificate 15](#_Toc132799735)

[Import root certificate 16](#_Toc132799736)

[Import intermediate certificate 18](#_Toc132799737)

[Save the keystore 20](#_Toc132799738)

[Import server certificate from all other servers to enable communication 21](#_Toc132799739)

[Upload the keystore and truststore 21](#_Toc132799740)

[Update server.xml to point to trust store and keystore 22](#_Toc132799741)

[Restart Siebel services 22](#_Toc132799742)

[Test 22](#_Toc132799743)

# 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

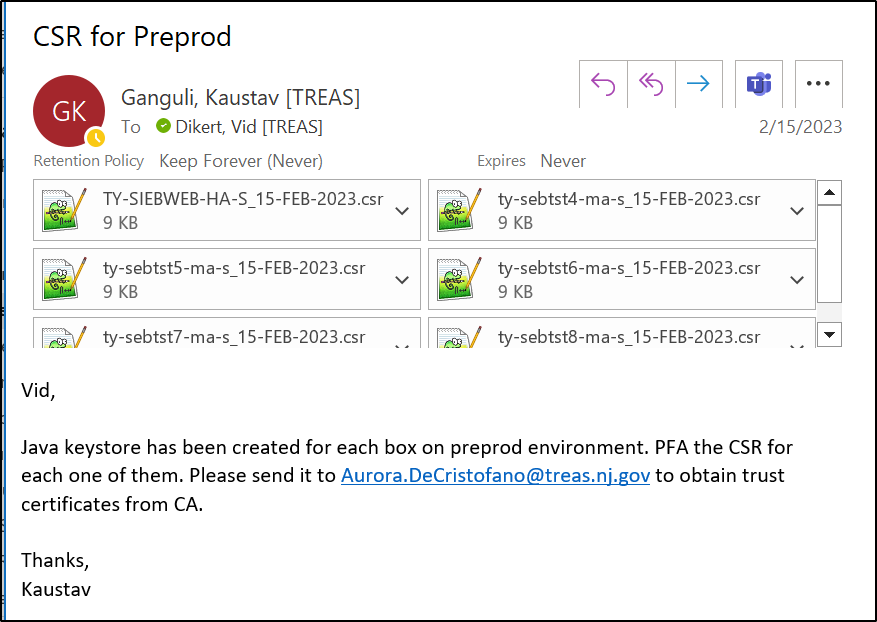
## Generate CSR

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

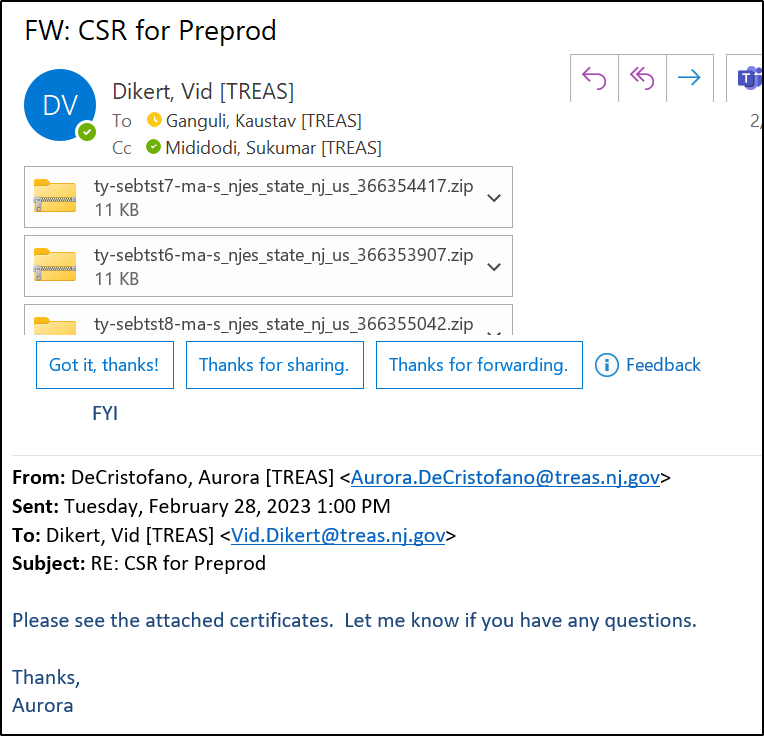
### example

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

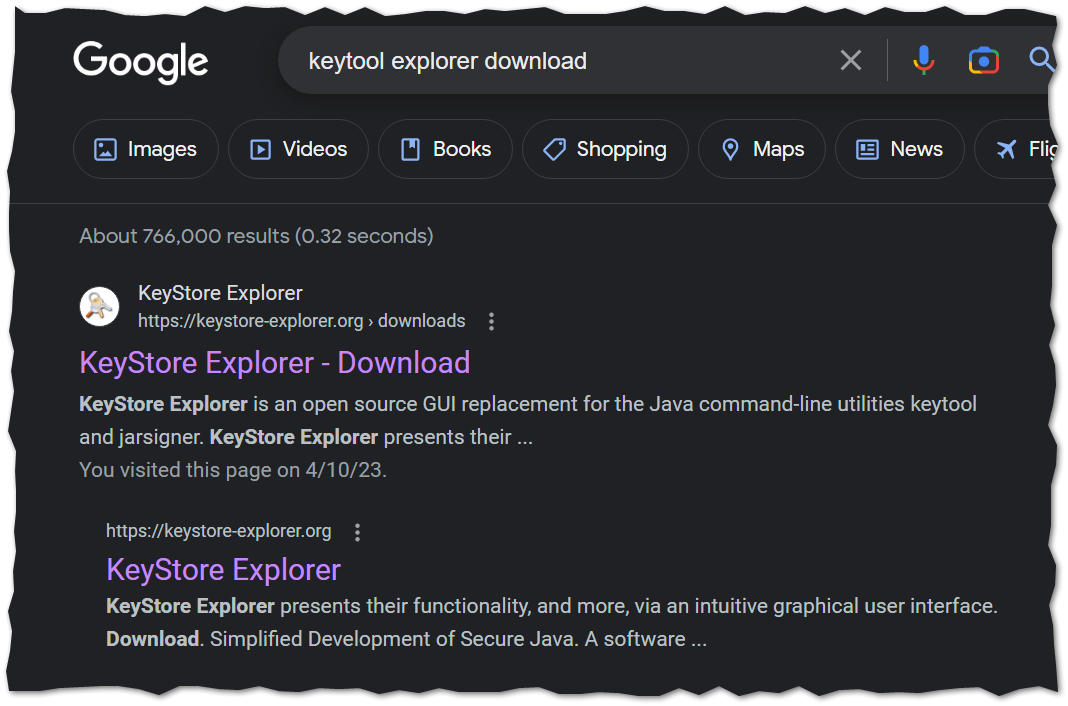
## Forward CSR to digicert

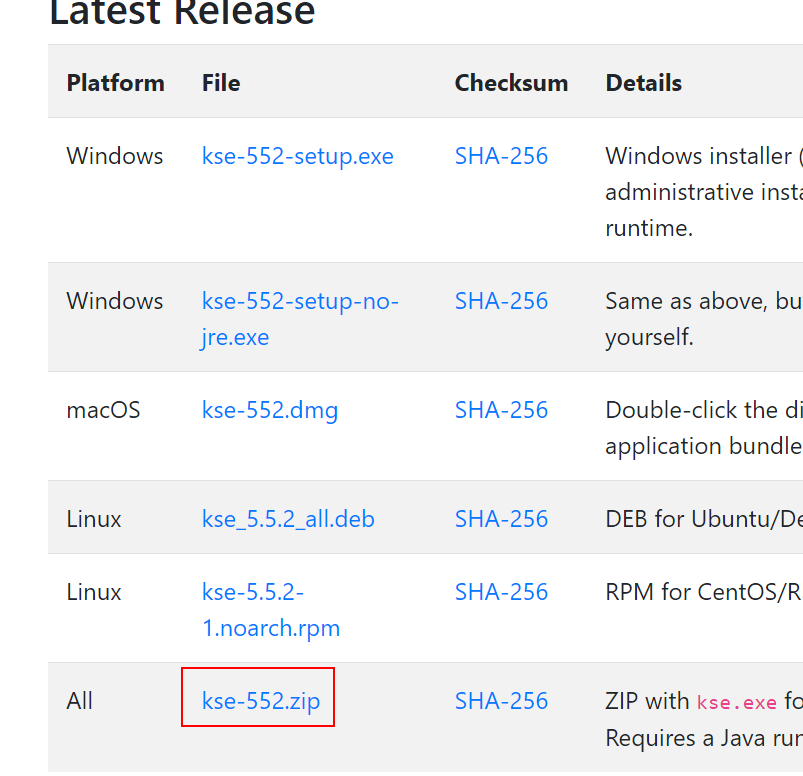


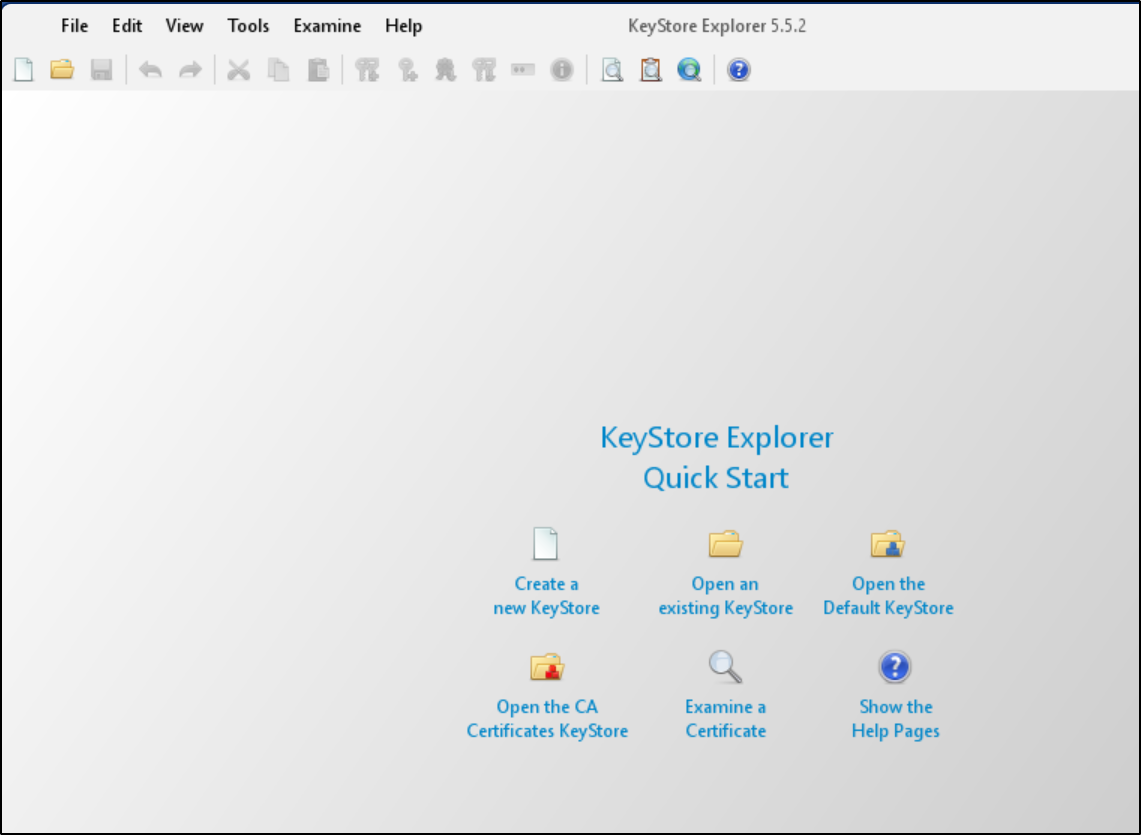
## Get certificate in return



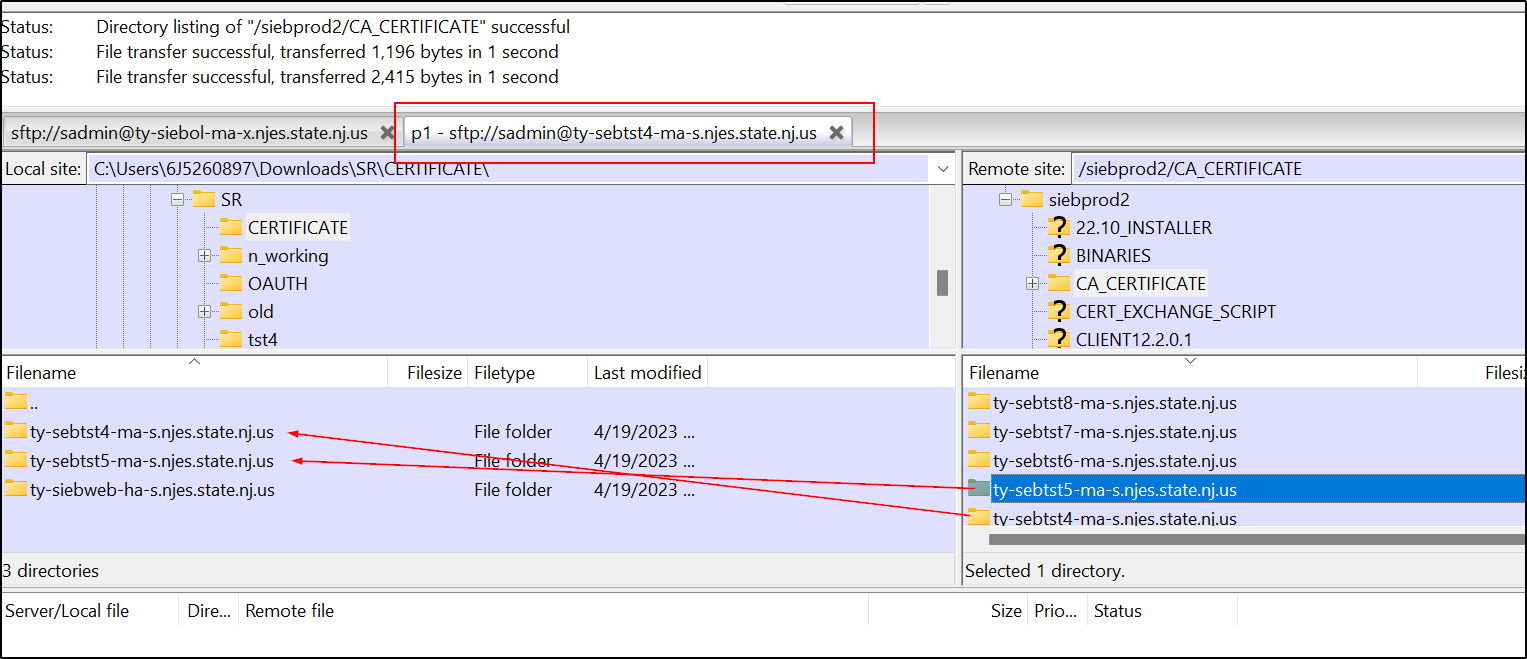
## Get keytool-explorer







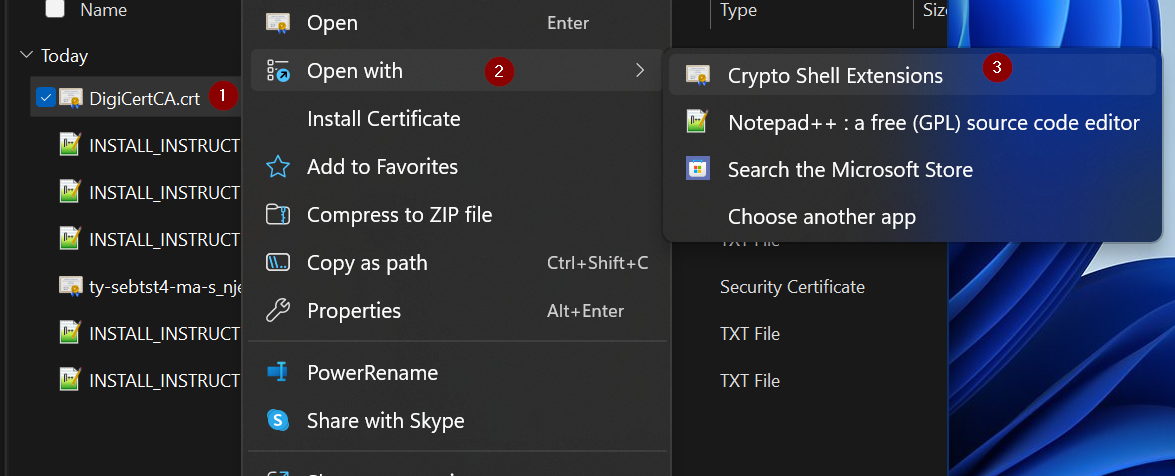
## Download the keystore from server if generated in server

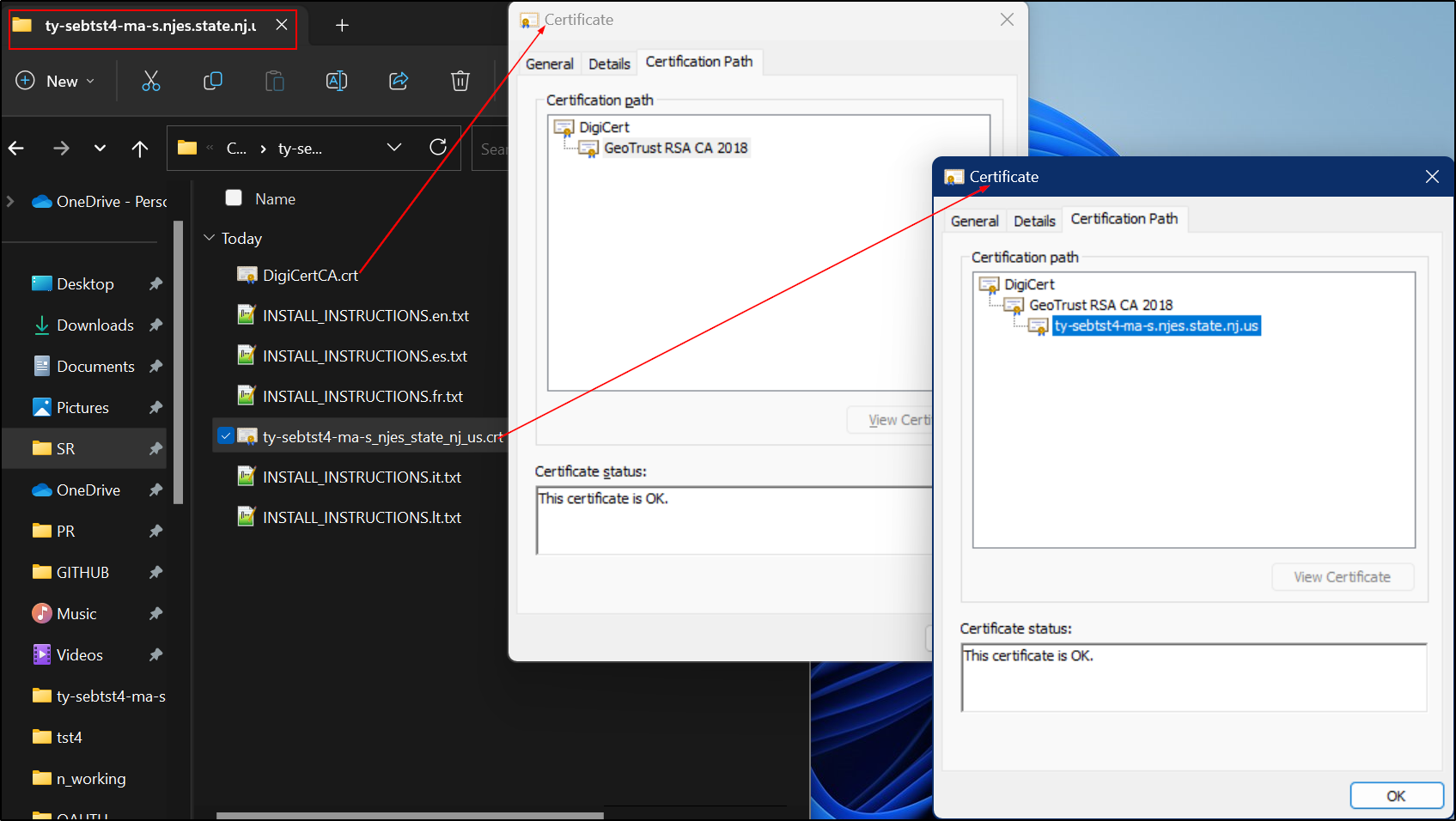


## Inspect the certificate received from digicert

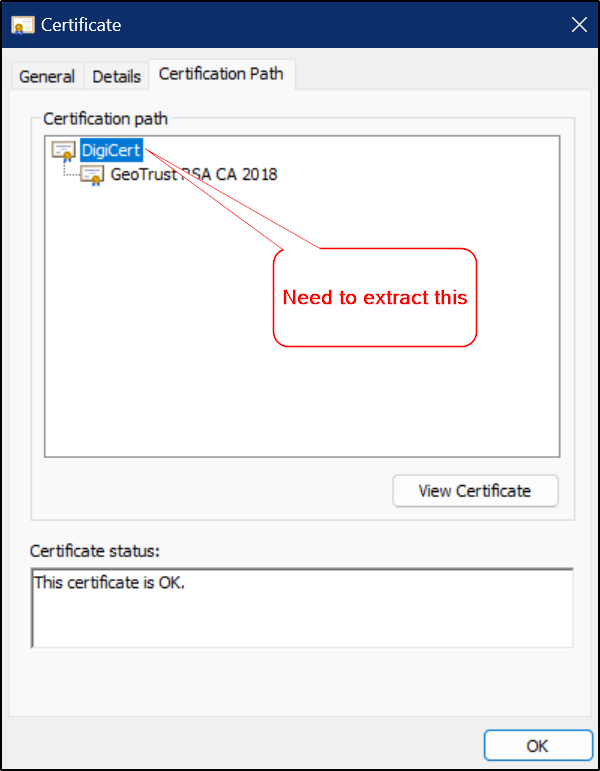
Digicert sends two files. One trust certificate that has root and intermediate certificate chained together, and a server certificate (for which it received the CSR for), that has all three certificates chained together –

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

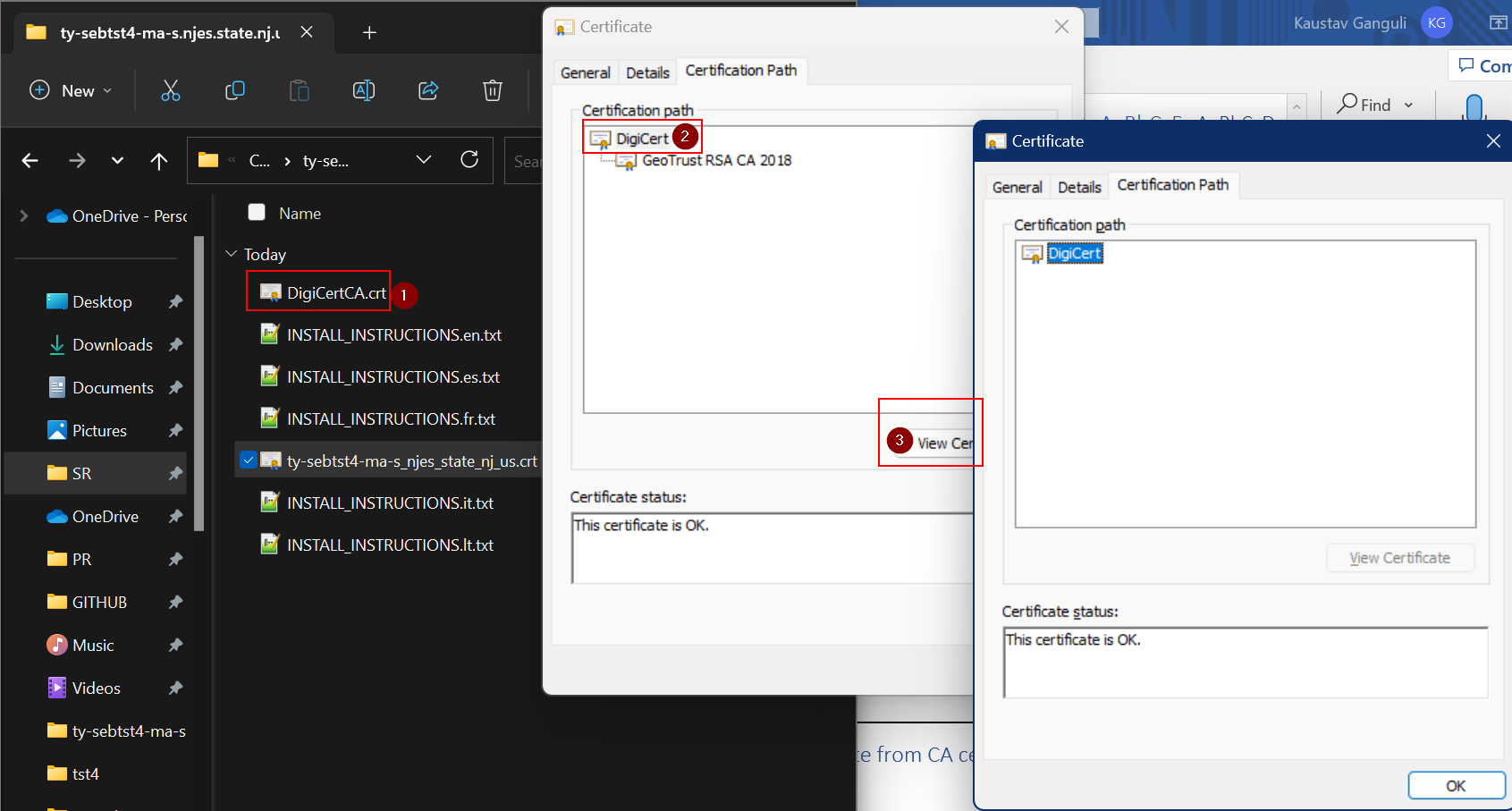


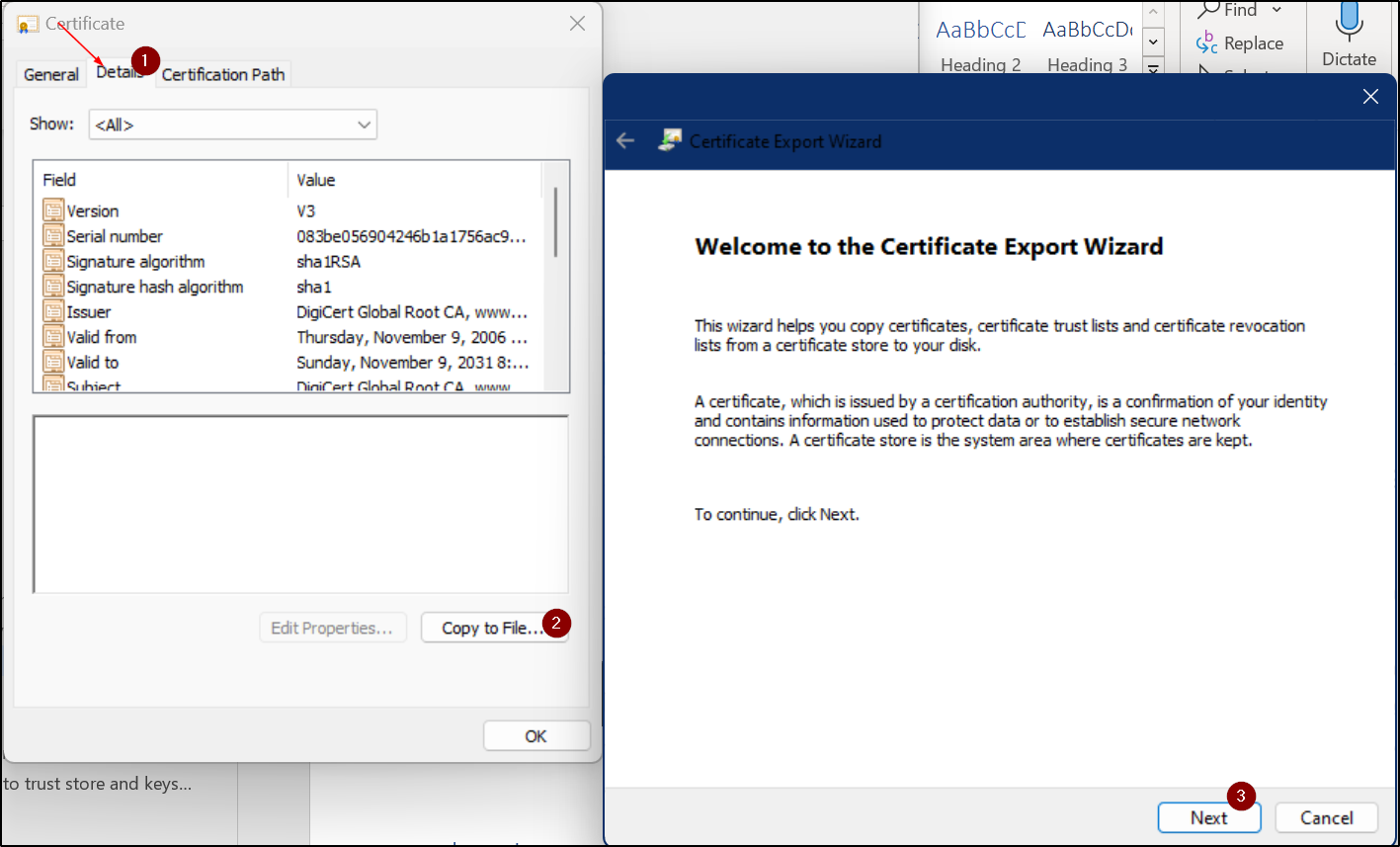


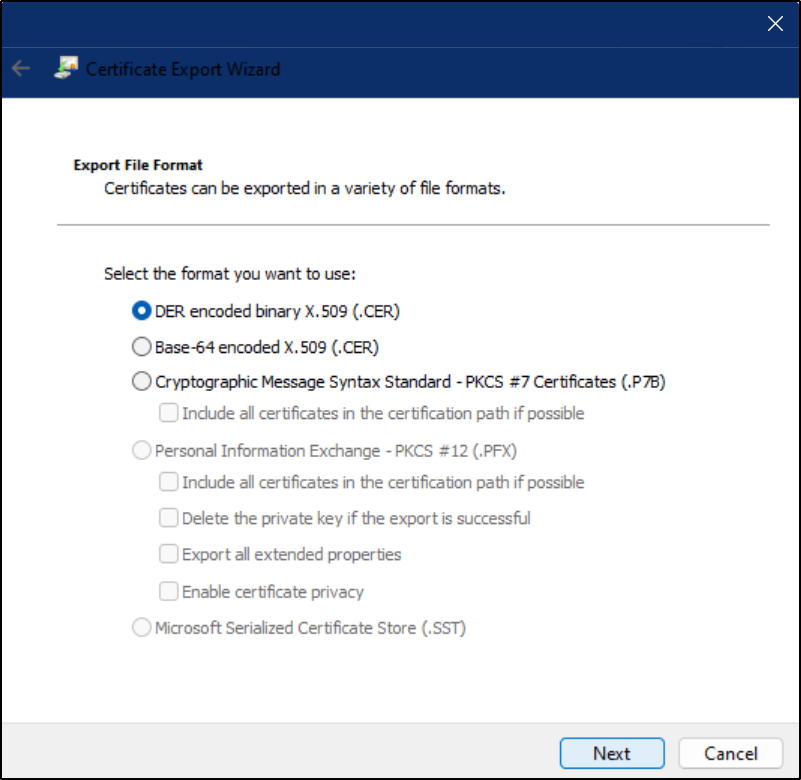
We would need the root certificate extracted in a separate file and then use keytool explorer to import. Without extracting the root certificate, keytool explorer only imports the intermediate certificate from “DigicertCA.crt” file

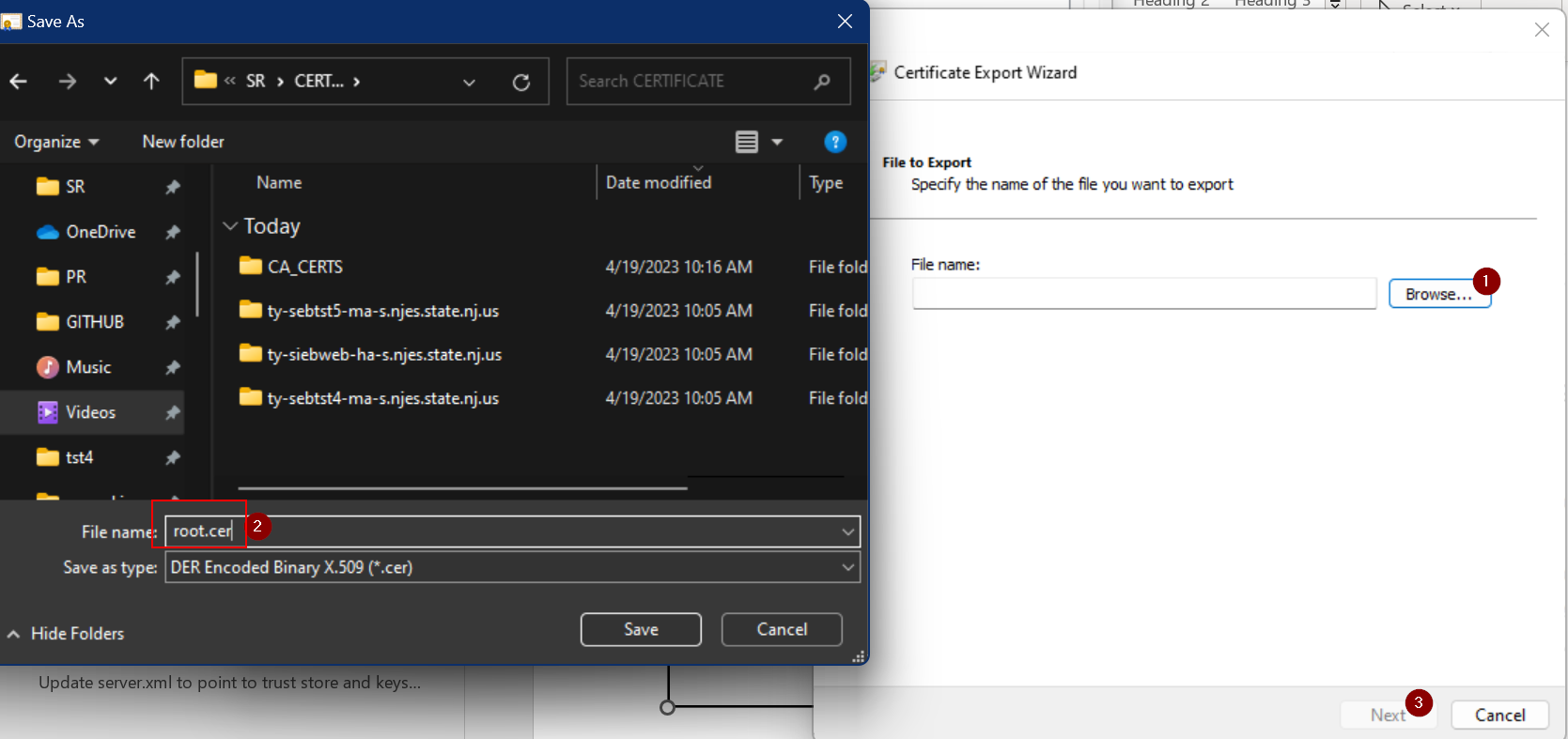


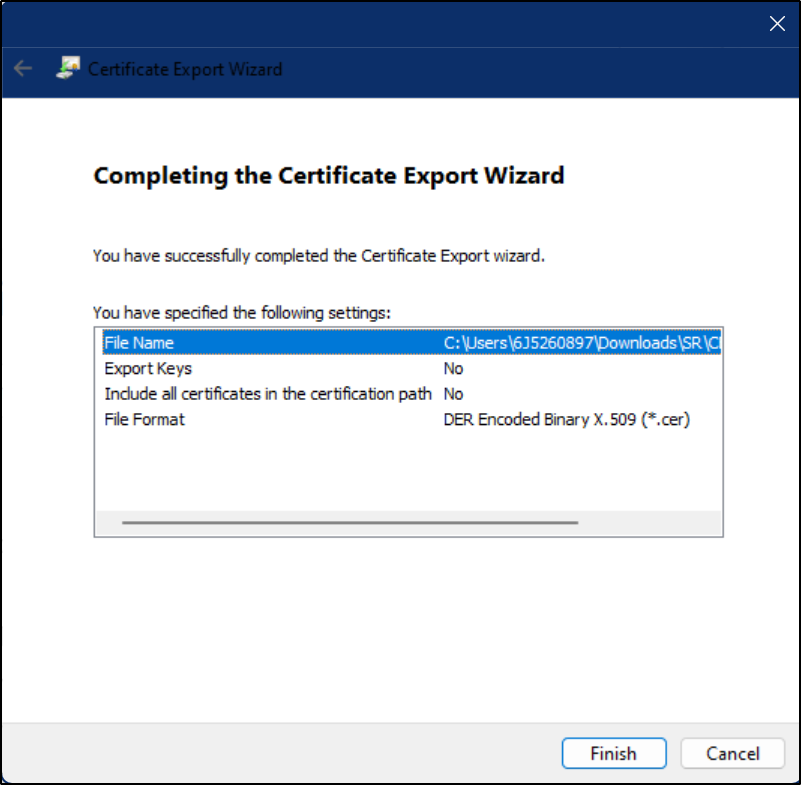
## Extract root certificate from CA cert chain



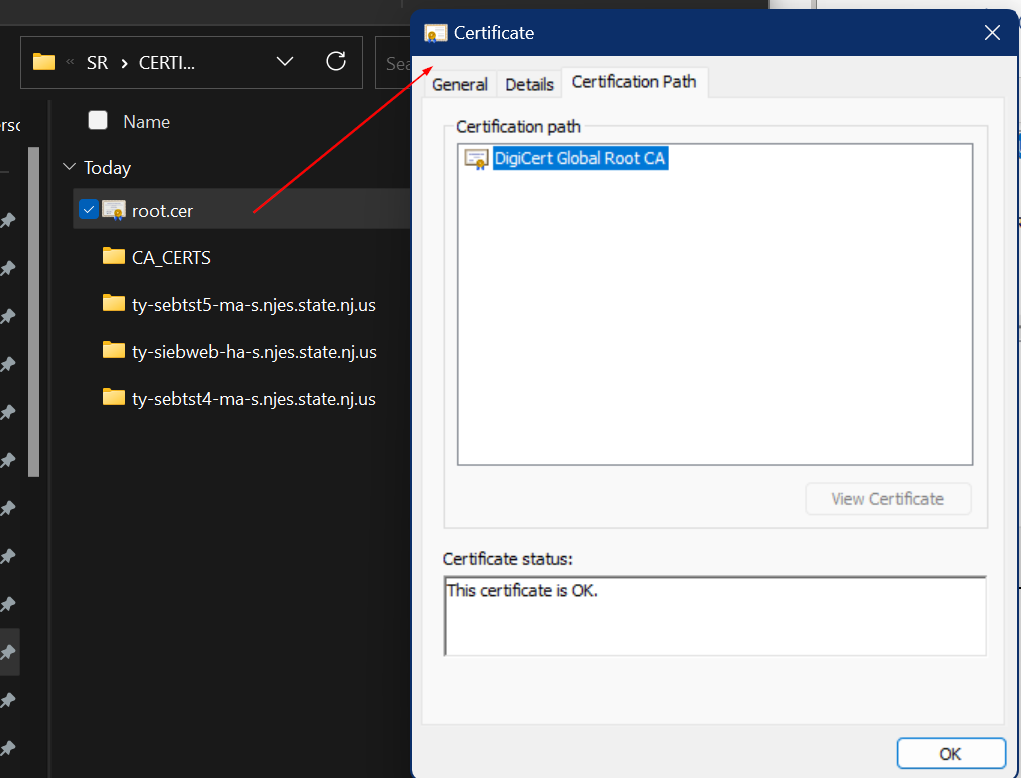






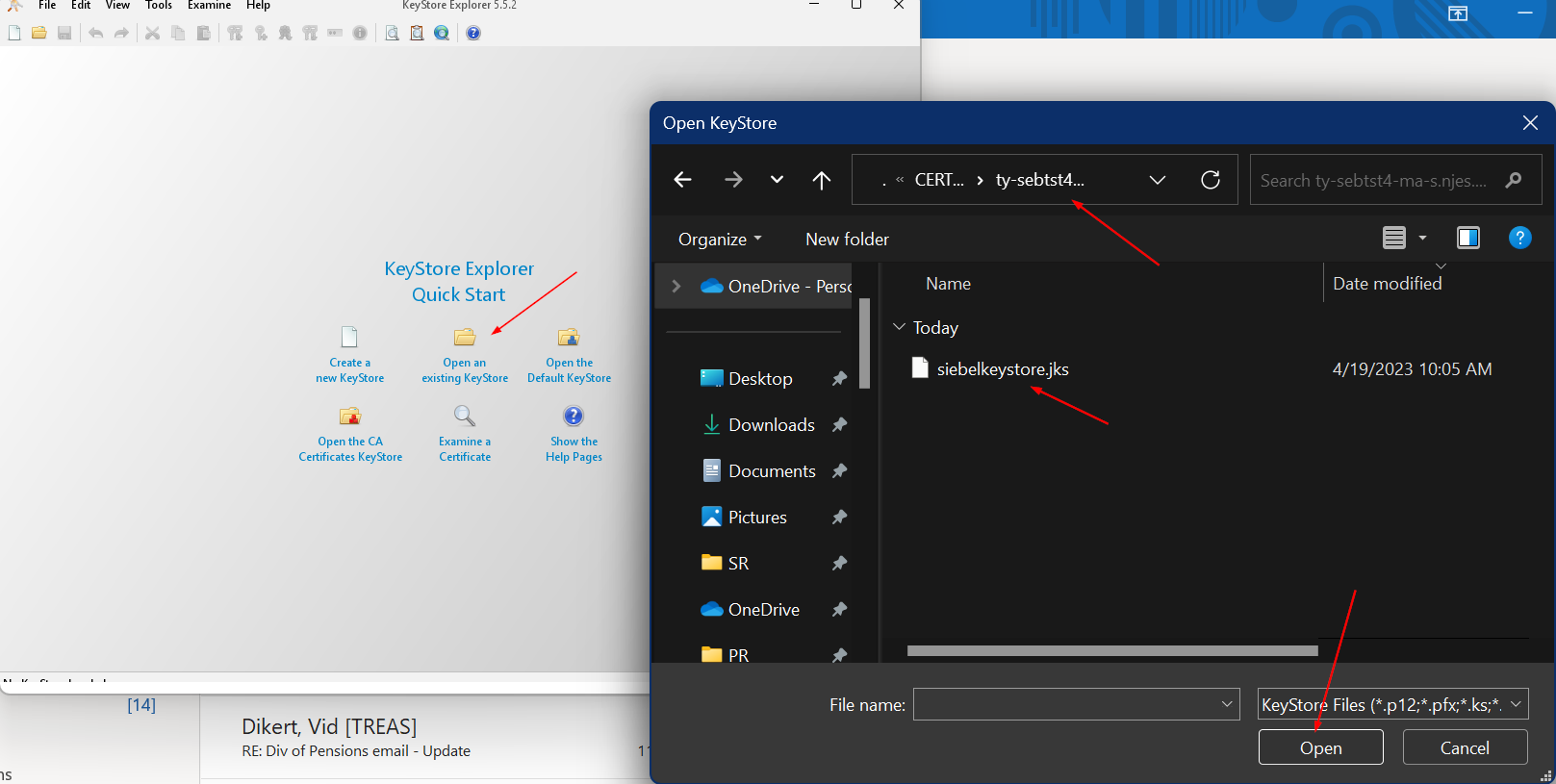


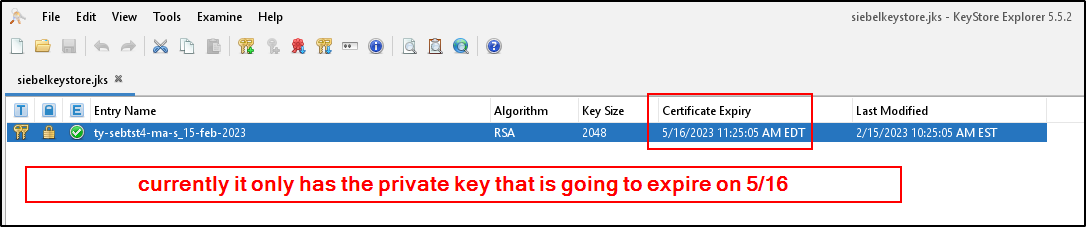
## Verify the extracted certificate

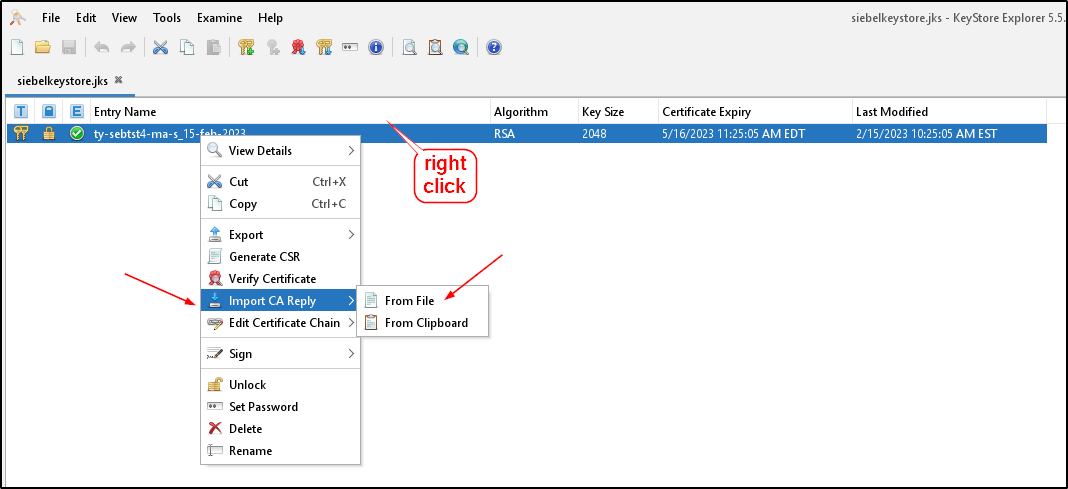


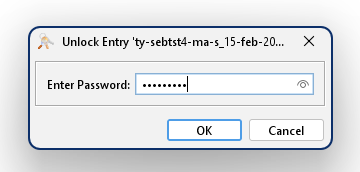
## Import server certificate

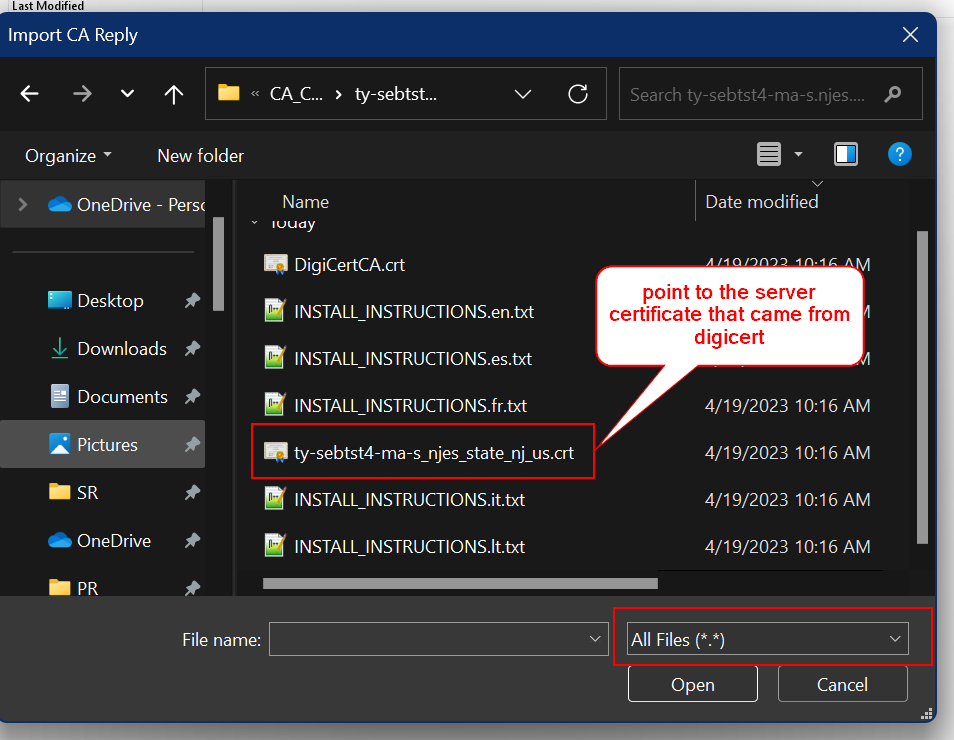
Open the keystore that was generated and downloaded

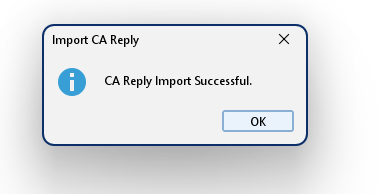


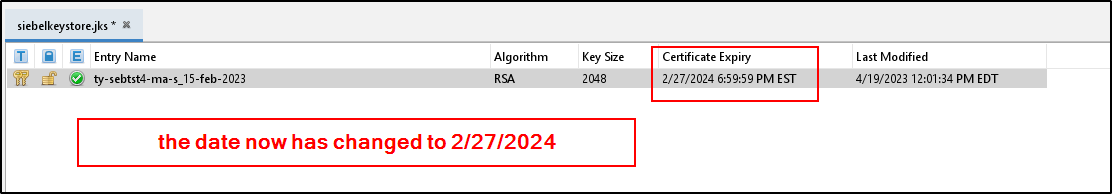


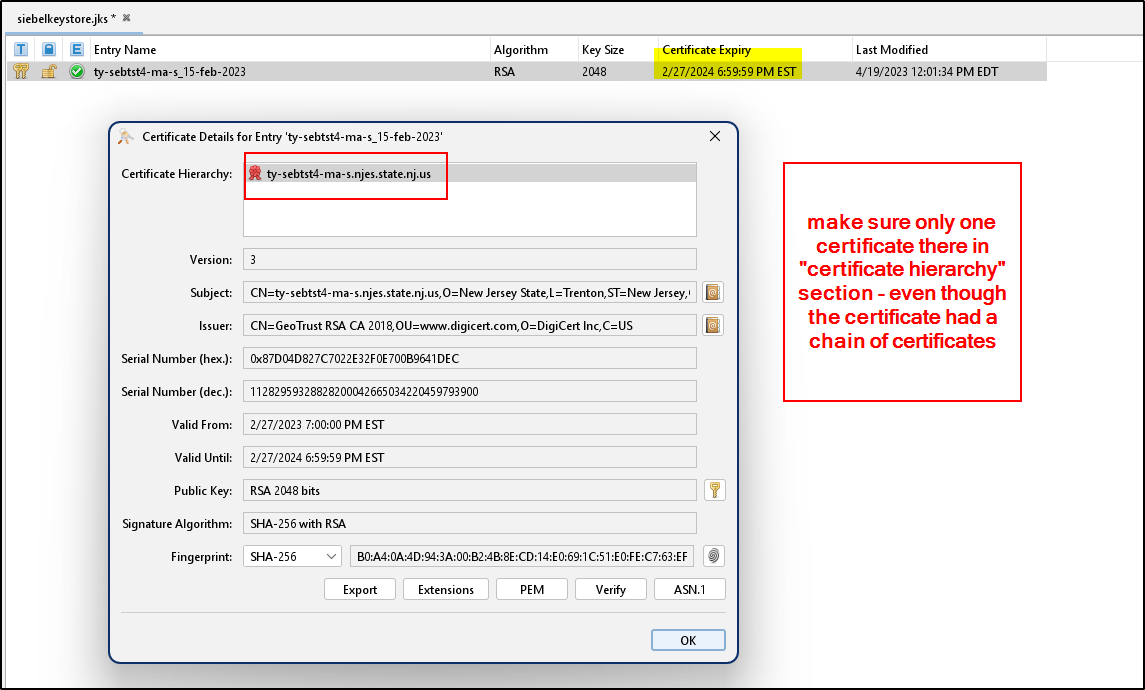




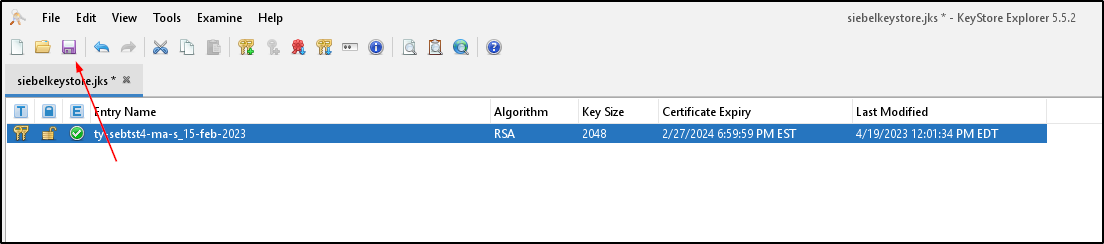




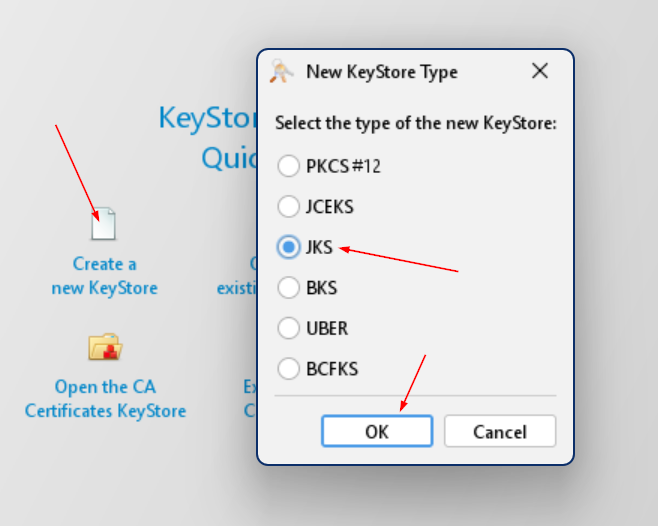


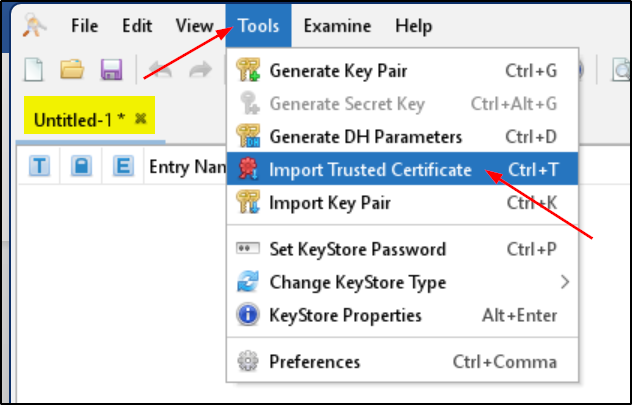


## Save the keystore before exiting or uploading to server

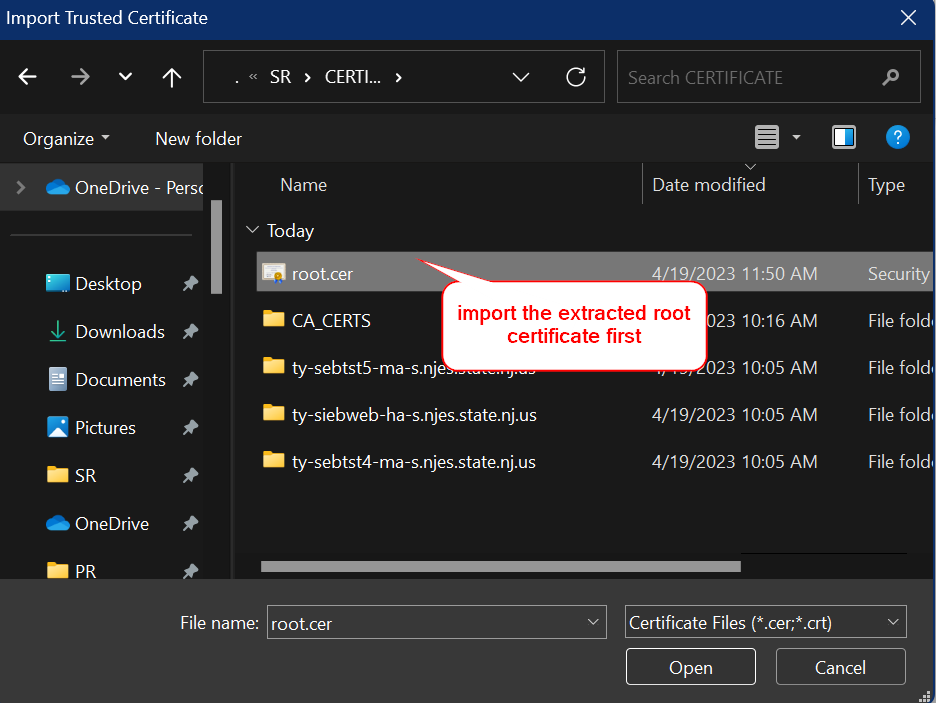


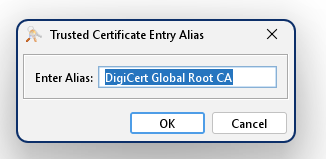
## Create Truststore and Import trust certificate

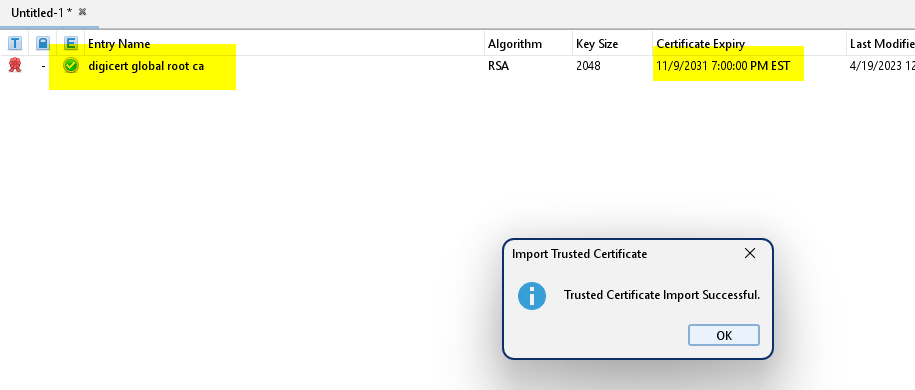




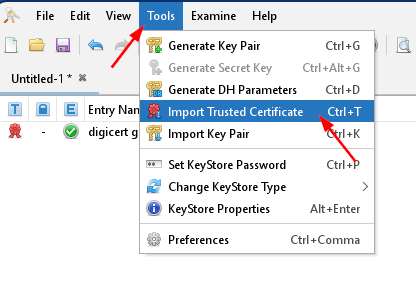
### Import root certificate

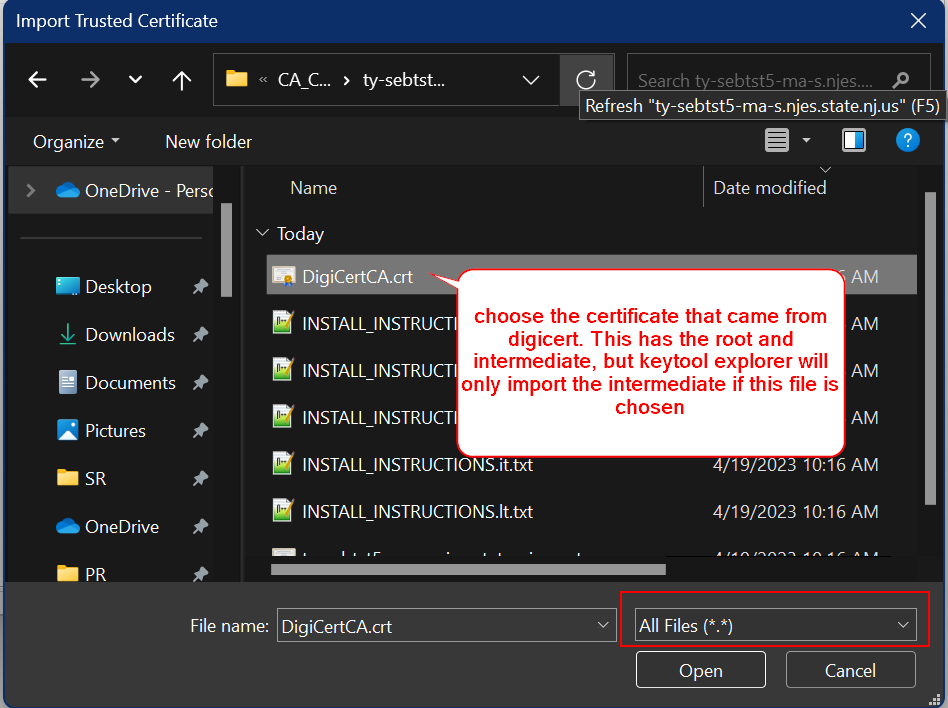


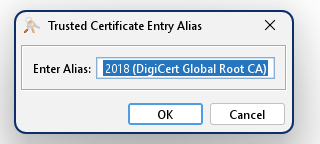


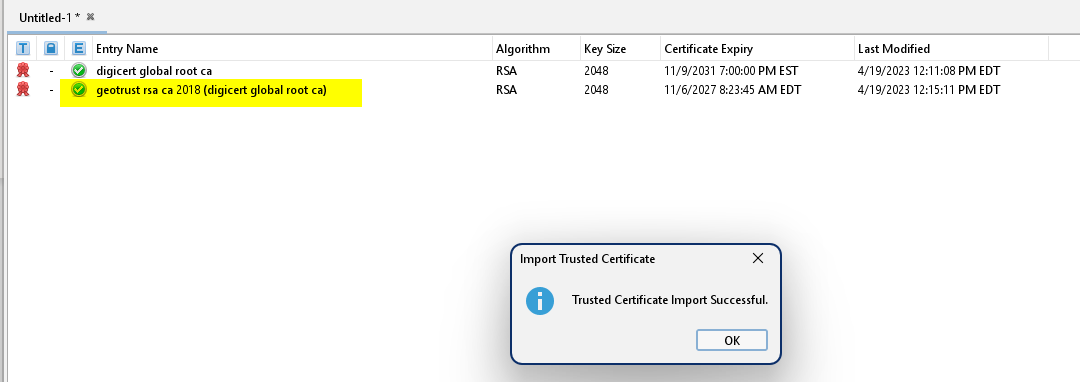


### Import intermediate certificate

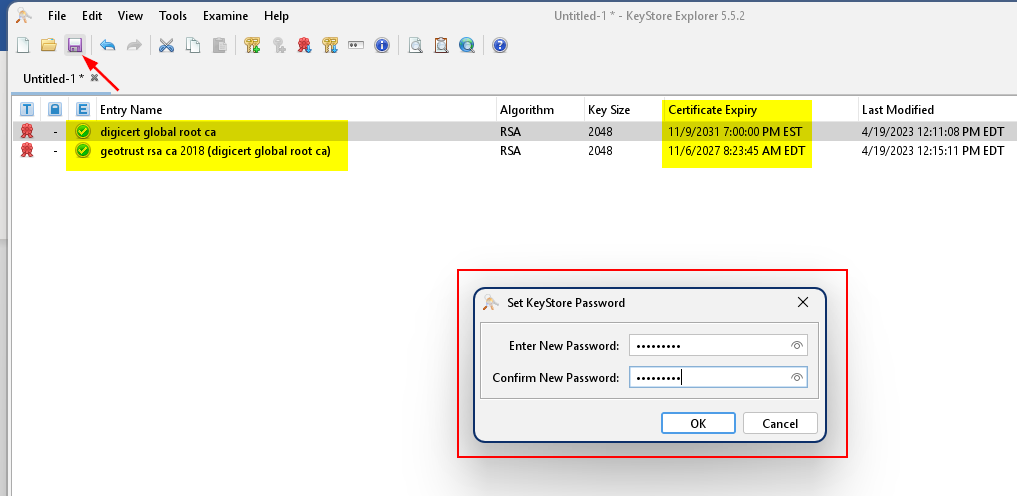


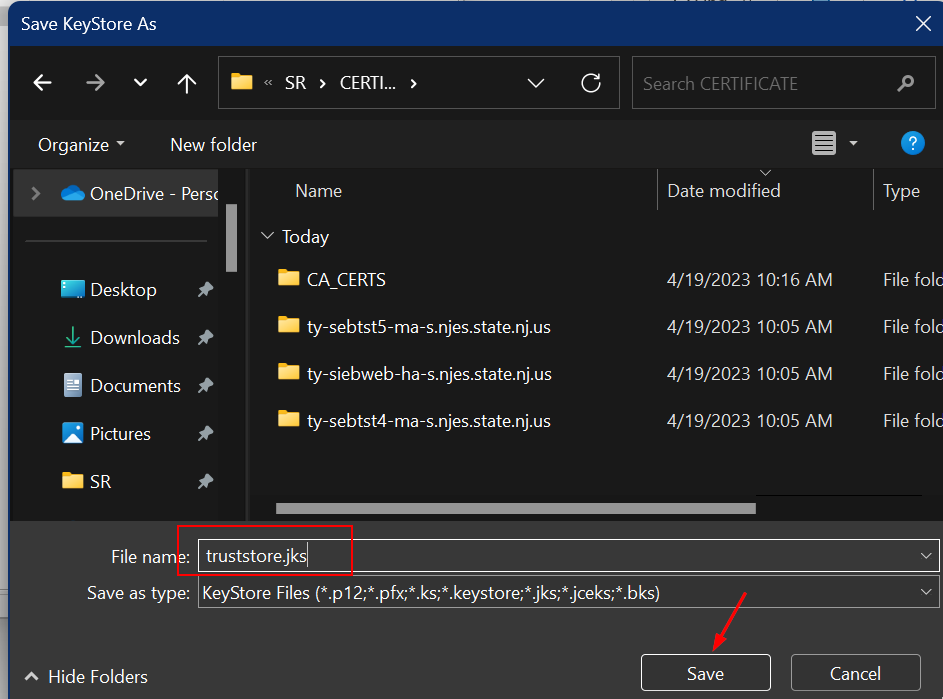


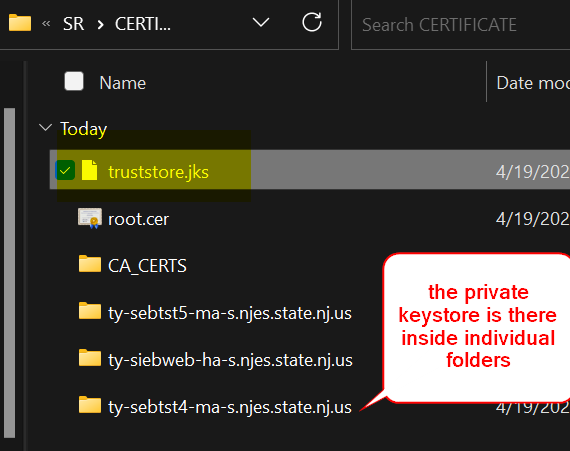




## Save the keystore



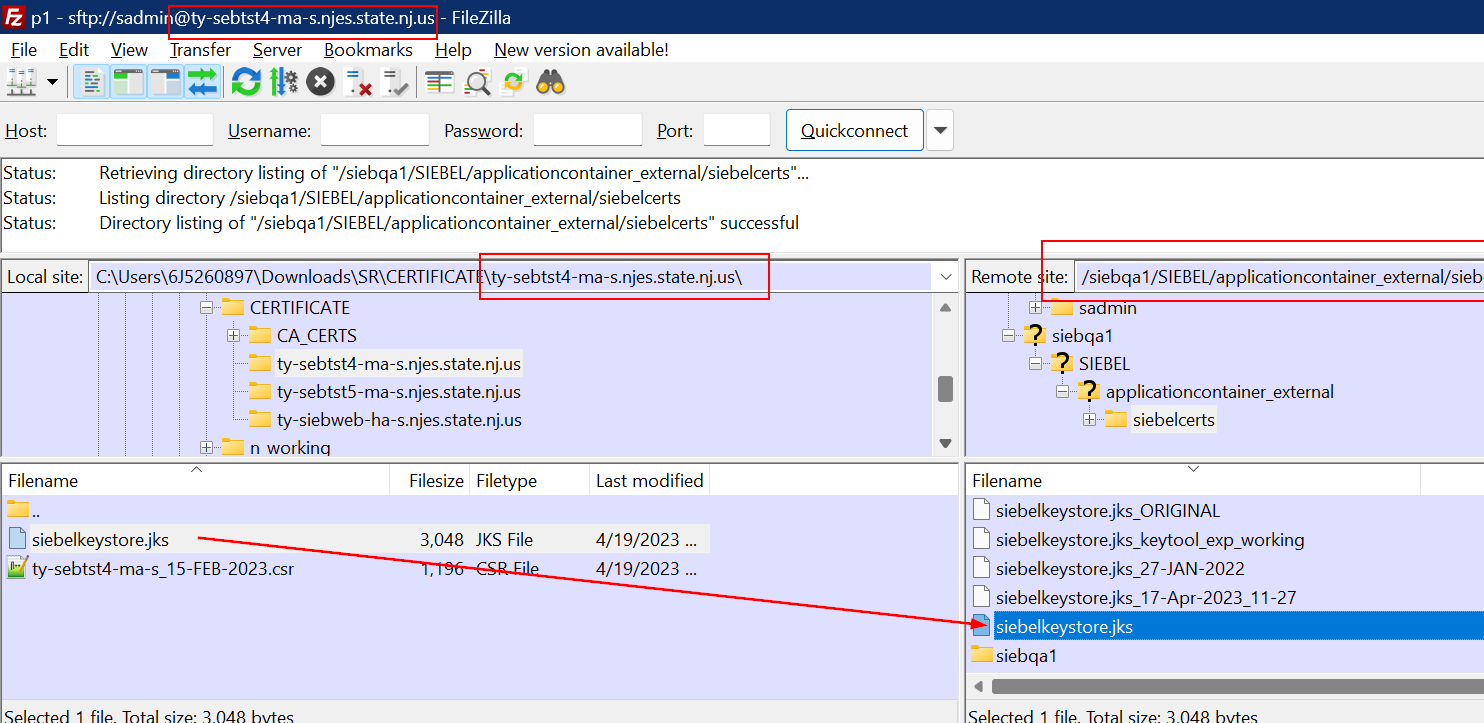


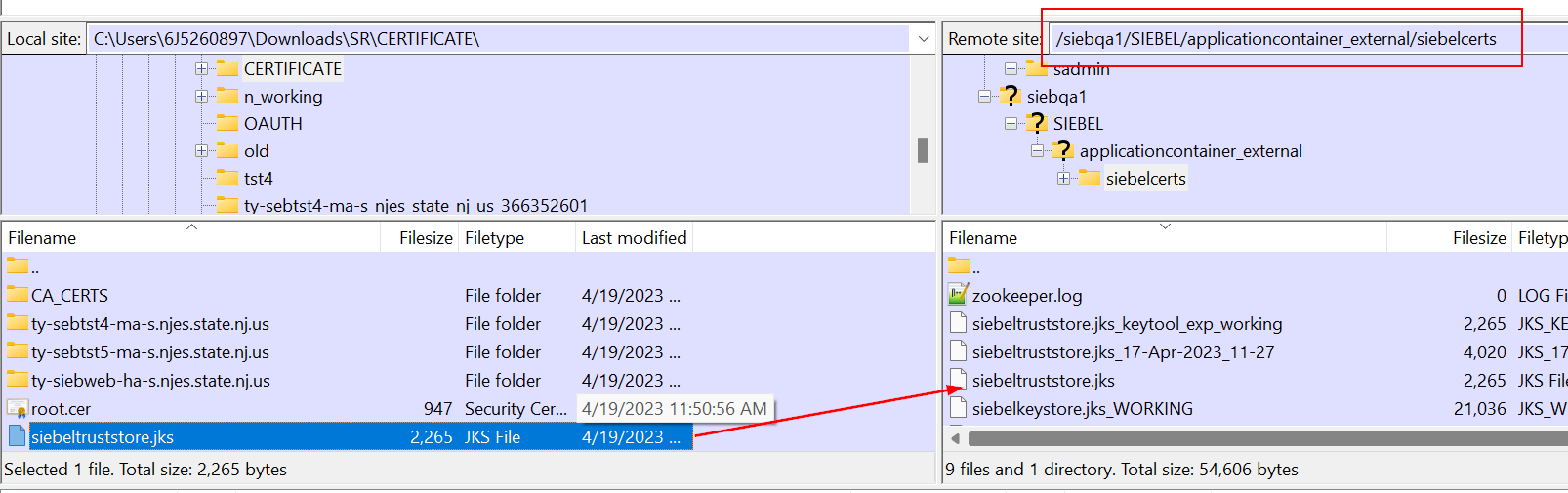


Renamed the “truststore.jks” to “siebeltruststore.jks” to match server configuration

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

## Upload the keystore and truststore





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

## Restart Siebel services

## Test

