Renew/Update SSL certs for PTPI(Cloud).

1. Why SSL certs are used in PTPI :

The PTPI application communicates with ROM using the SSL cert based authentication.

The types of the cert files in the jks file are mentioned in their order.

1. Root cert
2. Intermediate cert
3. Actual SSL leaf cert

2. Possible Scenarios For Expiry :

If any of the leaf, root or intermediate files are expired , generate the files from Rabo Cert Portal and replace the expired certificate with the new one.

3. Tools Used :

1. Terminal in Mac
2. Keystore Explorer in Mac

4. PreRequisites to raise a request for new Cert :

To raise the certificate we need to create a Certificate Signing Request (CSR) .

The steps involved are :

a. Generate an un-signed Rabo certificate with the public and the private key
b. Generate a CSR file from the private key created

a .Create a private key :

Execute the below command from the terminal in Mac:

```
Command : keytool -genkey -keyalg RSA -keysize 2048 -sigalg SHA256withRSA -alias <aliasName> -keystore
<keystoreName> -validity <ValidityDays>

Example : keytool -genkey -keyalg RSA -keysize 2048 -sigalg SHA256withRSA -alias ptpiacptkey -keystore ptpi-
acpt-keystore.jks -validity 360
```

While executing this command , you will be asked for a password. Post entering the password , we need to enter the details for the cert . They are as follows :

Field	Value
CN (Common Name). Keytool might ask you for your "first and last name" here.	ptpi-acpt.rabobank.nl (used in PTPI acceptance)
OU (Organizational Unit)	Payments Solution
O (Organization)	Cooperatieve Rabobank U.A.

ST (State)	Utrecht
L (Locality)	Utrecht
C (Country)	NL
E (Email address)	**Please leave this blank if possible.** We have seen that email addresses in certificates can sometimes be scrambled into unreadable strings in the certificate. In case you are mandated to fill out this address, please consult with Team Speed

b. Generate CSR file :

Execute the below commands from terminal in Mac

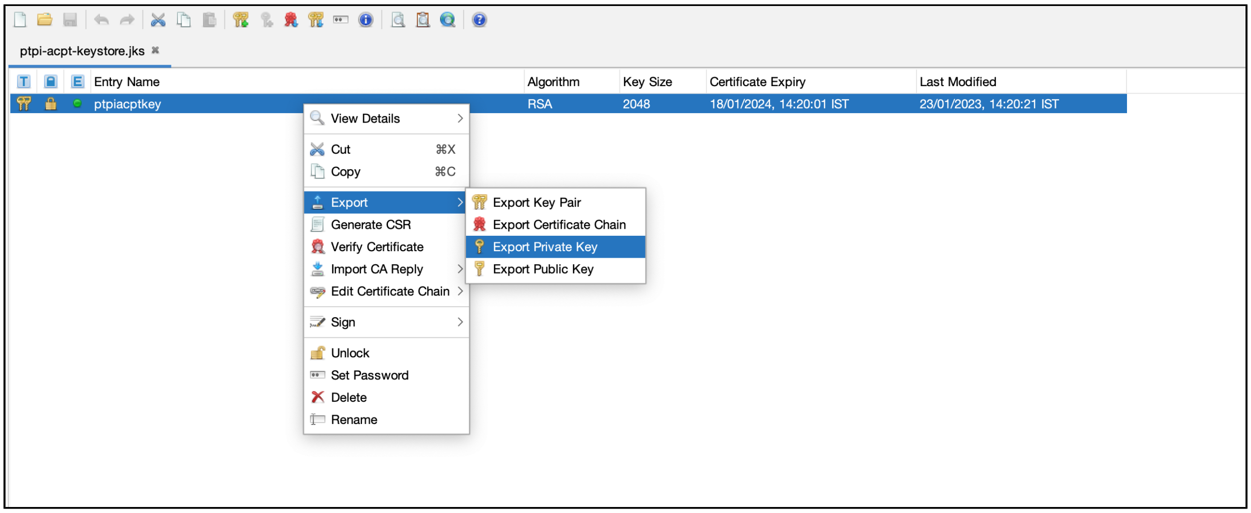
```
Command : keytool -certreq -keystore <privateKeyNameFromStep1> -keyalg RSA -alias <aliasName> -file
<csrFileName>

Example : keytool -certreq -keystore ptpi-acpt-keystore.jks -keyalg RSA -alias ptpiacptkey -file ptpi-acpt.csr
```

Now you will have a CSR file ready.

c. Export the private key alone from the jks keystore :

Open the jks keystore file created in Keystore explorer, right click on the key and select Export Export Private Key

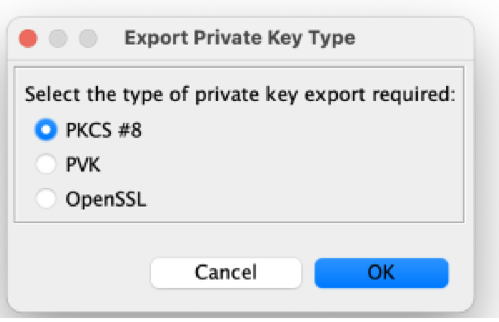


ptpi-acpt-keystore.jks

T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
		●	ptpiacptkey	RSA	2048	18/01/2024, 14:20:01 IST	23/01/2023, 14:20:21 IST

It will ask for password, enter the password.

Next a pop up will be shown to export the private key type. Choose PKCS #8 as shown below.

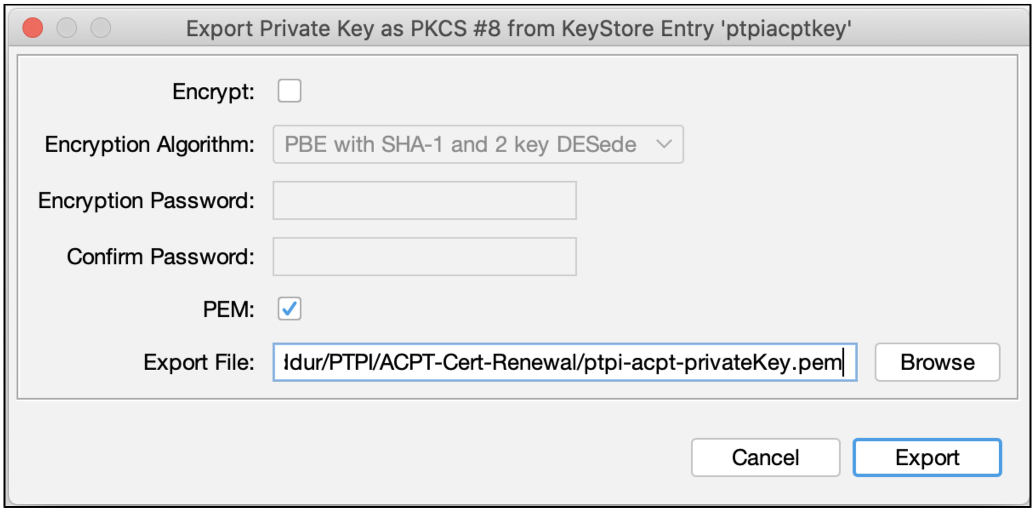


Export Private Key Type

Select the type of private key export required:

● PKCS #8
○ PVK
○ OpenSSL

Disable the Encrypt check box and export the private key as pem and store it as .pem



Export Private Key as PKCS #8 from KeyStore Entry 'ptpiacptkey'

Encrypt: □

Encryption Algorithm: PBE with SHA-1 and 2 key DESede

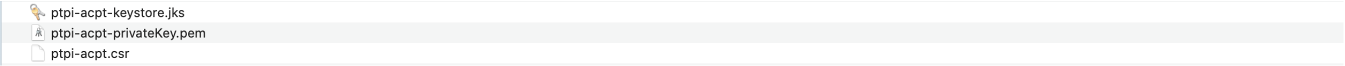
Encryption Password:

Confirm Password:

PEM: ☑

Export File: ldur/PTPI/ACPT-Cert-Renewal/ptpi-acpt-privateKey.pem

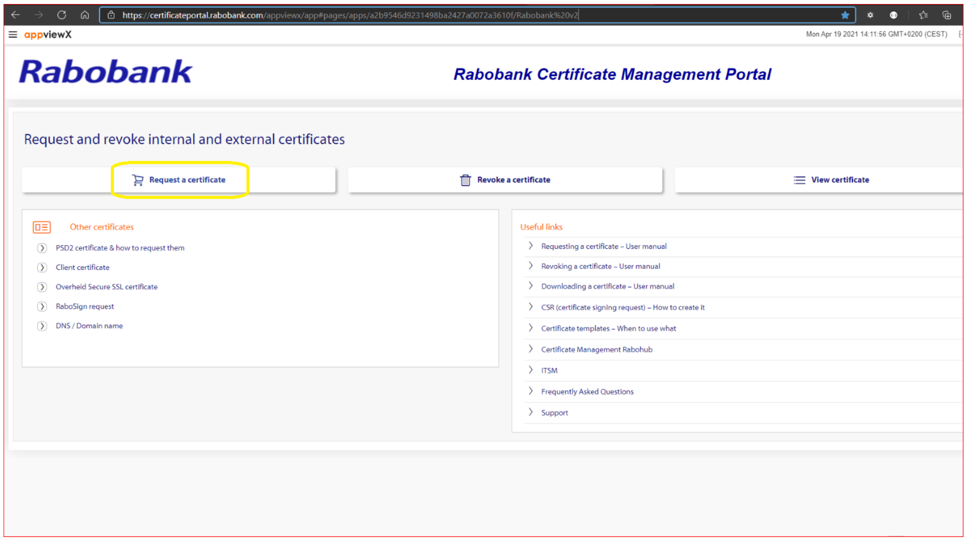
Now we will have 3 files (2 generated file and one exported private key)



ptpi-acpt-keystore.jks
ptpi-acpt-privateKey.pem
ptpi-acpt.csr

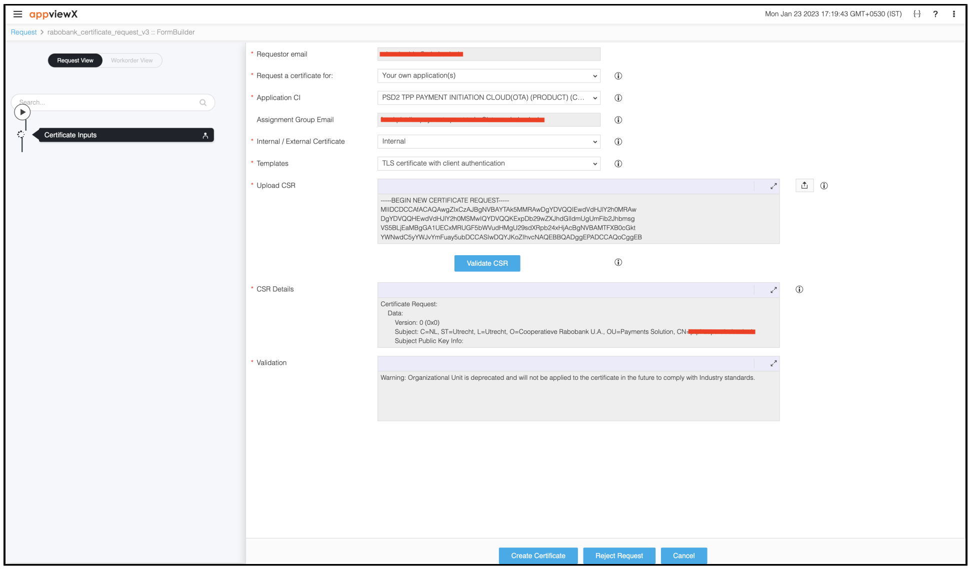
5. Raise a request in Rabo Cert Portal :

1. Go to https://certificateportal.rabobank.com/
2. Login with SSO



https://certificateportal.rabobank.com/appviewx/app#pages/apps/a2b9546d9231498ba2427a0072a3610f/Rabobank%20v2
appviewX
Mon Apr 19 2021 14:11:56 GMT+0200 (CEST)
Rabobank
Rabobank Certificate Management Portal
Request and revoke internal and external certificates
Request a certificate
Revoke a certificate
View certificate
Other certificates
PSD2 certificate & how to request them
Client certificate
Overheid Secure SSL certificate
RaboSign request
DNS / Domain name
Useful links
Requesting a certificate – User manual
Revoking a certificate – User manual
Downloading a certificate – User manual
CSR (certificate signing request) – How to create it
Certificate templates – When to use what
Certificate Management Rabohub
ITSM
Frequently Asked Questions
Support

3. Choose the following options:
    a. Request a certificate for: Your own application(s)
    b. Application CI: **Enter your Application CI**
    c. Internal / External: **Internal**
    d. Templates: **TLS certificate with client authentication**
    e. ***Upload your CSR file*** that you created in previous steps
    f. Click ***Validate***
    g. Click ***Create Certificate***
    h. **Confirm submission**


appviewX
Mon Jan 23 2023 17:19:43 GMT+0530 (IST)
Request > rabobank_certificate_request_v3 :: FormBuilder
Request View
Workorder View
Search...
Certificate Inputs

* Requestor email	[redacted]
* Request a certificate for:	Your own application(s)
* Application CI	PSD2 TPP PAYMENT INITIATION CLOUD(OTA) (PRODUCT) (C...
Assignment Group Email	[redacted]
* Internal / External Certificate	Internal
* Templates	TLS certificate with client authentication

* Upload CSR

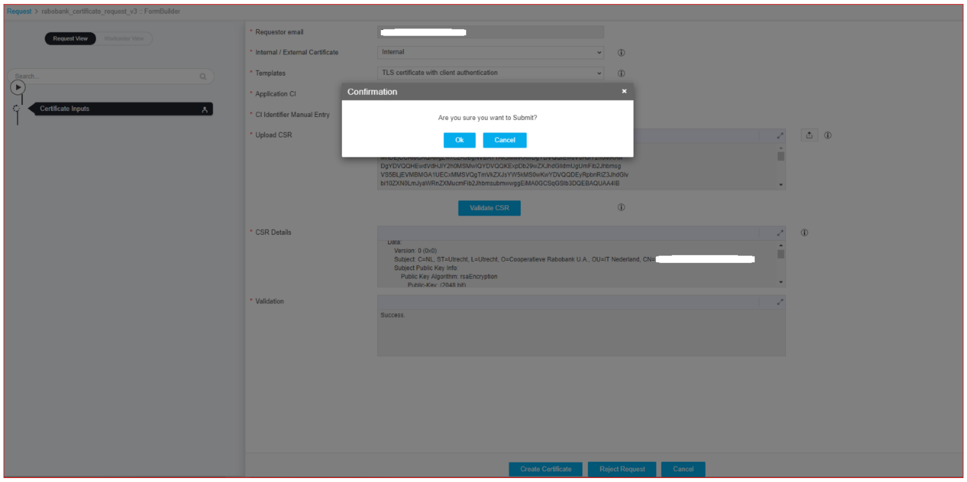
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDCDCCAfACAQAwgZIxCzAJBgNVBAYTAk5MMRAwDgYDVQQIEwdVdHJlY2h0MRAw
DgYDVQQHEwdVdHJlY2h0MSMwIQYDVQQKExpDb29wZXJhdGlldmUgUmFib2Jhbmsg
VS5BLjEaMBgGA1UECxMRUGF5bWVudHMgU29sdXRpb24xHjAcBgNVBAMTFXB0cGkt
YWNwdC5yYWJvYmFuay5ubDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
```

* CSR Details

```
Certificate Request:
  Data:
    Version: 0 (0x0)
    Subject: C=NL, ST=Utrecht, L=Utrecht, O=Cooperatieve Rabobank U.A., OU=Payments Solution, CN=[redacted]
    Subject Public Key Info:
```

* Validation

```
Warning: Organizational Unit is deprecated and will not be applied to the certificate in the future to comply with Industry standards.
```



* Requestor email	[redacted]
* Internal / External Certificate	Internal
* Templates	TLS certificate with client authentication
* Application CI	
* CI Identifier Manual Entry	

* Upload CSR

```
DgYDVQQHEwdVdHJlY2h0MSMwIQYDVQQKExpDb29wZXJhdGlldmUgUmFib2Jhbmsg
VS5BLjEVMBMGA1UECxMMSVQgTmVkZXJsYW5kMS0wKwYDVQQDEyRpbnRlZ3JhdGlv
bi10ZXN0LmJyaWRnZXMucmFib2JhbmsubmwwggEiMA0GCSqGSIb3DQEBAQUAA4IB
```

Confirmation

Are you sure you want to Submit?

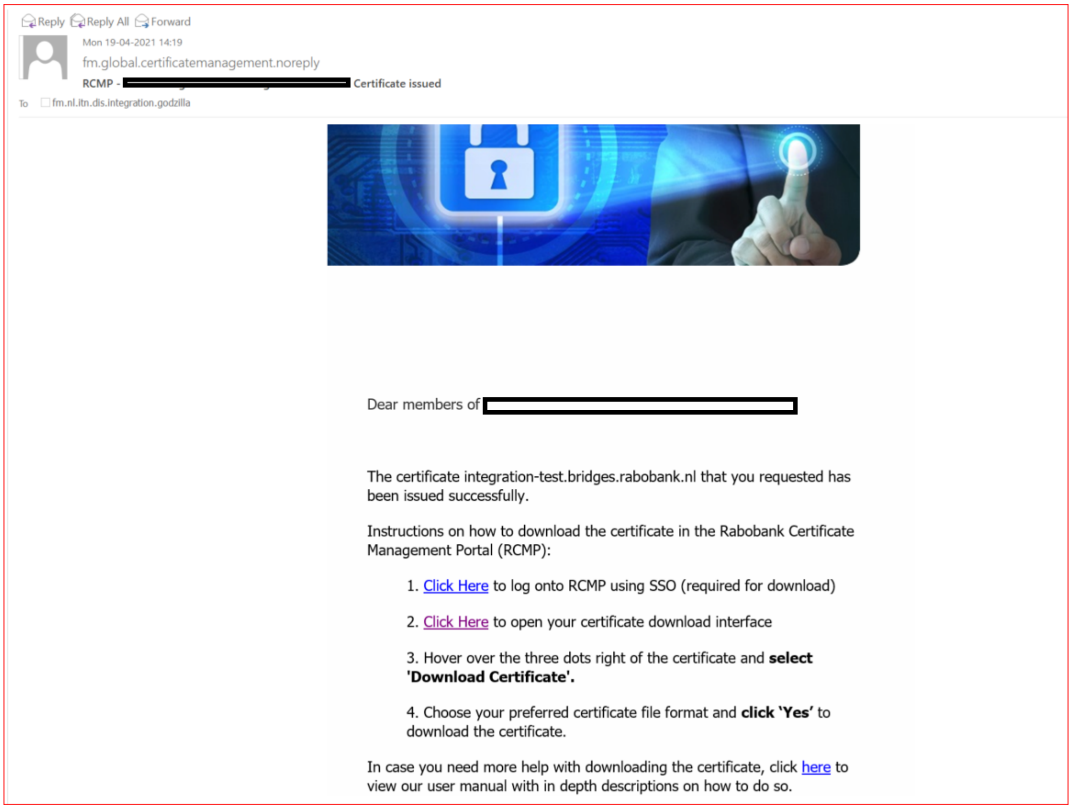
* CSR Details

```
  Data:
    Version: 0 (0x0)
    Subject: C=NL, ST=Utrecht, L=Utrecht, O=Cooperatieve Rabobank U.A., OU=IT Nederland, CN=[redacted]
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
```

* Validation

```
Success.
```

4. In time (can be as fast as 1 minute) you will receive the link to the signed certificate in your functional mailbox.



Mon 19-04-2021 14:19

fm.global.certificatemanagement.noreply

RCMP - [redacted] Certificate issued

To □ fm.nl.itn.dis.integration.godzilla

Dear members of [redacted]

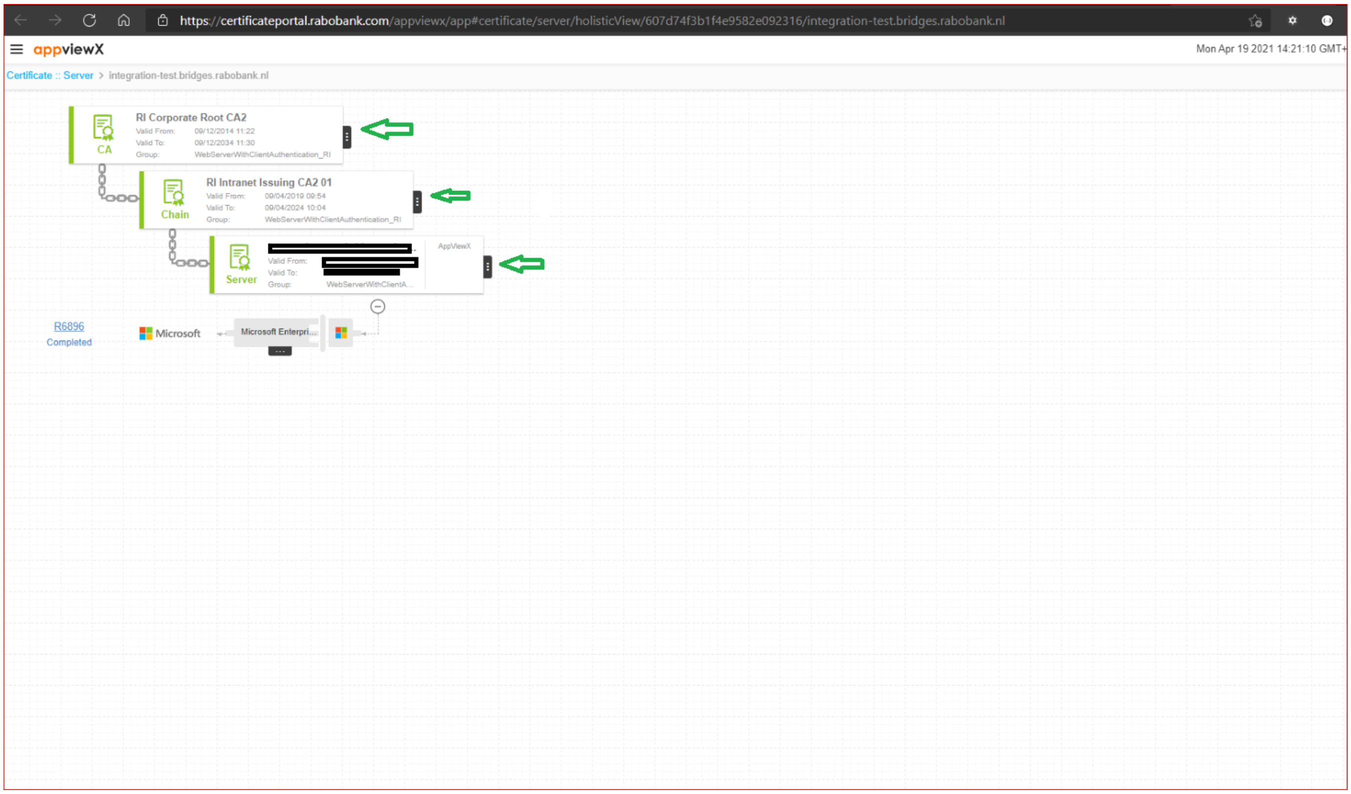
The certificate integration-test.bridges.rabobank.nl that you requested has been issued successfully.

Instructions on how to download the certificate in the Rabobank Certificate Management Portal (RCMP):

1. Click Here to log onto RCMP using SSO (required for download)
2. Click Here to open your certificate download interface
3. Hover over the three dots right of the certificate and **select 'Download Certificate'.**
4. Choose your preferred certificate file format and **click 'Yes'** to download the certificate.

In case you need more help with downloading the certificate, click here to view our user manual with in depth descriptions on how to do so.

Download all three certificates choose **PEM(*.pem) format**



https://certificateportal.rabobank.com/appviewx/app#certificate/server/holisticView/607d74f3b1f4e9582e092316/integration-test.bridges.rabobank.nl

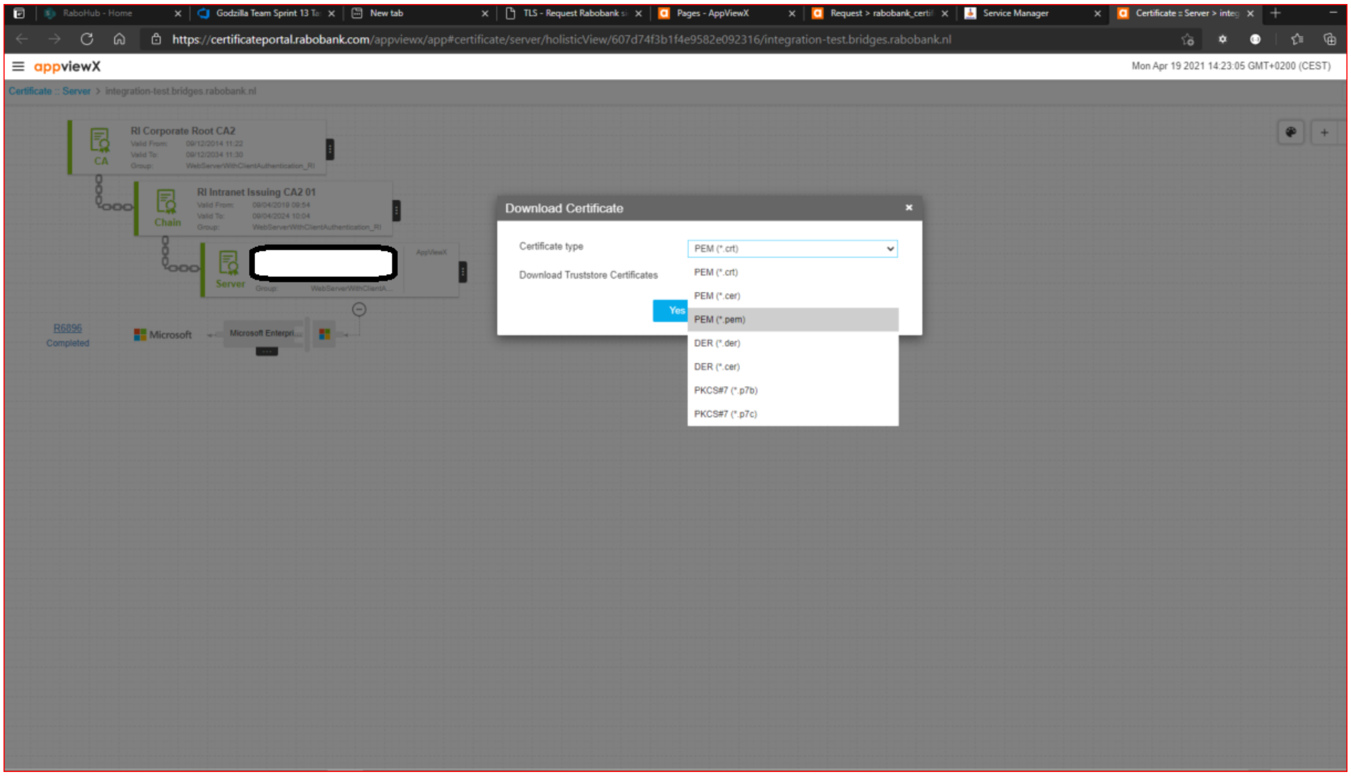
Certificate :: Server > integration-test.bridges.rabobank.nl

CA
RI Corporate Root CA2
Valid From: 09/12/2014 11:22
Valid To: 09/12/2034 11:30
Group: WebServerWithClientAuthentication_RI

Chain
RI Intranet Issuing CA2 01
Valid From: 09/04/2019 09:54
Valid To: 09/04/2024 10:04
Group: WebServerWithClientAuthentication_RI

Server
[redacted]
Valid From: [redacted]
Valid To: [redacted]
Group: WebServerWithClientA...
AppViewX

R6896
Completed



https://certificateportal.rabobank.com/appviewx/app#certificate/server/holisticView/607d74f3b1f4e9582e092316/integration-test.bridges.rabobank.nl

Mon Apr 19 2021 14:23:05 GMT+0200 (CEST)

Certificate :: Server > integration-test.bridges.rabobank.nl

RI Corporate Root CA2
Valid From: 09/12/2014 11:22
Valid To: 09/12/2034 11:30
Group: WebServerWithClientAuthentication_RI

RI Intranet Issuing CA2 01
Valid From: 09/04/2019 09:54
Valid To: 09/04/2024 10:04
Group: WebServerWithClientAuthentication_RI

[redacted]
Group: WebServerWithClientA...

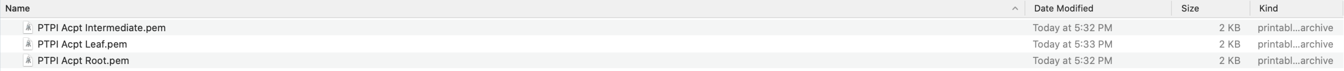
R6896
Completed

Download Certificate

Certificate type: PEM (*.crt)

Download Truststore Certificates

Download and rename all 3 certificates in one folder and navigate to the download certificates folder. Below is the Directory structure post downloaded.



Name	Date Modified	Size	Kind
PTPI Acpt Intermediate.pem	Today at 5:32 PM	2 KB	printabl...archive
PTPI Acpt Leaf.pem	Today at 5:33 PM	2 KB	printabl...archive
PTPI Acpt Root.pem	Today at 5:32 PM	2 KB	printabl...archive

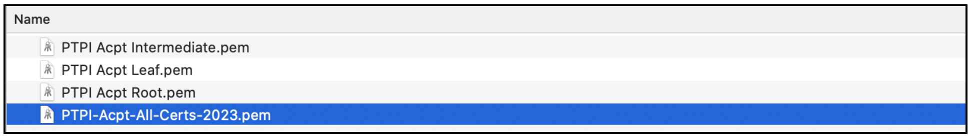
Note : We will be receiving all the Root ,Intermediate and Actual cert for each request we raise.

---

6. Changes specific to PTPI app :

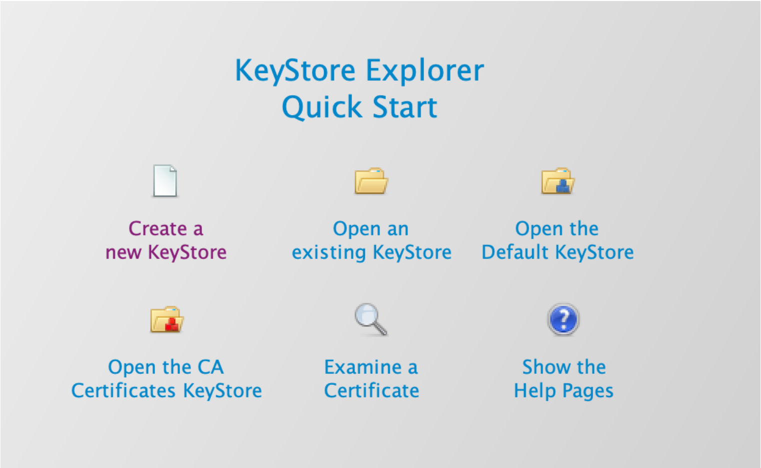
We have the certs ready from the Rabo Cert Portal . Now we have three things to do for PTPI:

a. Create a PEM file with all the three certs (root, intermediate, leaf). Drag and drop all the three cert files in TextMate app. All three certs will be displayed together, save the file as .pem

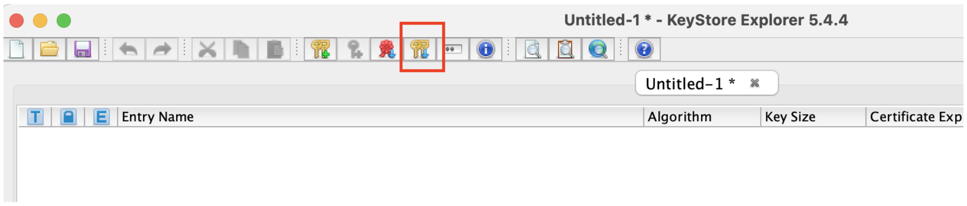


Name
PTPI Acpt Intermediate.pem
PTPI Acpt Leaf.pem
PTPI Acpt Root.pem
PTPI-Acpt-All-Certs-2023.pem

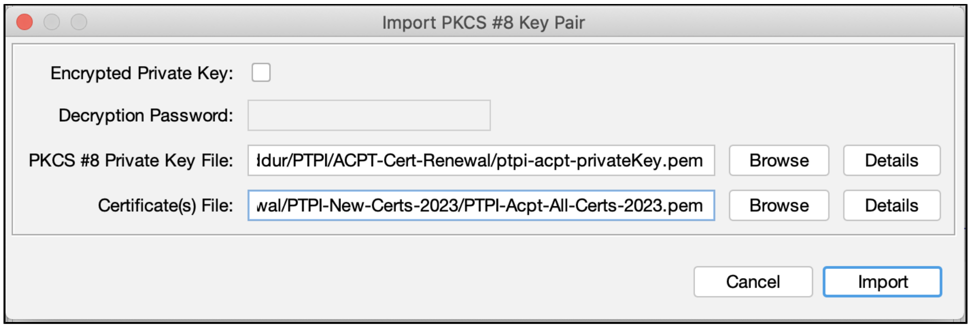
b. Now we have to create a new Keystore file using the pem which we created. To do this, follow the below steps,
   i. Open the Keystore Explorer app. Click on Create a new Keystore from the screen shown below



ii. Select JKS from the type pop up
iii. Click on Import Key Pair option



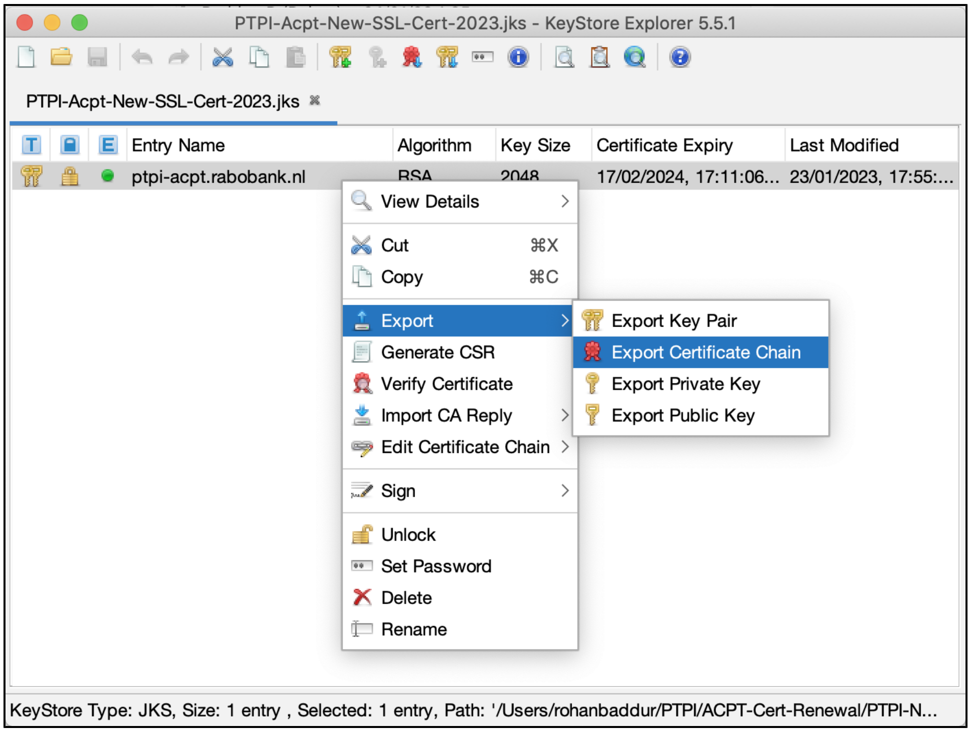
iv. Choose PKCS #8 in Import Key pair type pop up and click on OK.
v. Disable the Encrypted Private Key text box. Browse the path of the private key which we exported in step 4 section c and the certificate (PEM file with all 3 combined certificate) which we created in step 6 section a.
vi. Click on import.



Encrypted Private Key: □
Decryption Password:
PKCS #8 Private Key File: ldur/PTPI/ACPT-Cert-Renewal/ptpi-acpt-privateKey.pem
Certificate(s) File: wal/PTPI-New-Certs-2023/PTPI-Acpt-All-Certs-2023.pem

vii. Give the alias name and enter the password for the JKS file.
viii. The keystore will be imported successfully and will be opened in the Keystore Explorer app.
ix. Click on SAVE to save the keystore file.

c. Update the truststore with newly created SSL cert. To do this, follow the below steps,
  i. Export the newly created SSL cert in .cer format as shown below

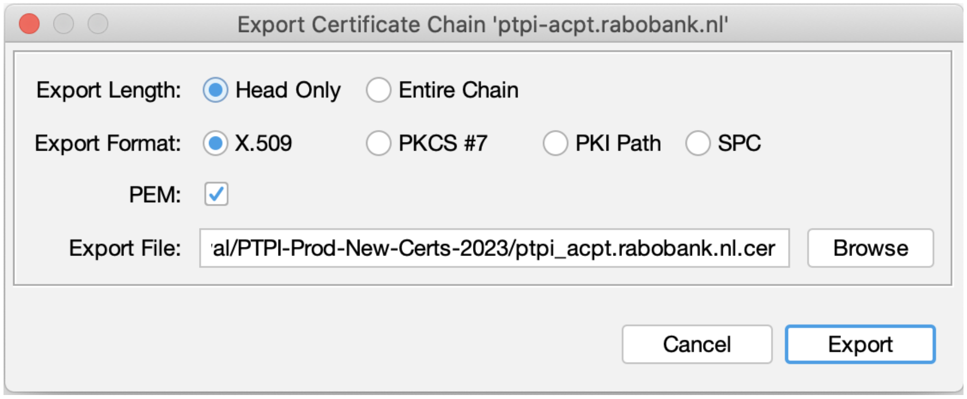
ii. 

PTPI-Acpt-New-SSL-Cert-2023.jks - KeyStore Explorer 5.5.1

PTPI-Acpt-New-SSL-Cert-2023.jks

T	🔒	E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
		●	ptpi-acpt.rabobank.nl	RSA	2048	17/02/2024, 17:11:06...	23/01/2023, 17:55:...

KeyStore Type: JKS, Size: 1 entry , Selected: 1 entry, Path: '/Users/rohanbaddur/PTPI/ACPT-Cert-Renewal/PTPI-N...

iii. 

Export Certificate Chain 'ptpi-acpt.rabobank.nl'

Export Length: ● Head Only ○ Entire Chain

Export Format: ● X.509 ○ PKCS #7 ○ PKI Path ○ SPC

PEM: ☑

Export File: al/PTPI-Prod-New-Certs-2023/ptpi_acpt.rabobank.nl.cer

iv. Import this certificate in the truststore by replacing the existing one and save the truststore in jks format.

7. Update the certs in JSON file of PTPI-Credhub :

1. visit base64Convertor . Use the option "**File to Base64**". Upload the keystore file of SSL cert generated in above step.

2. Copy the encoded content and format it using any text editor. You can also use Yaml_Formatter to format the content.

3. Update the content in the json file of PTPI-Credhub and save it.

4. Visit again to base64Convertor. Use the option "**File to Base64**". Upload the keystore file of truststore generated in above step.

5. Copy the encoded content and format it using any text editor. You can also use Yaml_Formatter to format the content.

6. Update the content in the json file of PTPI-Credhub and save it.

7. Configure the new json of PTPI-Credhub in CF.

8. Restage the applications and test the flow.