

**IRCC Entrust certificate procedures for AWS cloud**

REVISION STATUS SHEET

| Document No. | Date | Changed by | Status/Comments |
| --- | --- | --- | --- |
|  | October 13th, 2020 | Marc Bélanger | First draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

[1. CSR File generation 1](#_Toc54597015)

[1.1 Generate Password 1](#_Toc54597016)

[1.2 Access KeePass tool 1](#_Toc54597017)

[1.3 Update KeePass with cert details/password 2](#_Toc54597020)

[1.4 Create Keystore (.JKS File) 2](#_Toc54597021)

[1.5 Generate and Export CSR file 3](#_Toc54597025)

[2. Installation of the certificate 4](#_Toc54597030)

[2.1 Reception of the certificate 4](#_Toc54597031)

[2.2 Download certificate 4](#_Toc54597032)

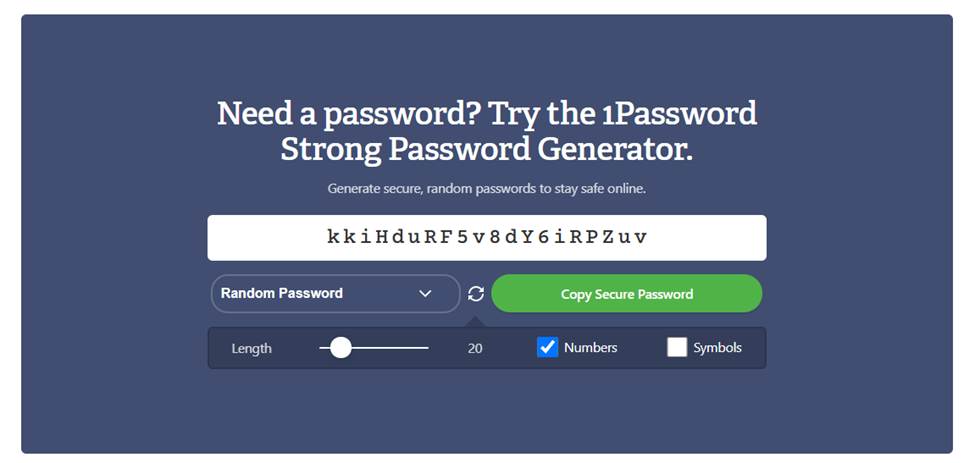
[2.3 Install the certificate 6](#_Toc54597038)

# CSR File generation

## Generate Password

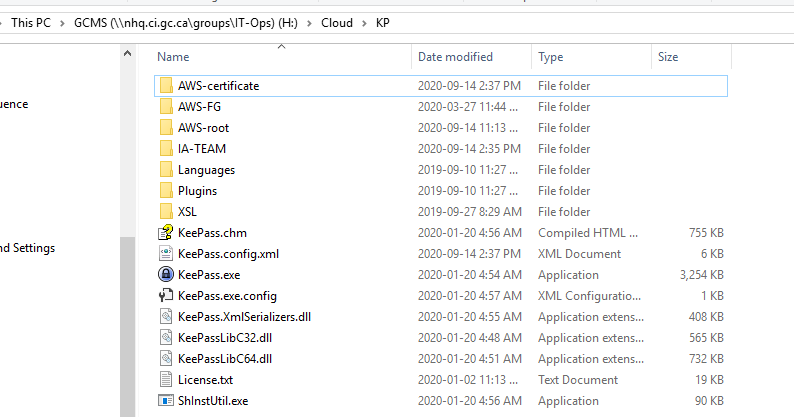
Access website the following website to choose a password:

[**https://1password.com/password-generator/**](https://1password.com/password-generator/)

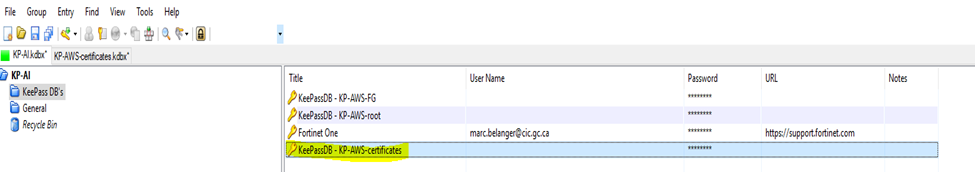


## Access KeePass tool

### Launch KeePass.exe and open file KP-AI.kdbx under H:\Cloud\KP\IA-TEAM

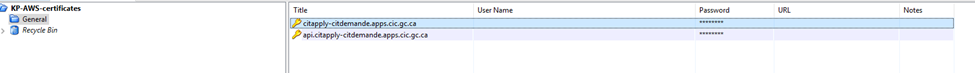


### Copy password from KeePassDB-KP-AWS-certificates and open file KP-AWS-certificates.kdbx under H:\Cloud\KP\AWS-certificate



## Update KeePass with cert details/password

Create a new entry under KeePassDB-KP-AWS-certificates using the DNS alias name and store the generated password in step 1) into it.



## Create Keystore (.JKS File)

### Log in with your APPs account (admin.firstname.lastname) and password to NJES1S7618 and start a Command Prompt session

### Point to D: drive and change directory to D:\Java\jdk8\_64\bin

### Commands to generate keystore:

No SAN:

keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore **[alias]**.jks

With SAN:

keytool -genkey -alias server -keyalg RSA -keysize 2048 -ext san=dns:**[SAN 1]**,dns:**[SAN 2]** -keystore **[alias]**.jks

N.B.: SAN – or Subject Alternative Name is used when we have multiple DNS Aliases with the same certificate.

Examples:

D:\Java\jdk8\_64\bin>keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore citapply-citdemande.apps.cic.gc.ca.jks

D:\Java\jdk8\_64\bin>keytool -genkey -alias server -keyalg RSA -sigalg SHA256withRSA -keysize 2048 -ext san=dns:citapply-citdemande.apps.cic.gc.ca,dns:api.citapply-citdemande.apps.ci

c.gc.ca -keystore citapply-citdemande-dev.apps.cic.gc.ca.jks

Enter keystore password: Password from the KeePass DB KP-AWS-certificates

Re-enter new password:

What is your first and last name? (DNS)

[Unknown]: ***citapply-citdemande.apps.cic.gc.ca***

What is the name of your organizational unit? (IRCC Branch)

[Unknown]: ***DSB***

What is the name of your organization?

[Unknown]: ***IRCC***

What is the name of your City or Locality?

[Unknown]: ***Ottawa***

What is the name of your State or Province?

[Unknown]: ***ON***

What is the two-letter country code for this unit?

[Unknown]: ***CA***

Is CN=citapply-citdemande.apps.cic.gc.ca, OU=DSB, O=IRCC, L=Ottawa, ST=ON, C=CA

correct?

[no]: ***yes***

Enter key password for <server>

(RETURN if same as keystore password): Password from the KeePass DB KP-AWS-certificates

Re-enter new password:

## Generate and Export CSR file

### Command to generate CSR file:

keytool -certreq -alias server -keystore [alias].jks -file [alias].csr

Example:

D:\Java\jdk8\_64\bin>keytool -certreq -alias server -keystore citapply-citdemande.apps.cic.gc.ca.jks -file citapply-citdemande.apps.cic.gc.ca.csr

Enter keystore password: Password from the KeePass DB KP-AWS-certificates

### Copy the CSR file to your workstation and attach to TFS ticket.

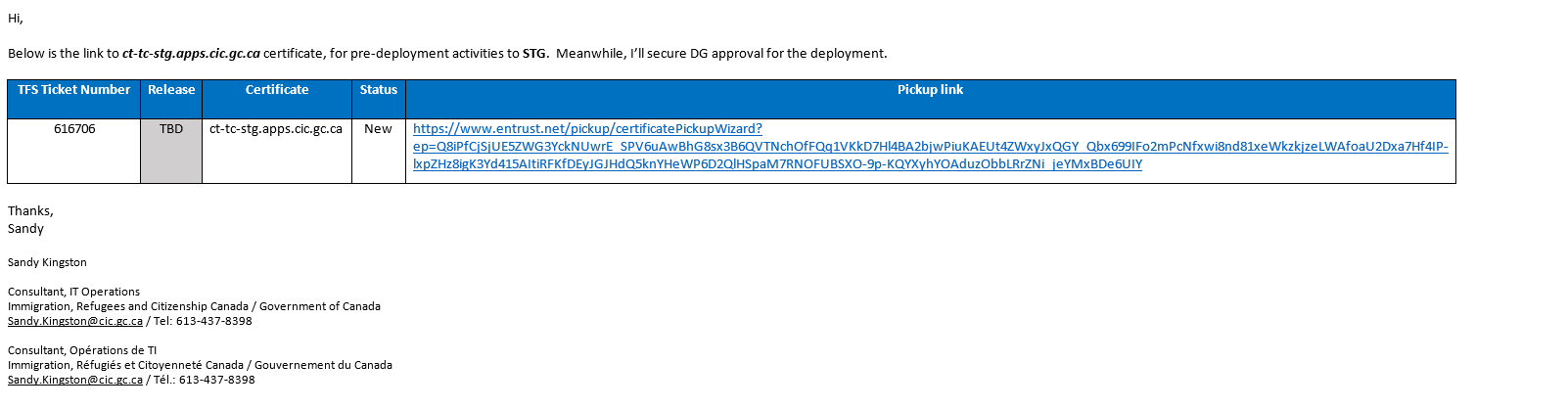
### Assign TFS ticket to Sandy/Release Management. Release Management will send certificate request to SSC.

### Cut the .jks and .csr files and paste them under a new folder under D:\Cloudcerts on server NJES1S7618.

# Installation of the certificate

## Reception of the certificate

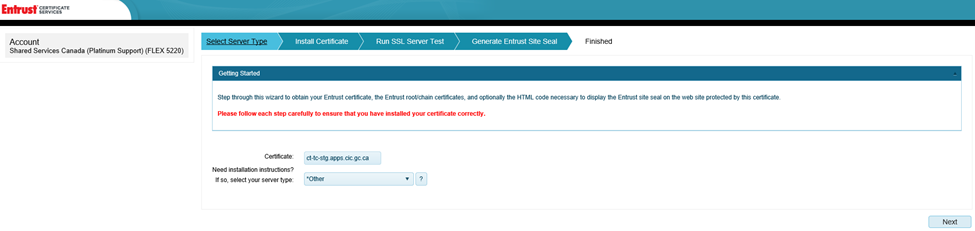
Release Management send an Entrust link to the requestor



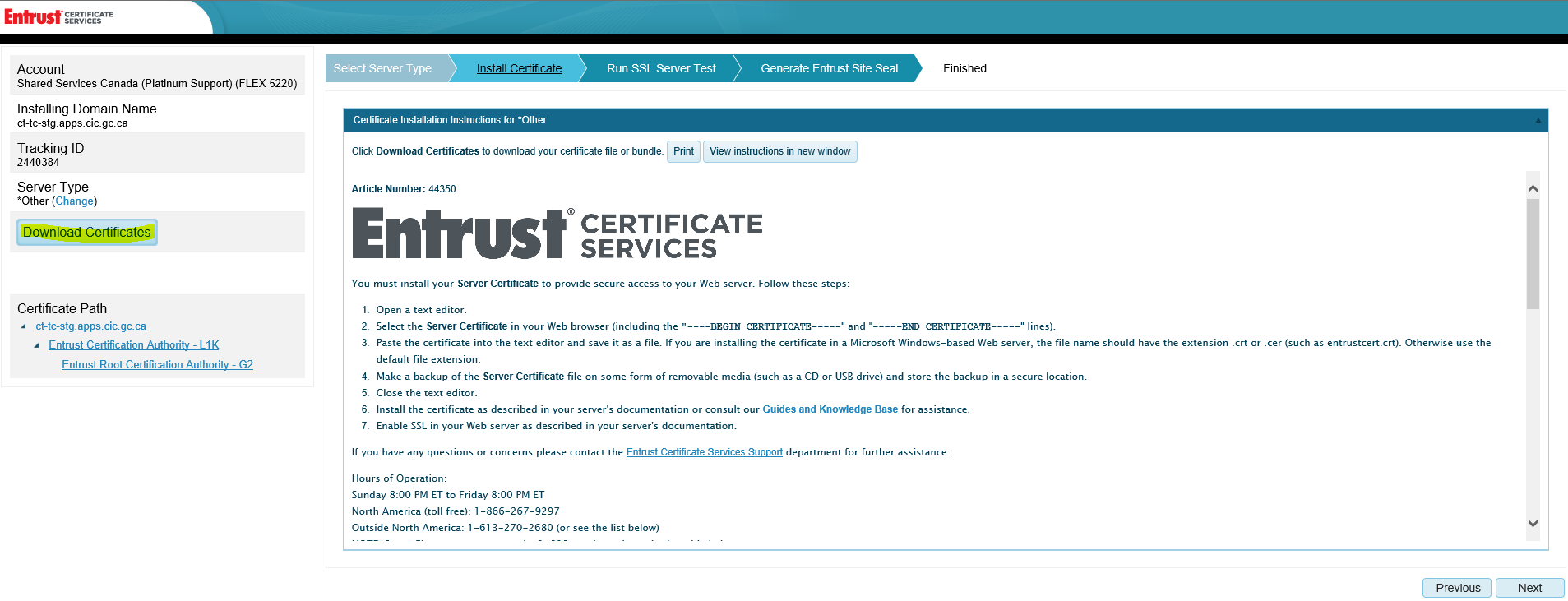
## Download certificate

### Requestor download Certificate from Entrust Site

Click ‘Next’

****

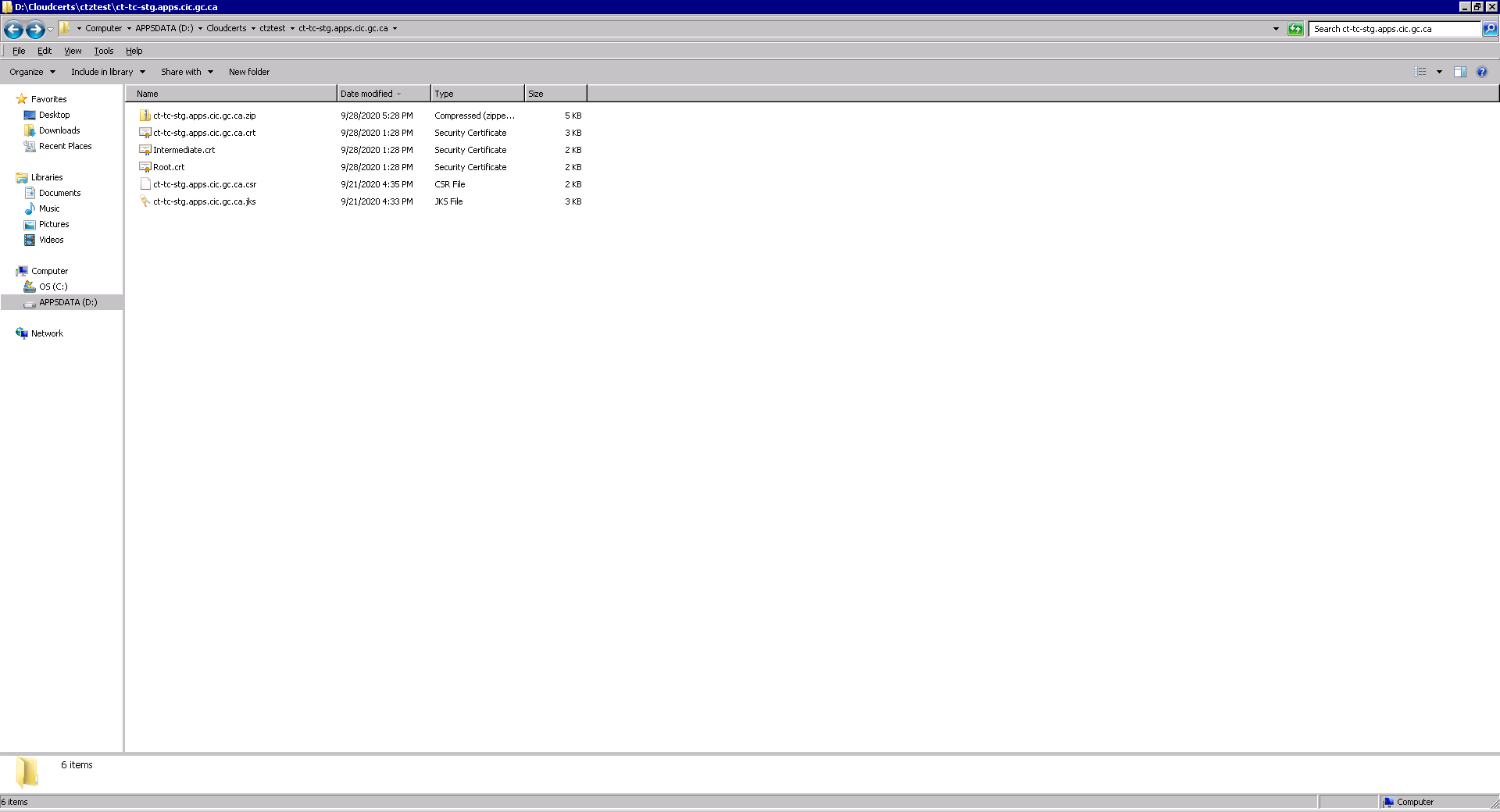
### Click ‘Download’ and copy the zip file under D:\Cloudcerts on server NJES1S7618.



### Rename zip file to [alias].zip

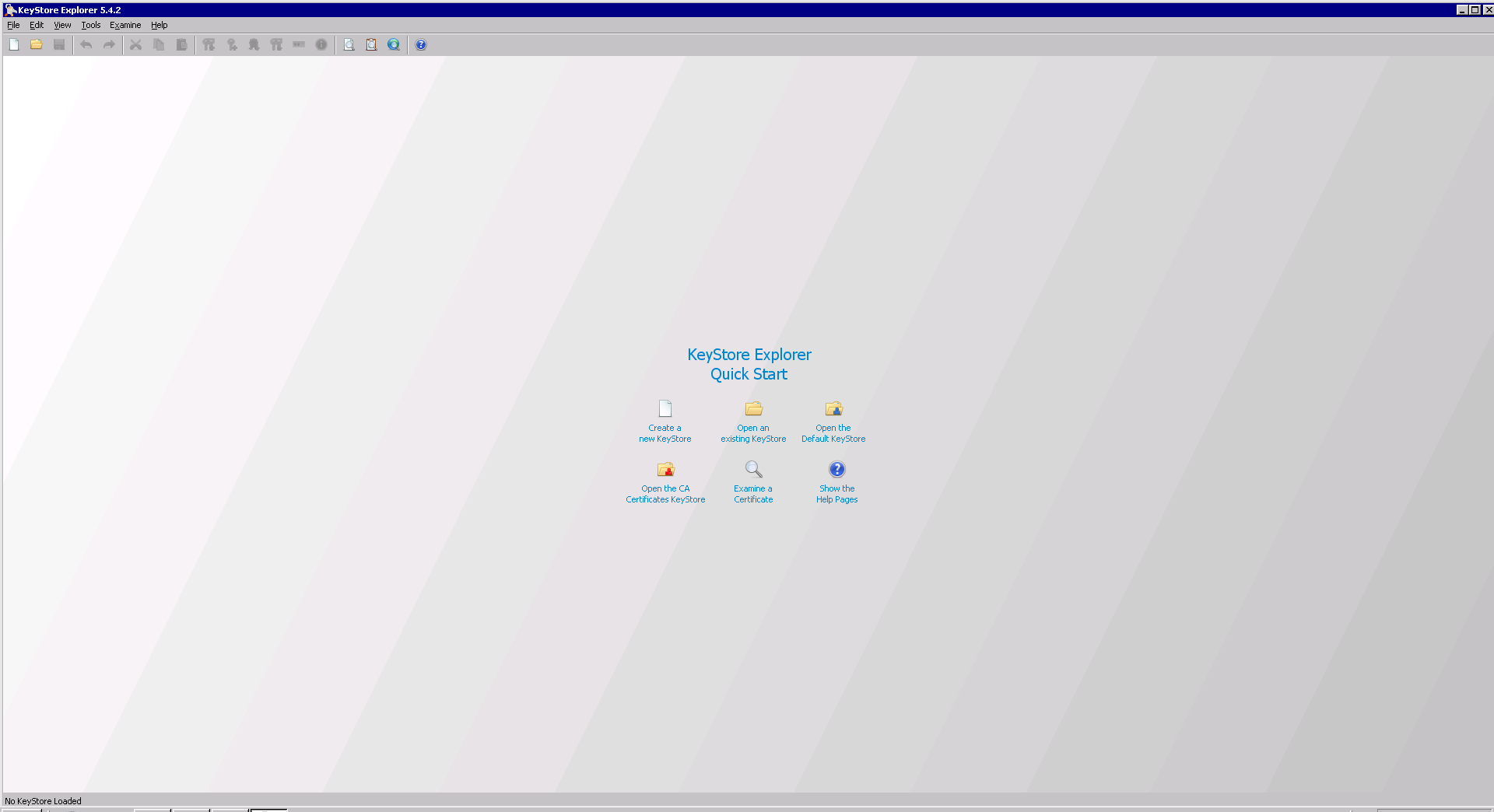
### Unzip the [alias].zip file

### Rename ServerCertificate.crt file to [alias].crt



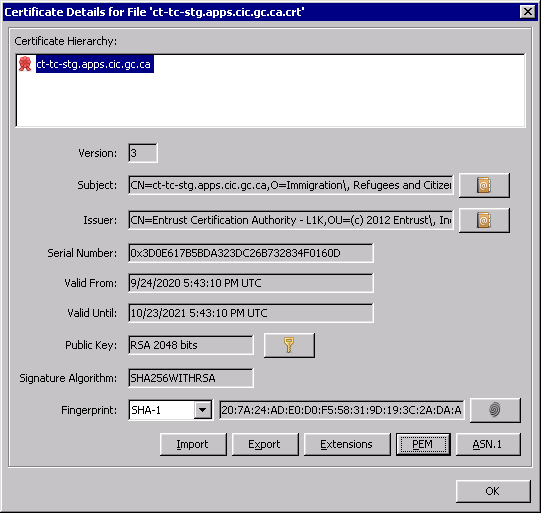
## Install the certificate

### Open the KeyStore Explorer tool and select ‘Examine a Certificate’

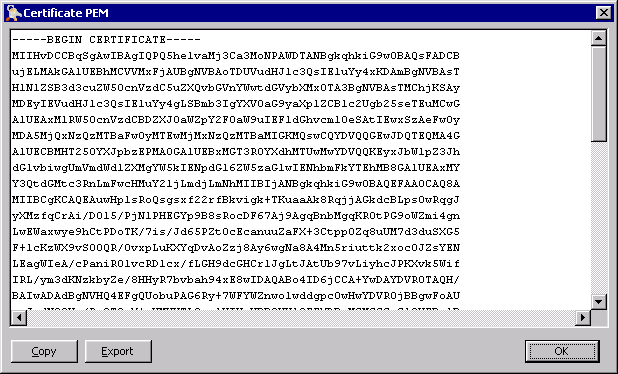


### Select the [alias].crt certificate

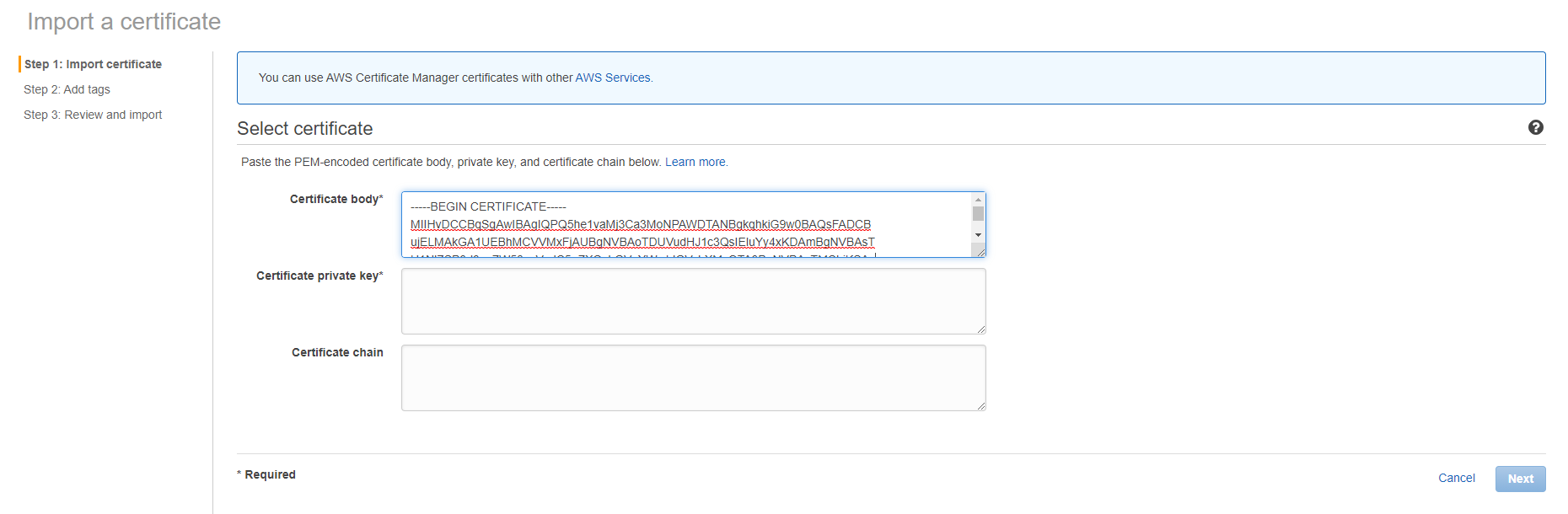
### To be able to import the certificate in AWS, it has to be converted to the PEM format.



### Click on the ‘PEM’ and copy the content.

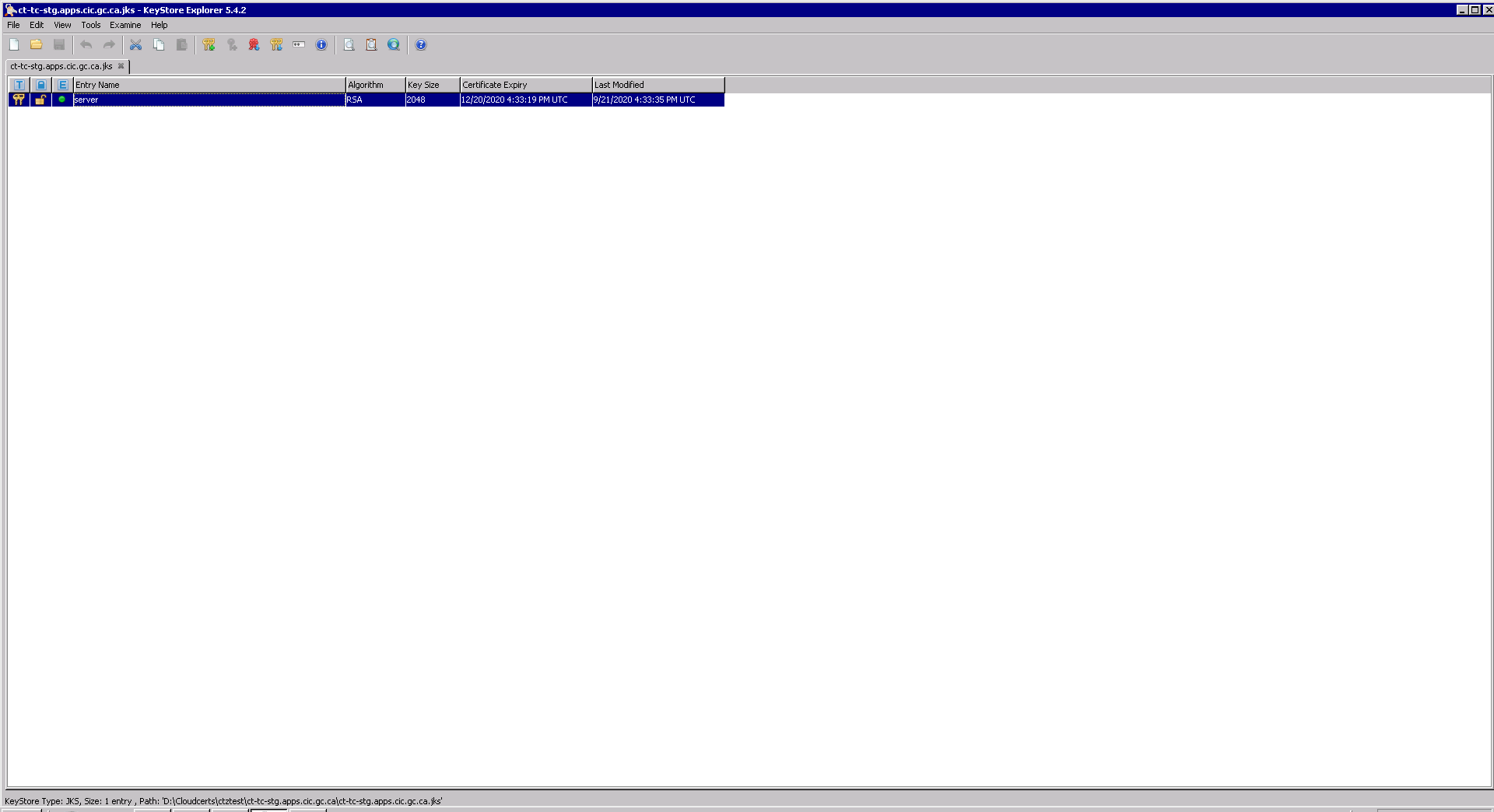


### Paste it into AWS (Certificate Manager Service)



### Repeat the process for the private key, you need to extract it from the JKS file. Open the JKS file. You will be prompted for password. Use the one stored in KeePass.

### Right click and select View Details, and then Private Key Details



### Click on the ‘PEM’ and copy the content.

### Paste it into AWS (Certificate Manager Service)

### For the certificate chain, use NotePad

The certificates must be concatenated in order so that each directly certifies the one preceding, that is:

-----BEGIN CERTIFICATE-----

*Server cert*

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

*Int cert*

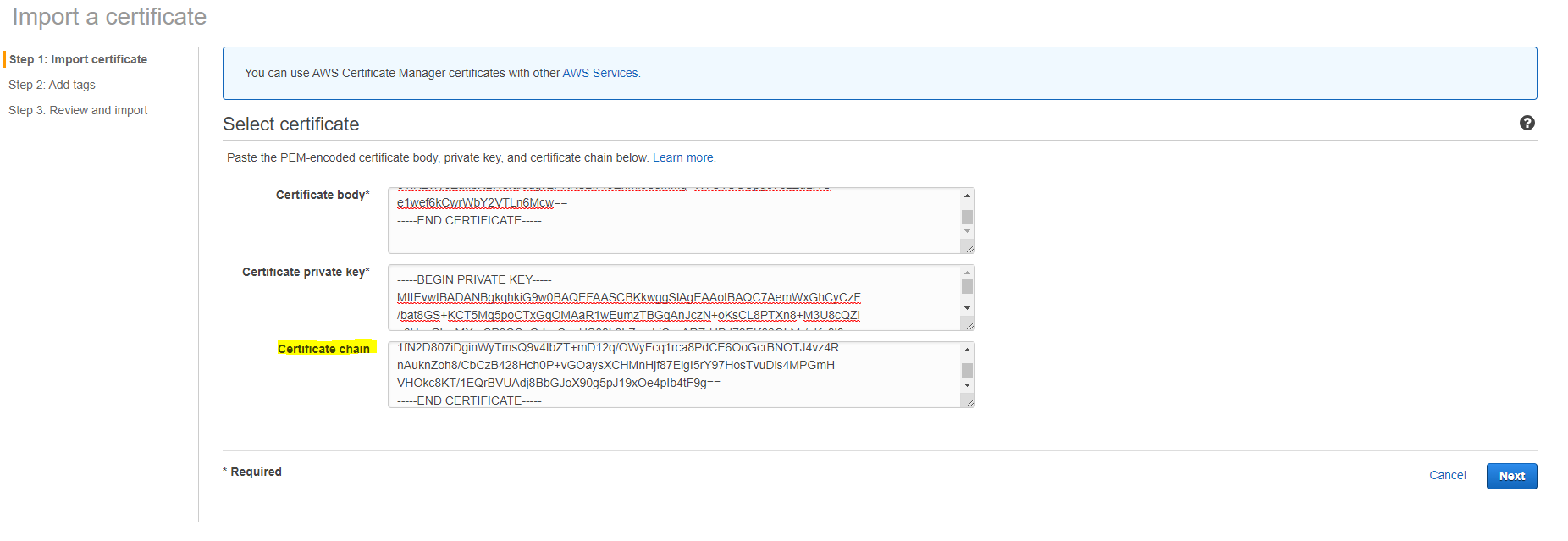
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

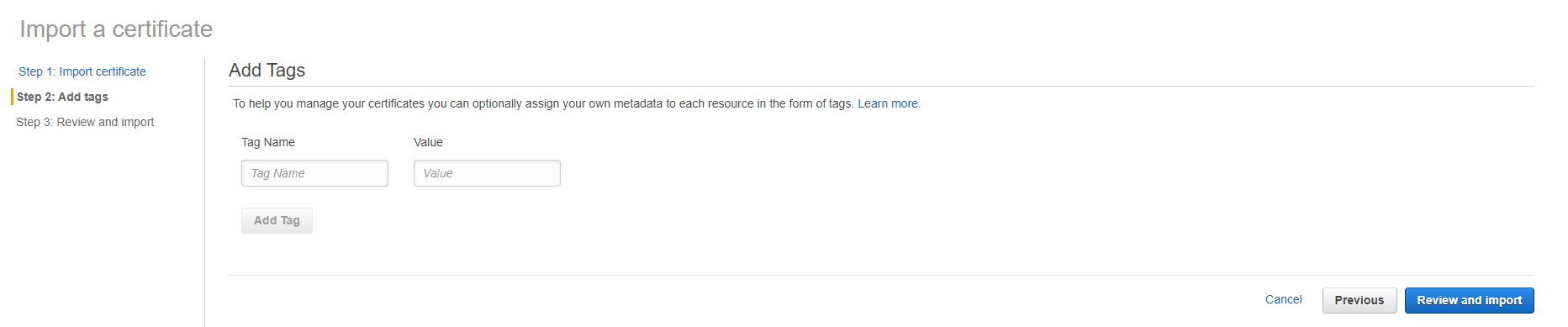
*Root cert*

-----END CERTIFICATE-----

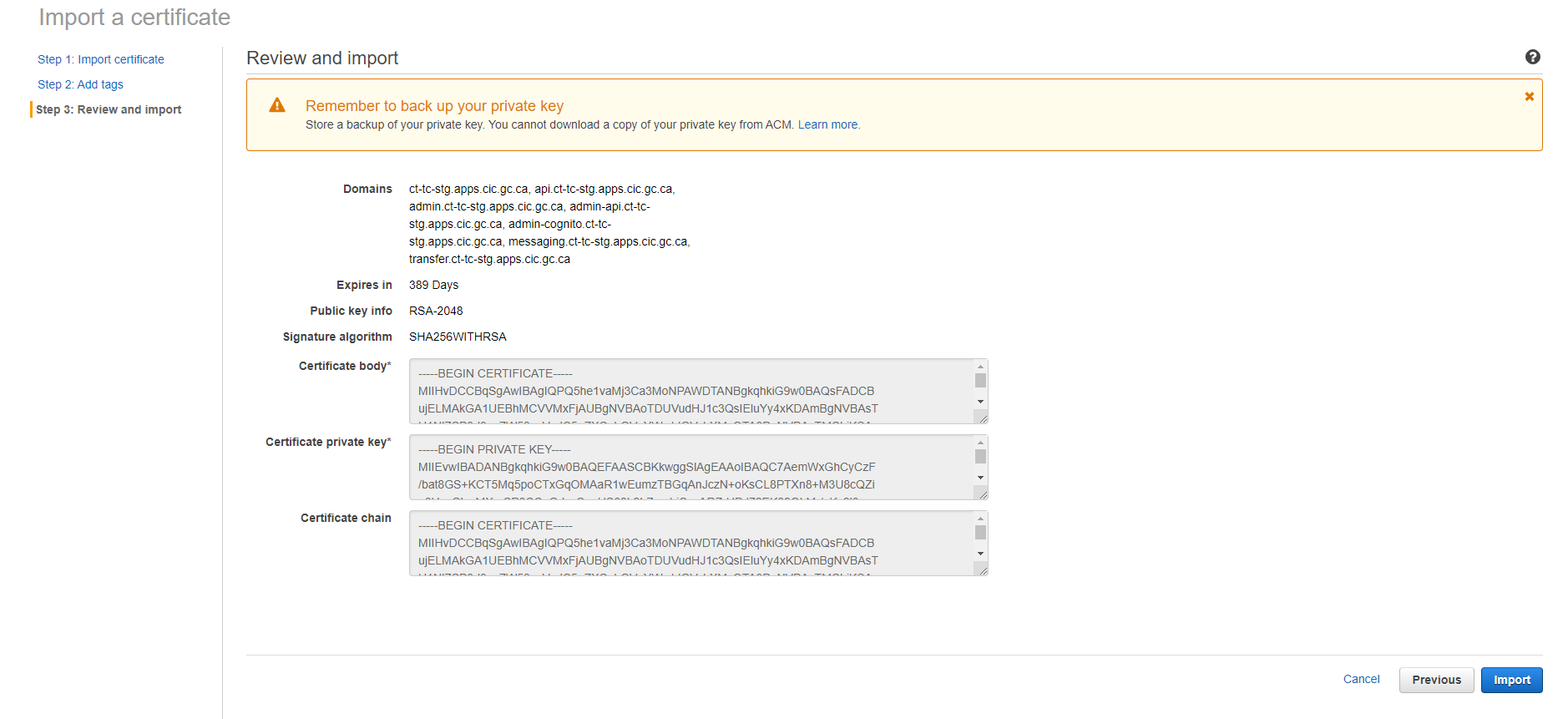
1. Select the [alias].crt certificate. Click on the ‘PEM’ and copy the content in NotePad.
2. Select the Intermediate.crt certificate. Click on the ‘PEM’ and copy the content in NotePad.
3. Select the Root.crt certificate. Click on the ‘PEM’ and copy the content in NotePad.
4. Copy the whole content of the NotePad, and paste it in AWS
5. Click Next



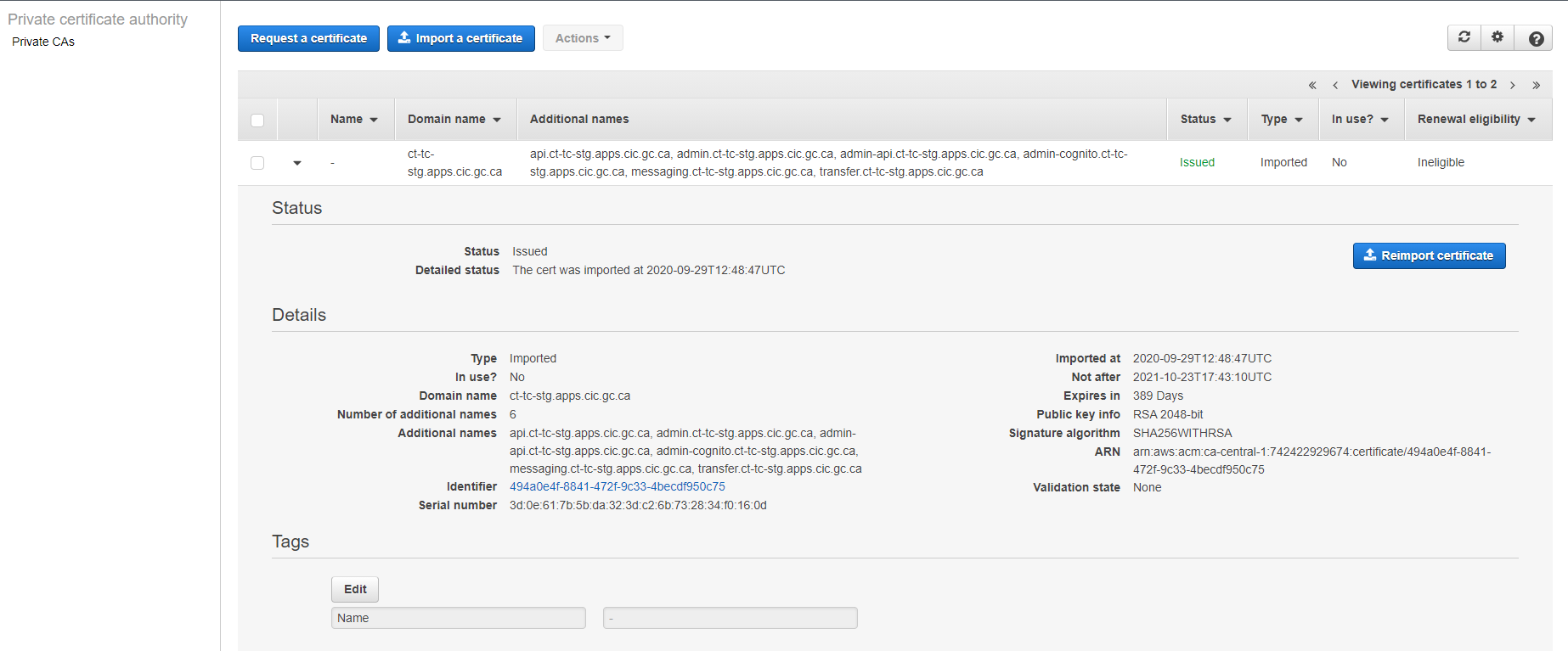
1. Click Review and import



1. Click Import



Result



N.B.

Keep in mind that if you’re importing these certificates for usage with a Global CloudFront distribution you will need to add them in the US-EAST-1 (N. Virginia) region. AWS uses this region for a number of Global services. If the team is also using these certs with the APIGW you will also need to import the certs in the CA-CENTRAL-1 region.