Certificates Used in ACE-Platform

Advanced Conversational Engagement

Exported on 06/06/2025

Table of Contents

In ACE Platform we use 3 different certificates as below

- Infra CA G3 certificate (self-signed)
- Chained Certificate (Signed by trusted CA)
- Root Certificate

Infra CA G3 certificate:

We use Infra CA G3 certificate for

- Ingress in AKS
- To connect to other third-party applications by third-party service application used by Integration team
- Private Appgw certificates used for Advisor Assist

Procedure to deploy Infra CA G3 certificate:

There are 2 methods to deploy Infra CA G3 certificate:

1. Manually
2. Through Release Pipeline
3. Through Automated Pipeline

Steps to create Infra CA G3 certificate manually:

1 Required tools

- OpenSsl[1]
- KeyStore[2]
- Bash

[1] https://www.openssl.org/

[2] https://keystore-explorer.org/

2 Steps to create SSL certificate

2.1 Config file with SAN

For the current project, approach to connect to the services is through alternate names on the same certificate. That is the Common Name (CN) says the same `ace-<env>.nl.eu.abnamro.com`[3]

Subject Alternate Names (SAN) values are provided during the certificate generation.

Create a supporting config file with required parameters:

```
 ## input config file
## filename: ace-csr-config.txt

default_bits       = 2048 # may also be 4096
distinguished_name = req_distinguished_name
req_extensions    = req_ext
prompt = no
[ req_distinguished_name ]
countryName                 = NL
stateOrProvinceName         = Noord-Holland
organizationName            = ABN AMRO Bank N.V.
commonName                  = ace-d.nl.eu.abnamro.com
[ req_ext ]
subjectAltName = @alt_names
[alt_names]
DNS.1   = ace-d.nl.eu.abnamro.com
DNS.2   = pvt-dev-ace-d.nl.eu.abnamro.com
DNS.3   = labelstudio-ace-d.nl.eu.abnamro.com
DNS.4   = botstudio-ace-d.nl.eu.abnamro.com
DNS.5   = ml-model-simple-1-ace-d.nl.eu.abnamro.com
DNS.6   = botium-anna-ace-d.nl.eu.abnamro.com
DNS.7   = conversation-selector-ace-d.nl.eu.abnamro.com
DNS.8   = autolabelling-1-ace-d.nl.eu.abnamro.com
DNS.9   = airflow.ace-d-nl.eu.abnamro.com
DNS.10  = airflow-test-ace-d.nl.eu.abnamro.com
```

[3] http://nl.eu.abnamro.com

```
DNS.11  = airflow-annacb-ace-d.nl.eu.abnamro.com
DNS.12  = hasura-ace-d.nl.eu.abnamro.com
DNS.13  = temporal-ace-d.nl.eu.abnamro.com
DNS.14  = ace-be-fe-d.nl.eu.abnamro.com
```

2.2 CSR file using Config

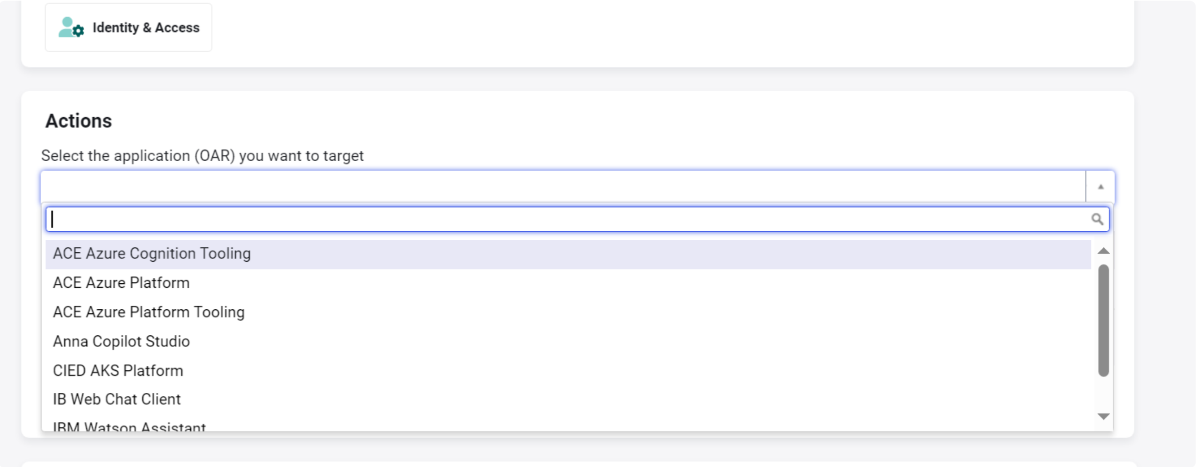
Now that we have the config, using openssl, generate `*.csr` file along with the private key in pem format `key.pem`.

Use the following to generate the certificate (`ace.csr`) with private key (`ace-key.pem`):

```
openssl req -out ace.csr -newkey rsa:2048 -nodes -keyout ace-key.pem -config ace-csr-config.txt
```

2.3 Upload the CSR

- Browse Security services from MYIT (IT Security Services (CISO) - MyIT Portal (service-now.com)[4]) to select the Block and OAR. In our case it is ACE Azure Platform



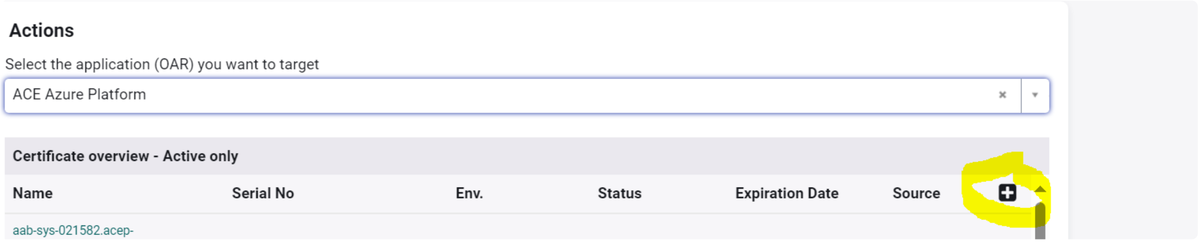
Actions

Select the application (OAR) you want to target

ACE Azure Cognition Tooling
ACE Azure Platform
ACE Azure Platform Tooling
Anna Copilot Studio
CIED AKS Platform
IB Web Chat Client
IBM Watson Assistant

- Once you choose the OAR you will get the list of created certificates under the specific OAR
- To request new Certificate you have to click on plus icon as below and select **New Digital Certificate**

[4] https://aabsiampr.service-now.com/esc?id=emp_taxonomy_topic_rff&topic_id=21f0f7761b93ddd0ee0ca68ee54bcb7c

- 

  Actions

  Select the application (OAR) you want to target

  ACE Azure Platform

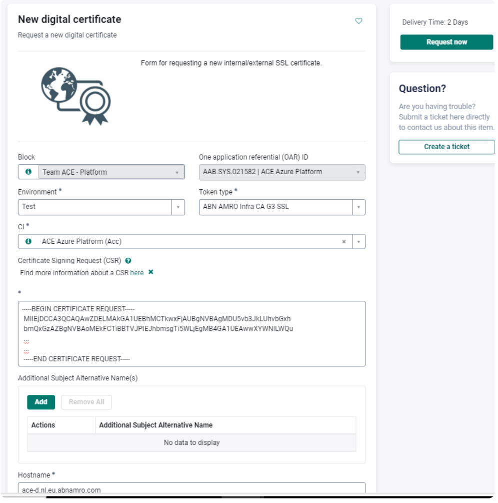
  Certificate overview - Active only

Name	Serial No	Env.	Status	Expiration Date	Source
aab-sys-021582.acep-					

- Open `.csr` in a text editor and copy the content (exclude the empty line at the end of the file). Content starts and ends as below

```
 -----BEGIN CERTIFICATE REQUEST-----
MIIEjDCCA3QCAQAwZDELMAkGA1UEBhMCTkwxFjAUBgNVBAgMDU5vb3JkLUhvbGxh
bmQxGzAZBgNVBAoMEkFCTiBBTVJPIEJhbmsgTi5WLjEgMB4GA1UEAwwXYWNlLWQu
...
...
-----END CERTIFICATE REQUEST-----
```

- Redirected to upload the certificate, fill the form and select **Order Now**



New digital certificate

Request a new digital certificate

Form for requesting a new internal/external SSL certificate.

Block: Team ACE - Platform

One application referential (OAR) ID: AAB.SYS.021582 | ACE Azure Platform

Environment *: Test

Token type *: ABN AMRO Infra CA G3 SSL

CI *: ACE Azure Platform (Acc)

Certificate Signing Request (CSR)

Find more information about a CSR here

```
-----BEGIN CERTIFICATE REQUEST-----
MIIEjDCCA3QCAQAwZDELMAkGA1UEBhMCTkwxFjAUBgNVBAgMDU5vb3JkLUhvbGxh
bmQxGzAZBgNVBAoMEkFCTiBBTVJPIEJhbmsgTi5WLjEgMB4GA1UEAwwXYWNlLWQu
...
...
-----END CERTIFICATE REQUEST-----
```

Additional Subject Alternative Name(s)

Actions	Additional Subject Alternative Name
No data to display	

Hostname *: ace-d.nl.eu.abnamro.com

Delivery Time: 2 Days

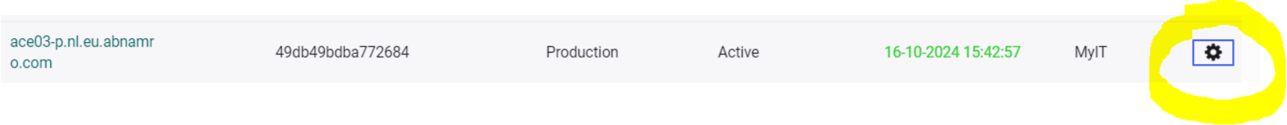
Question?

Are you having trouble? Submit a ticket here directly to contact us about this item.

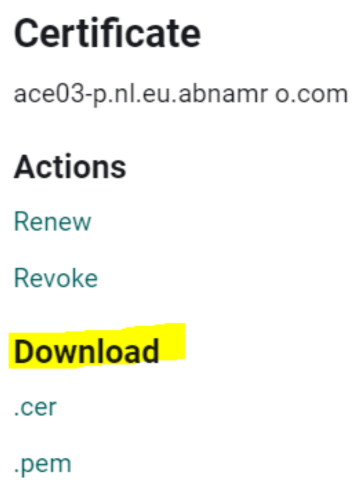
  - Common Name should match Hostname
  - Do not copy empty line at the end
- Upon ordering ServiceNow ticket is created it takes around 5mins to provision the certificate and to be visible in MYIT.

2.4 Convert OU Signed CER to PEM

As the process completes, the certificate should be available for download.Click on the settings icon as below to download the .cer or.pem file of the cert



ace03-p.nl.eu.abnamro.com	49db49bdba772684	Production	Active	16-10-2024 15:42:57	MyIT



Certificate

ace03-p.nl.eu.abnamr o.com

Actions

Renew

Revoke

Download

.cer

.pem

Download the `.pem`, resulting in `certificate.pem`

2.5 Upload certificate and Key to secure files

Upload both downloaded pem certificate and certificate key to secure files like below

2.6 Upload to Azure Key Vault

Using the stage : push_aks_certificate_kv from pre-infra-pipeline.yaml - Repos (azure.com)[5] deploy the certificate into KV and using

deploy_ingressTLS_certificate from post-aks-pipeline.yaml - Repos (azure.com)[6] create `ace-ingress-tls-secret` secret in AKS cluster

How to renew the aks ingress certificate:

- Use the config file aks cert of specific environment for which the cert is going to expire and generate CSR and private key using the below command

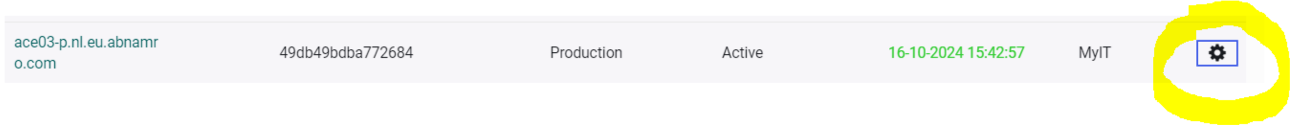
openssl req -out ace.csr -newkey rsa:2048 -nodes -keyout ace-key.pem -config ace-csr-config.txt

replace the values with your existing config file name

Navigate to myIT
Click on the settings icon of certificate which needs to be renewed as below

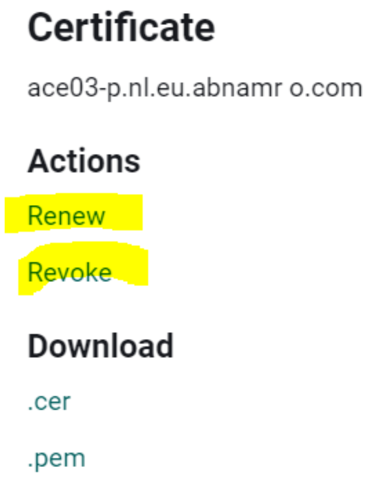
[5] https://dev.azure.com/cbsp-abnamro/GRD0001014/_git/acep-platform-infrastructure?path=/pipelines/pre-infra-pipeline.yaml&version=GBdevelop&_a=contents

[6] https://dev.azure.com/cbsp-abnamro/GRD0001014/_git/acep-platform-infrastructure?path=/pipelines/post-aks-pipeline.yaml&version=GBdevelop&_a=contents



ace03-p.nl.eu.abnamr o.com	49db49bdba772684	Production	Active	16-10-2024 15:42:57	MyIT	⚙

once you click on settings icon you should see two options RENEW OR REVOKE



Certificate

ace03-p.nl.eu.abnamr o.com

Actions

Renew

Revoke

Download

.cer

.pem

Click on Renew for renewal ,
it navigates to renewal page provide the above generated CSR in the CSR field

□

and click on request now

It takes around 5 mins for the renewed certificate to be visible in myit , once it is visible download the .pem file and upload the .pem and private key in secure files and to push the certificate to keyvault from secure files and download the certificate from keyvault and upload it into aks namespaces.

Once the pipeline is successful you can verify the latest certificate by hitting any of the SAN values of the certificate and checking the expiry as below

□

you should see renewed expiry date as per myIT

Note: Currently we are using Manual method to deploy ingress certificate

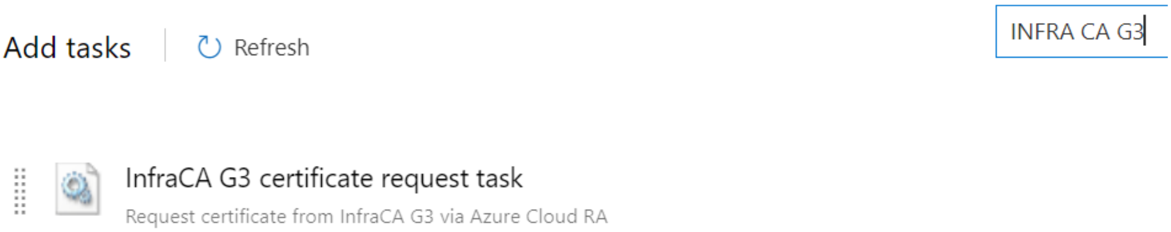
Through Release Pipeline:

To deploy the certificate using release navigate to Releases - Pipelines (azure.com)[7], the link takes you to the devops release pipeline where we have created release to deploy infra CA G3 certificate.

Click on edit release pipeline and choose the environment displayed on the stage to which env you want to create the Cert

- After you open the stage click on plus symbol on the agent job to add the required task
- Search for Infra CA G3 and select the task

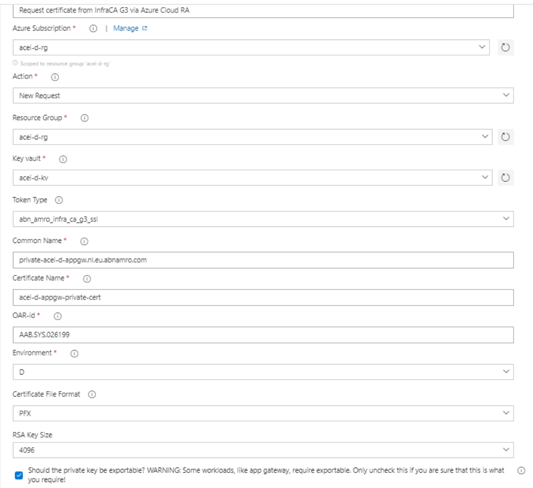
[7] https://dev.azure.com/cbsp-abnamro/GRD0001014/_release?_a=releases&view=all&definitionId=915



InfraCA G3 certificate request task

Request certificate from InfraCA G3 via Azure Cloud RA

- The infra CA G3 task contains different fields like below



Request certificate from InfraCA G3 via Azure Cloud RA

Azure Subscription * | Manage

acei-d-rg

Scoped to resource group 'acei-d-rg'

Action *

New Request

Resource Group *

acei-d-rg

Key vault *

acei-d-kv

Token Type

abn_amro_infra_ca_g3_ssl

Common Name *

private-acei-d-appgw.nl.eu.abnamro.com

Certificate Name *

acei-d-appgw-private-cert

OAR-id *

AAB.SYS.026199

Environment *

D

Certificate File Format

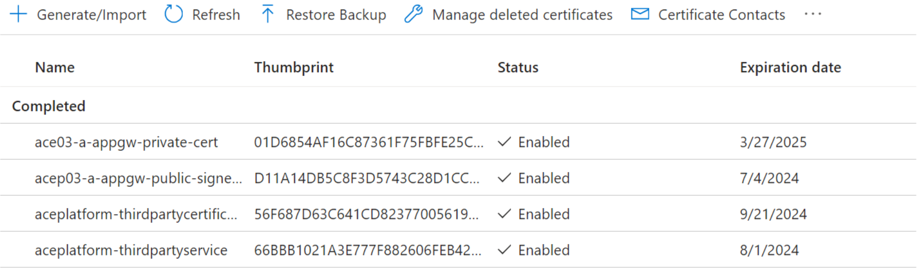
PFX

RSA Key Size

4096

☑ Should the private key be exportable? WARNING: Some workloads, like app gateway, require exportable. Only uncheck this if you are sure that this is what you require!

- To request a new certificate you can choose the action as new request and provide the details for RG, KV, OAR , Certifiacte Name , format , requied SAN values and environment to which you wnat to deploy and save the release and deploy the certificate
- Once you create the release it takes around 1min for the certificate to provision and once the release is successful the certificate will be available in the keyavult , you can verify the certificate by navigating into certifiactes section in KV as below acep03-a-kv - Microsoft Azure[8]



Name	Thumbprint	Status	Expiration date
Completed			
ace03-a-appgw-private-cert	01D6854AF16C87361F75FBFE25C...	✓ Enabled	3/27/2025
acep03-a-appgw-public-signe...	D11A14DB5C8F3D5743C28D1CC...	✓ Enabled	7/4/2024
aceplatform-thirdpartycertific...	56F687D63C641CD82377005619...	✓ Enabled	9/21/2024
aceplatform-thirdpartyservice	66BBB1021A3E777F882606FEB42...	✓ Enabled	8/1/2024

- To renew or revoke the certificate you can use action as renew or revoke and provide the same details as you have mentioned earlier and deploy the release and requested action will be provisioned

Through Automated Pipeline:

[8] https://portal.azure.com/#@abnamro.onmicrosoft.com/resource/subscriptions/bb5fe5fb-0b33-4cce-9d15-4397f5ab7487/resourceGroups/acep03-a-rg/providers/Microsoft.KeyVault/vaults/acep03-a-kv/certificates

There are 2 token types for automated pipeline approach

Token type: abn_amro_infra_ca_g3_ssl

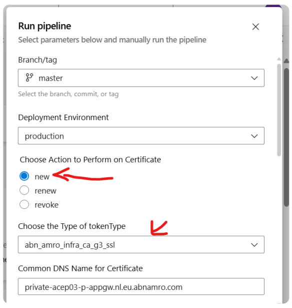
Reference automated Pipeline : Pipelines - Runs for acep-certificate-pipeline[9]

Automated Pipeline has 3 actions

1. New (To create new certificate)
2. Renew(To renew existing cert)
3. Revoke(To delete unused certificate)

Action : NEW

1. To create new certificate we need to choose new action with abnamro token type as mentioned in screenshot



Run pipeline
Select parameters below and manually run the pipeline

Branch/tag: master
Select the branch, commit, or tag

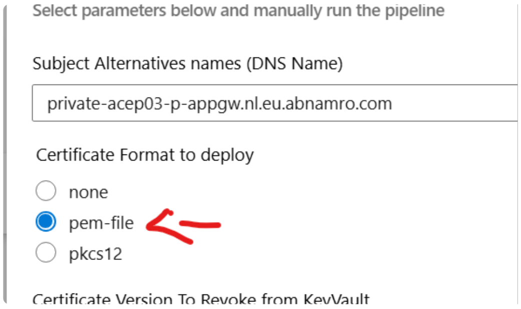
Deployment Environment: production

Choose Action to Perform on Certificate
● new
○ renew
○ revoke

Choose the Type of tokenType: abn_amro_infra_ca_g3_ssl

Common DNS Name for Certificate: private-acep03-p-appgw.nl.eu.abnamro.com

2. Provide the common DNS Name , certificate name to save in key vault and SAN values if any
3. After providing step 2 details select the format of cert to be deployed , except for application gateway all other certificate formats are PEM



Select parameters below and manually run the pipeline

Subject Alternatives names (DNS Name): private-acep03-p-appgw.nl.eu.abnamro.com

Certificate Format to deploy
○ none
● pem-file
○ pkcs12

Certificate Version To Revoke from KeyVault

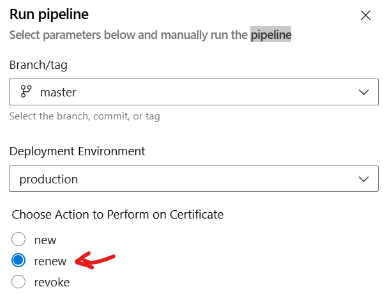
for application gateway it should be pkc12 format

4. During creation of certificate provide random value for certificate revoke version parameter because it is a required param to provide
5. After all above details are updated trigger the pipeline and the certificate will deployed to key vault with the mentioned name provided in the parameters during run time

Action : Renew

[9] https://dev.azure.com/cbsp-abnamro/GRD0001014/_build?definitionId=87478&_a=summary

1. For renew action follow the steps same as the process followed for Action : NEW, but select the action as renew as below



Run pipeline

Select parameters below and manually run the pipeline

Branch/tag: master

Select the branch, commit, or tag

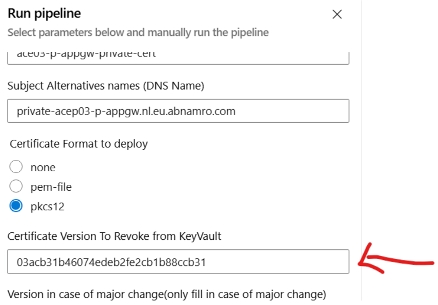
Deployment Environment: production

Choose Action to Perform on Certificate

○ new
● renew
○ revoke

Action: Revoke

1. For Revoke , provide all the details as provided for renew/new actions and additional to that we have to provide certificate version from keyvault which we want to remove as below



Run pipeline

Select parameters below and manually run the pipeline

ace03-p-appgw-private-cert

Subject Alternatives names (DNS Name): private-acep03-p-appgw.nl.eu.abnamro.com

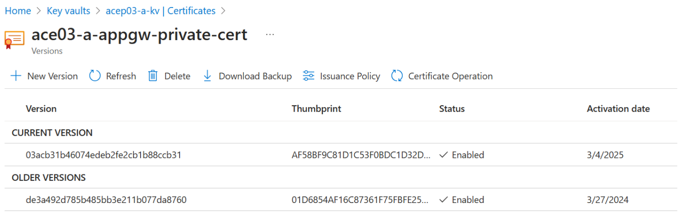
Certificate Format to deploy

○ none
○ pem-file
● pkcs12

Certificate Version To Revoke from KeyVault: 03acb31b46074edeb2fe2cb1b88ccb31

Version in case of major change(only fill in case of major change)

2. We can get certificate version from key vault as below



Home > Key vaults > acep03-a-kv | Certificates >

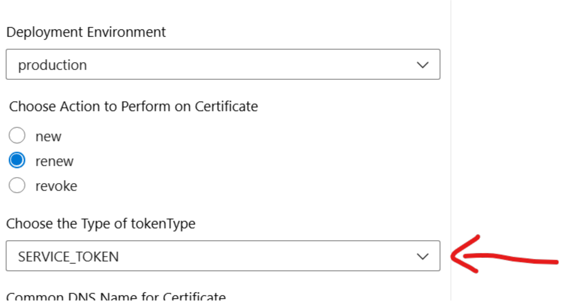
ace03-a-appgw-private-cert

Versions

Version	Thumbprint	Status	Activation date
CURRENT VERSION			
03acb31b46074edeb2fe2cb1b88ccb31	AF58BF9C81D1C53F0BDC1D32D...	✓ Enabled	3/4/2025
OLDER VERSIONS			
de3a492d785b485bb3e211b077da8760	01D6854AF16C87361F75FBFE25...	✓ Enabled	3/27/2024

Token type : service_token

For service_token , updation of all te parameters is same as abn amro token type except token selected is service_token



Deployment Environment: production

Choose Action to Perform on Certificate

○ new
● renew
○ revoke

Choose the Type of tokenType: SERVICE_TOKEN

Common DNS Name for Certificate

Note : We are using service token type only for Third party certificate "aceplatform-thirdpartyservice" in DTAP

Chained Certificate:

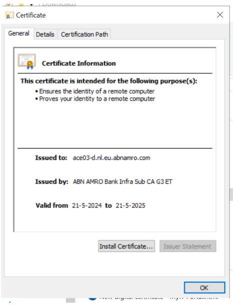
Procedure to deploy the Chained certificate is documented in the following wiki page Create Entrust Chained SSL Certificate - Overview (azure.com)[10]

Root Certificate :

We use root certificate as a SSL certificate in application gateway to identify the AKS as backend server since AKS uses Ingress certificate which also has the same root .

Procedure to deploy root cert :

- Go to MyIT and click on the AKS certificate for the env to which you are creating the root cert
- Click on settings icon and download the .cer file of the certificate
- Once you download the .cer and open it it looks something as below



Certificate Information

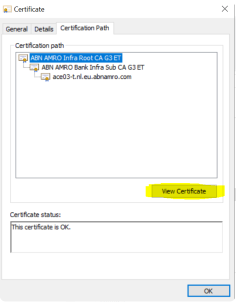
This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer
- Proves your identity to a remote computer

Issued to: ace03-d.nl.eu.abnamro.com

Issued by: ABN AMRO Bank Infra Sub CA G3 ET

Valid from 21-5-2024 to 21-5-2025

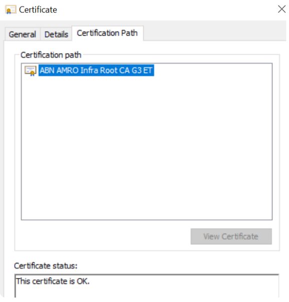
- Open .cer file of new certificate and click on certification path and open the root certificate by clicking on view certificate as below and it opens the root certificate



Certification path
- ABN AMRO Infra Root CA G3 ET
  - ABN AMRO Bank Infra Sub CA G3 ET
    - ace03-t.nl.eu.abnamro.com

Certificate status:
This certificate is OK.

  - after you click on view certificate of root you will see the root cert as below

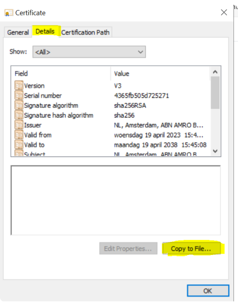


Certification path
- ABN AMRO Infra Root CA G3 ET

Certificate status:
This certificate is OK.

[10] https://dev.azure.com/cbsp-abnamro/GRD0001014/_wiki/wikis/GRD0001014.wiki/71494/Create-Entrust-Chained-SSL-Certificate

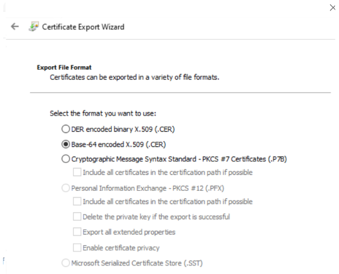
- Now click on details and click on copy to file



Show: <All>

Field	Value
Version	V3
Serial number	4365fb505d725271
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	NL, Amsterdam, ABN AMRO B...
Valid from	woensdag 19 april 2023 15:4...
Valid to	maandag 19 april 2038 15:45:08
Subject	NL, Amsterdam, ABN AMRO B

- After clicking on copy to file click on next and choose the base-64 format of certificate

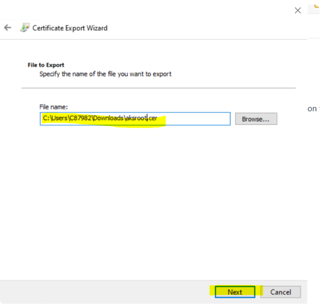


Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
□ Enable certificate privacy
○ Microsoft Serialized Certificate Store (.SST)

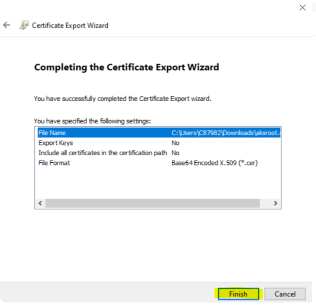
- Give the name of the file and choose the folder



File to Export
Specify the name of the file you want to export

File name: C:\Users\C87982\Downloads\aksroot.cer

- Click on next and click on finish



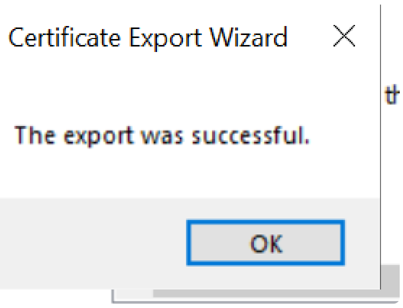
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\C87982\Downloads\aksroot.
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

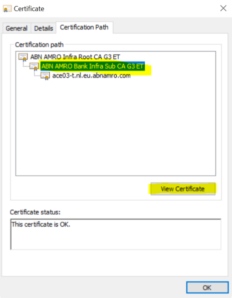
- After you click on finish you should message as export was successful



Certificate Export Wizard

The export was successful.

- Repeat the above steps for intermediate certificate



Certificate

General | Details | Certification Path

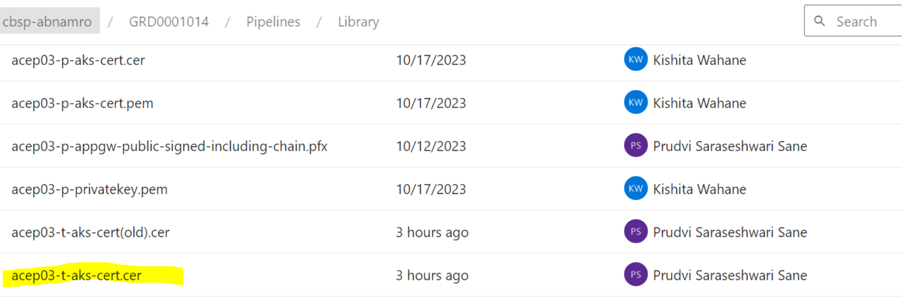
Certification path

- ABN AMRO Infra Root CA G3 ET
  - ABN AMRO Bank Infra Sub CA G3 ET
    - ace03-t.nl.eu.abnamro.com

Certificate status:

This certificate is OK.

- Export the intermediate certificate
- After two certs are imported open the root and intermediate certificates with notepad
- Append the content of intermediate certificate after the content of root certificate as attached file acep03-t-aks-cert.cer[11]
- Upload the combined .cer file in secure files



cbsp-abnamro / GRD0001014 / Pipelines / Library

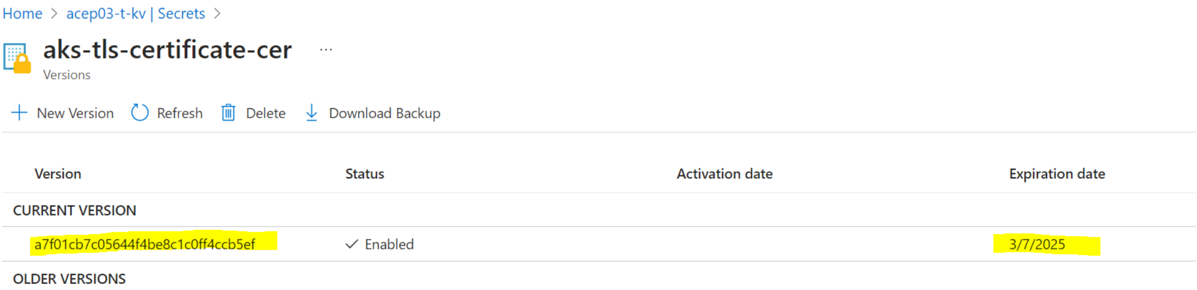
acep03-p-aks-cert.cer	10/17/2023	KW Kishita Wahane
acep03-p-aks-cert.pem	10/17/2023	KW Kishita Wahane
acep03-p-appgw-public-signed-including-chain.pfx	10/12/2023	PS Prudvi Saraseshwari Sane
acep03-p-privatekey.pem	10/17/2023	KW Kishita Wahane
acep03-t-aks-cert(old).cer	3 hours ago	PS Prudvi Saraseshwari Sane
acep03-t-aks-cert.cer	3 hours ago	PS Prudvi Saraseshwari Sane

- After it is uploaded provide the permission to block and run the pre-infratructure-pipeline by choosing only

  push_aks_certificate_kv from pre-infra-pipeline.yaml - Repos (azure.com)[12]
- After the pipeline is successful check the version in kv if the secret is uploaded

[11] https://confluence.int.abnamro.com/download/attachments/635450707/acep03-t-aks-cert.cer?api=v2&modificationDate=1709816331067&version=1

[12] https://dev.azure.com/cbsp-abnamro/GRD0001014/_git/acep-platform-infrastructure?path=/pipelines/pre-infra-pipeline.yaml

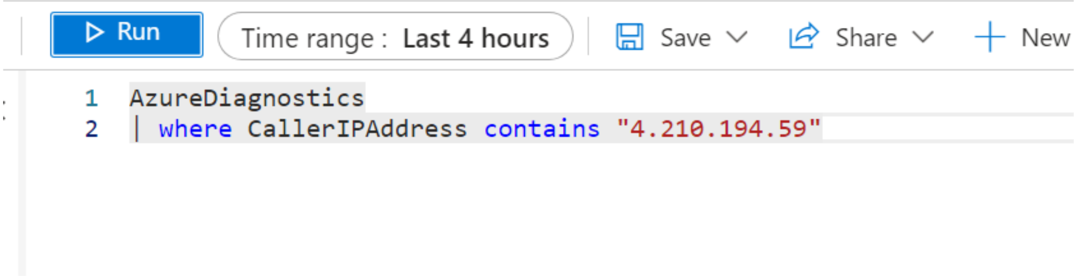


Version	Status	Activation date	Expiration date
CURRENT VERSION			
a7f01cb7c05644f4be8c1c0ff4ccb5ef	✓ Enabled		3/7/2025
OLDER VERSIONS			

- With the above process Root certificate upload to kv is done

Validation of certificate with appgw:

- Appgw automatically checks if any new version of cert exists in Key vault for every 4hrs and pulls the latest updated cert so you can use below KQL query in key vault logs



```
AzureDiagnostics
| where CallerIPAddress contains "4.210.194.59"
```

- Check when does the latest pull happened , check the time at which you have uploaded the cert in KV and Revalidate the public URL(ace-t.abnamro.nl/message-hub/ping[13]) access after the appgw has pull the updated cert from kv.
- We don't need to wait for 4hours for application gateway to pull the latest certificate , to mitigate the above error you can manually update the latest version of kv secret using below command

az network application-gateway root-cert update --gateway-name acep03-d-appgw --name chatbot-trustedCert --resource-group acep-d-rg --keyvault-secret https://acep03-d-kv.vault.azure.net/secrets/aks-tls-certificate-cer/0952af44bca34fc8b9129029d412f466

Note: The root and sub root of infra ca g3 certificate expiry is not similar to other certificate expiries which we request through MYIT , since these are managed through crypto team they provide us the update on when the certificates are going to expire till then we don't need to update the root or sub root if we are using latest ca g3 certificates. In our case we don't need to update the secure file ace03-env-aks-cer.cer from library until crypto notifies us if there is any change for the root or sub root

Note: We use Chained Certificate and Root Certificate for application Gateway

[13] https://ace-t.abnamro.nl/message-hub/ping