How you can renew the certificates of a two-tier PKI

vmlabblog.com/2024/01/how-you-can-renew-the-certificates-of-a-two-tier-pki

January 19, 2024

In this blog post I'm going to show how you can renew the certificates of a two-tier PKI. A two-tier PKI is a Public Key Infrastructure that consists of two levels of certification authorities (CAs): a root CA and one or more issuing CA(s) (Subordinate). The root CA is typically offline and highly secure, while the issuing CAs are online and can be scaled horizontally to meet the organization's needs. In this blog post I am going to show how to renew the certificate of the root CA and of the issuing CA(s). I

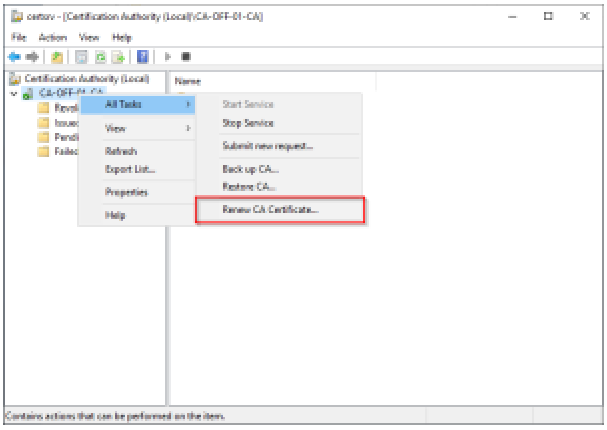
An important consideration before you start renewing your certificates: The validity period of certificates issued by the root CA cannot exceed the validity period of the Root CA certificate. If your Root CA's certificate expires in 2 months and you want to extend your issuing ca's certificate for 5 years, you must first extend your Root CA. If you do not, then the validity period of your Issuing CA will be 2 months instead of 5 years.

Renew the certificates of a two-tier PKI:

The Root CA

Let's start by renewing the Root CA. If the validity period of your root CA is longer than the period by which you want to renew Issuing CA, you can choose to skip this step and proceed to Issuing CA.

1. Turn on the Root CA and Log on. Open the Certification Authority console. Make a right-mouse click on the CA name, select "All Tasks" and "Renew CA Certificate…".

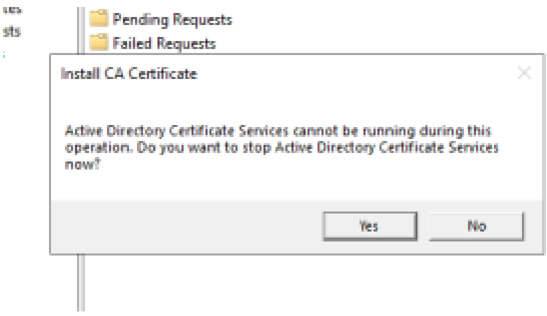


2. A screen will appear with the question to stop Active Directory Certificate Services. Click "Yes" on the question to stop certificate services.

3. On the next screen answer the question "Do you want to generate a new public and private key pair?" with "No" because we only want to renew the certificate and click "OK".

4. Because the Root CA is a completely offline we need to copy the new Root CA certificate to Issuing CA. In this example I am using the network, but if you don't have a network connection you will have to use another way.

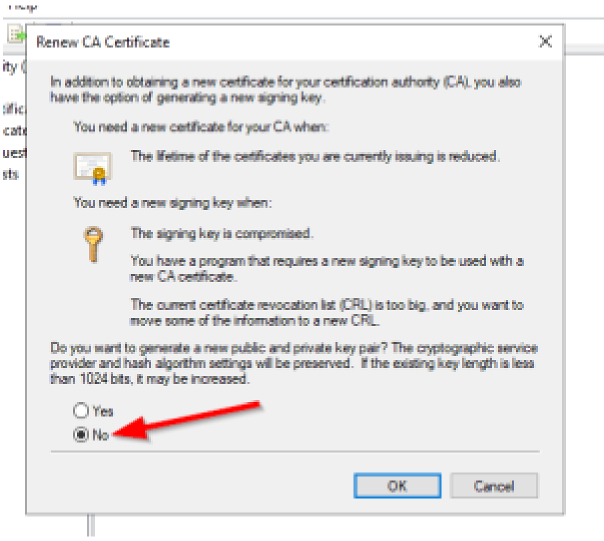
5. Open a Command Prompt and Execute: "Certutil.exe -f -dspublish <Root CA>.cer RootCA" this command will publish the root CA to the Active Directory. The machines in AD will get the new root CA cert installed with the next GPO update or reboot, whatever is sooner.



Install CA Certificate

Active Directory Certificate Services cannot be running during this operation. Do you want to stop Active Directory Certificate Services now?

6. The Root CA certificate has now been renewed. If you only want to renew your Root CA certificate you can now shut down the Root CA server, otherwise keep it to renew the certificate of the Issuing CA.



Renew CA Certificate

In addition to obtaining a new certificate for your certification authority (CA), you also have the option of generating a new signing key.

You need a new certificate for your CA when:

The lifetime of the certificates you are currently issuing is reduced.

You need a new signing key when:

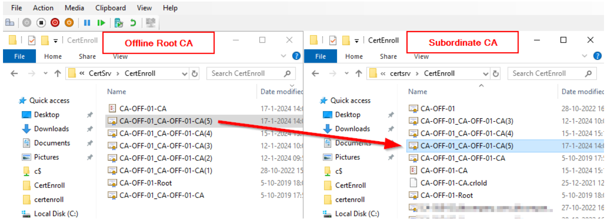
The signing key is compromised.

You have a program that requires a new signing key to be used with a new CA certificate.

The current certificate revocation list (CRL) is too big, and you want to move some of the information to a new CRL.

Do you want to generate a new public and private key pair? The cryptographic service provider and hash algorithm settings will be preserved. If the existing key length is less than 1024 bits, it may be increased.

○ Yes
● No

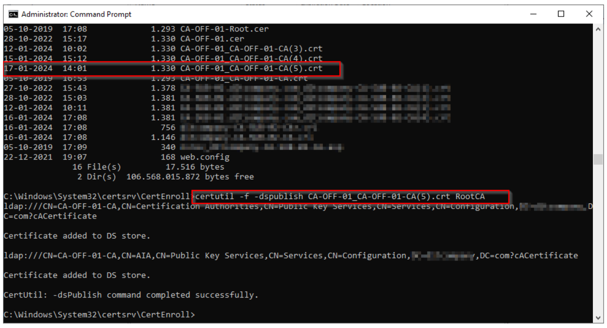


Offline Root CA:

Name	Date modified
CA-OFF-01-CA	17-1-2024 14:
CA-OFF-01_CA-OFF-01-CA(5)	17-1-2024 14:
CA-OFF-01_CA-OFF-01-CA(4)	15-1-2024 15:
CA-OFF-01_CA-OFF-01-CA(3)	12-1-2024 10:
CA-OFF-01_CA-OFF-01-CA(2)	12-1-2024 09:
CA-OFF-01_CA-OFF-01-CA(1)	28-10-2022 15
CA-OFF-01-Root	5-10-2019 18:
CA-OFF-01_CA-OFF-01-CA	5-10-2019 17:

Subordinate CA:

Name	Date modified
CA-OFF-01	28-10-2022 16
CA-OFF-01_CA-OFF-01-CA(3)	12-1-2024 10:
CA-OFF-01_CA-OFF-01-CA(4)	15-1-2024 15:
CA-OFF-01_CA-OFF-01-CA(5)	17-1-2024 14:
CA-OFF-01_CA-OFF-01-CA	5-10-2019 17:
CA-OFF-01-CA	15-1-2024 15:
CA-OFF-01-CA.crlold	25-12-2021 12
CA-OFF-01-Root	5-10-2019 18:
[redacted]	27-10-2022 16



Administrator: Command Prompt

```
05-10-2019  17:08             1.293 CA-OFF-01-Root.cer
28-10-2022  15:17             1.330 CA-OFF-01.cer
12-01-2024  10:02             1.330 CA-OFF-01_CA-OFF-01-CA(3).crt
15-01-2024  15:12             1.330 CA-OFF-01_CA-OFF-01-CA(4).crt
17-01-2024  14:01             1.330 CA-OFF-01_CA-OFF-01-CA(5).crt
05-10-2019  16:53             1.293 CA-OFF-01_CA-OFF-01-CA.crt
27-10-2022  15:43             1.378 [redacted]
28-10-2022  15:03             1.381 [redacted]
12-01-2024  10:11             1.381 [redacted]
16-01-2024  17:08             1.381 [redacted]
16-01-2024  17:08               756 [redacted]
16-01-2024  17:08             1.146 [redacted]
05-10-2019  17:09               340 [redacted]
22-12-2021  19:07               168 web.config
              16 File(s)         17.516 bytes
               2 Dir(s)  106.568.015.872 bytes free

C:\Windows\System32\certsrv\CertEnroll>certutil -f -dspublish CA-OFF-01_CA-OFF-01-CA(5).crt RootCA
ldap:///CN=CA-OFF-01-CA,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,[redacted],D
C=com?cACertificate

Certificate added to DS store.

ldap:///CN=CA-OFF-01-CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,[redacted],DC=com?cACertificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.

C:\Windows\System32\certsrv\CertEnroll>
```

The Issuing CA

Now that the Root CA's certificate has been renewed, let us move on to renewing the Issuing CA's certificate. This is similar to the steps of the Root CA, but with the difference that the certificate is not issued by the Issuing CA itself, but by the Root CA. The Issuing CA only has delegated authority to issue certificates on behalf of the Root CA.

7. If you have just renewed your Root CA certificate run "gpupdate /force" to make sure the new root CA certificate is installed on your Issuing CA.

8. Open the Certification Authority console on the Issuing CA. Make a right-mouse click on the CA name, select “All Tasks” and “Renew CA Certificate…”.

9. A screen will appear with the question to stop Active Directory Certificate Services. Click “Yes” on the question to stop certificate services.

10. On the next screen answer the question “Do you want to generate a new public and private key pair?” with “No” because we only want to renew the certificate and click “OK”.

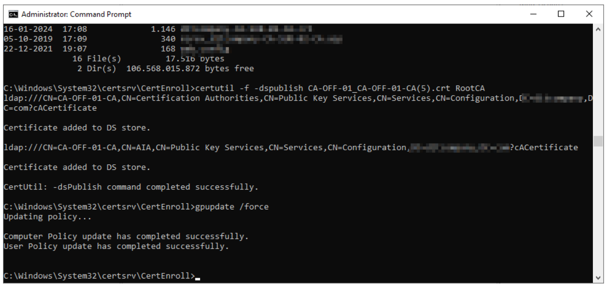
11. A window appears where you can select an online CA to renew the certificate. Since we are using an Offline Root CA, you can press “Cancel.” This will not send the request file but store it locally on the C drive. The exact location and filename are displayed at the bottom of the window (c:\*.req).

12. Copy the request file from your Issuing CA to the Root ca.

13. Open then Certification Authority console on the Root CA, right mouse clicks on the ca name, select “All Tasks” and “Submit new request…”.

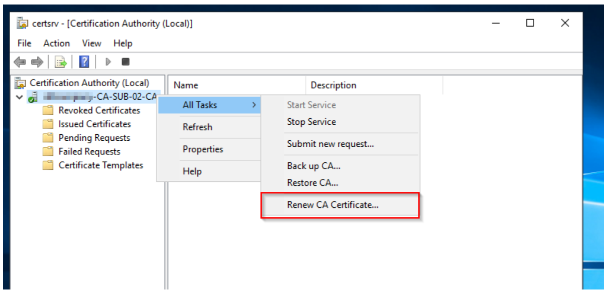
14. Select the request file and press “Open”.

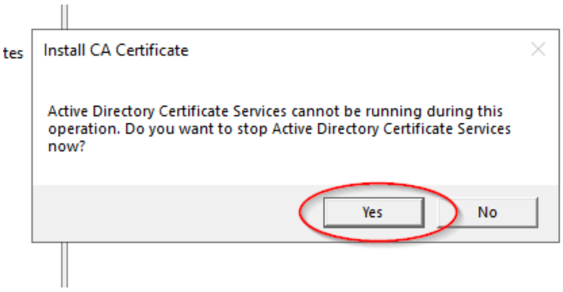
15. Go to “Pending Requests” and issue the pending certificate for the subordinate server.



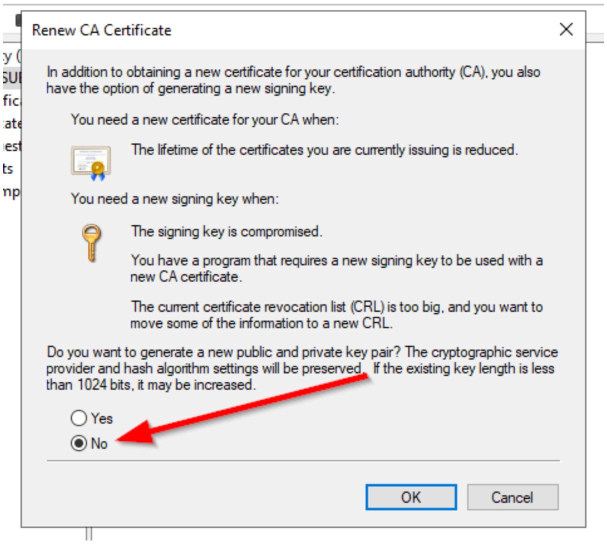
Administrator: Command Prompt

```
16-01-2024  17:08             1.146 [redacted]
05-10-2019  17:09               340 [redacted]
22-12-2021  19:07               168 [redacted]
              16 File(s)         17.516 bytes
               2 Dir(s)  106.568.015.872 bytes free

C:\Windows\System32\certsrv\CertEnroll>certutil -f -dspublish CA-OFF-01_CA-OFF-01-CA(5).crt RootCA
ldap:///CN=CA-OFF-01-CA,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,[redacted],D
C=com?cACertificate

Certificate added to DS store.

ldap:///CN=CA-OFF-01-CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,[redacted]?cACertificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.

C:\Windows\System32\certsrv\CertEnroll>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Windows\System32\certsrv\CertEnroll>_
```





Active Directory Certificate Services cannot be running during this operation. Do you want to stop Active Directory Certificate Services now?



In addition to obtaining a new certificate for your certification authority (CA), you also have the option of generating a new signing key.

You need a new certificate for your CA when:

The lifetime of the certificates you are currently issuing is reduced.

You need a new signing key when:

The signing key is compromised.

You have a program that requires a new signing key to be used with a new CA certificate.

The current certificate revocation list (CRL) is too big, and you want to move some of the information to a new CRL.

Do you want to generate a new public and private key pair? The cryptographic service provider and hash algorithm settings will be preserved. If the existing key length is less than 1024 bits, it may be increased.

○ Yes
● No

16. Now go to “Issued certificates”, select the certificate what was just issued and open it.

17. Go to the “Details” tab and click on “Copy to File…”.

18. Select Export File Format *.P7B and check “include all certificates in the certification path if possible”!

19. Save the file on the local disk.

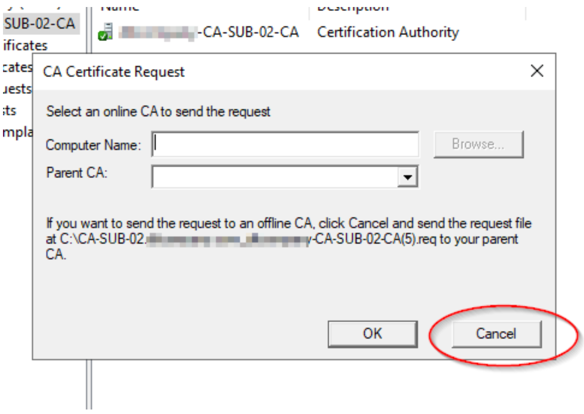
20. Copy the certificate file to the subordinate CA. Start the certificate services and the subordinate CA.

21. Open the Certification Authority console. Make a right-mouse click on the CA name, select “All Tasks” and “Install CA Certificate…”.

22. Click “Yes” on the question to stop certificate services.

23. Select the certificate and press “Open”.

24. The renewal is now completed for both the root CA and the Subordinate CA. When you check the certificate properties of the Subordinate CA it will show the new validity period. Do not forget to shutdown the root CA server. This is how you renew the certificates of a two-tier PKI.



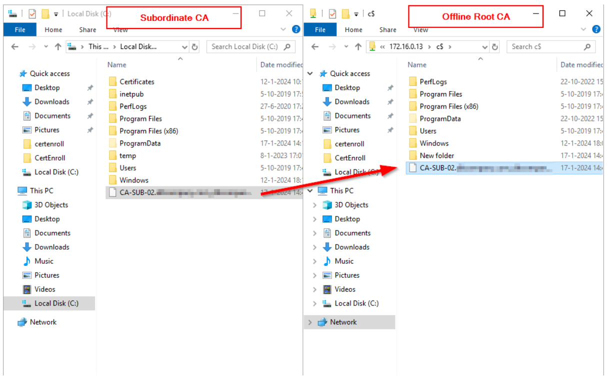
CA Certificate Request

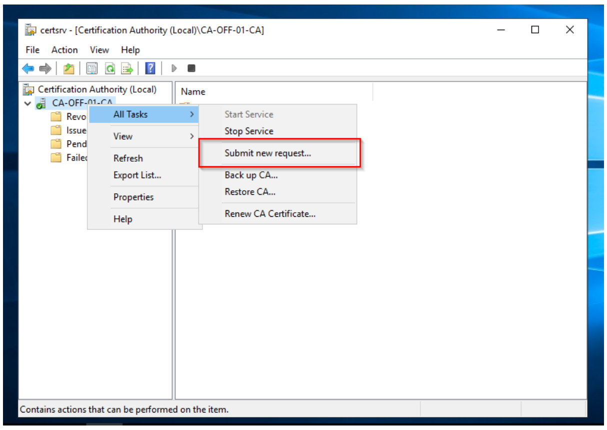
Select an online CA to send the request

Computer Name:

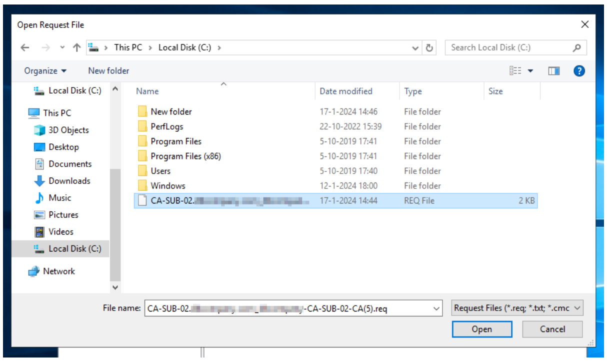
Parent CA:

If you want to send the request to an offline CA, click Cancel and send the request file at C:\CA-SUB-02.[redacted]y-CA-SUB-02-CA(5).req to your parent CA.




certsrv - [Certification Authority (Local)\CA-OFF-01-CA]

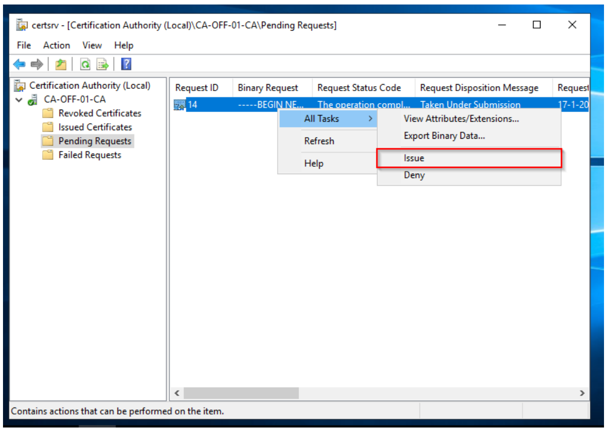
Contains actions that can be performed on the item.


Open Request File

Name	Date modified	Type	Size
New folder	17-1-2024 14:46	File folder	
PerfLogs	22-10-2022 15:39	File folder	
Program Files	5-10-2019 17:41	File folder	
Program Files (x86)	5-10-2019 17:41	File folder	
Users	5-10-2019 17:40	File folder	
Windows	12-1-2024 18:00	File folder	
CA-SUB-02.[redacted]	17-1-2024 14:44	REQ File	2 KB

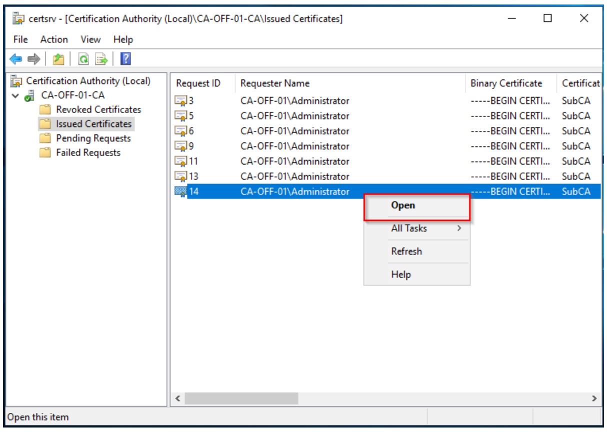
File name: CA-SUB-02.[redacted]-CA-SUB-02-CA(5).req

Request Files (*.req; *.txt; *.cmc



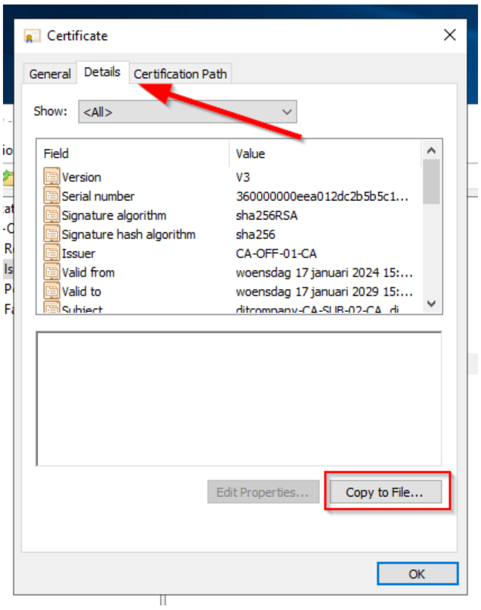
Request ID	Binary Request	Request Status Code	Request Disposition Message	Request
14	-----BEGIN NE...	The operation compl...	Taken Under Submission	17-1-20

Contains actions that can be performed on the item.



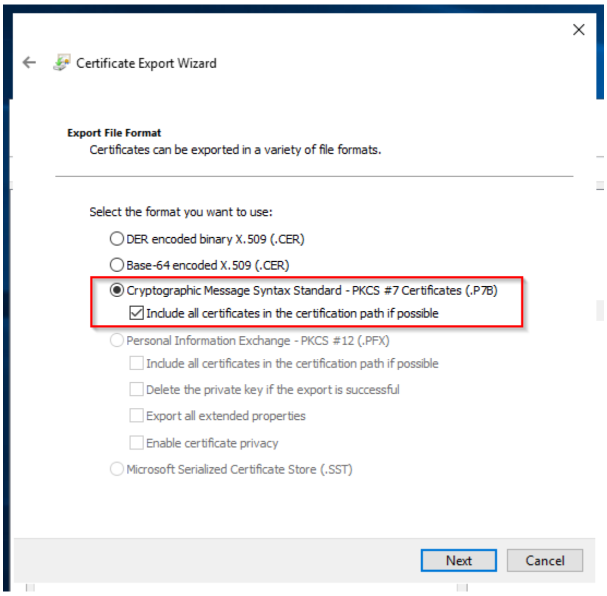
Request ID	Requester Name	Binary Certificate	Certificat
3	CA-OFF-01\Administrator	-----BEGIN CERTI...	SubCA
5	CA-OFF-01\Administrator	-----BEGIN CERTI...	SubCA
6	CA-OFF-01\Administrator	-----BEGIN CERTI...	SubCA
9	CA-OFF-01\Administrator	-----BEGIN CERTI...	SubCA
11	CA-OFF-01\Administrator	-----BEGIN CERTI...	SubCA
13	CA-OFF-01\Administrator	-----BEGIN CERTI...	SubCA
14	CA-OFF-01\Administrator	-----BEGIN CERTI...	SubCA

Open this item



Show: <All>

Field	Value
Version	V3
Serial number	360000000eea012dc2b5b5c1...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CA-OFF-01-CA
Valid from	woensdag 17 januari 2024 15:...
Valid to	woensdag 17 januari 2029 15:...
Subject	ditcompany-CA-SUB-02-CA, di...



Certificate Export Wizard

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)

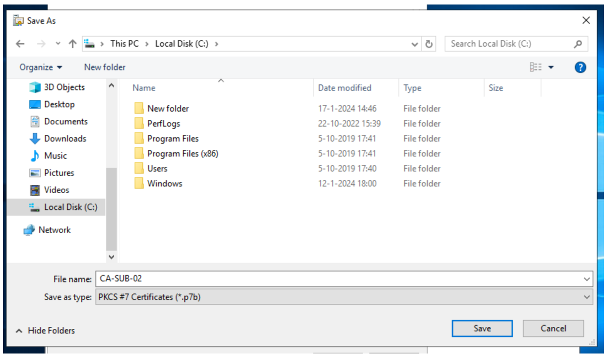
□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)



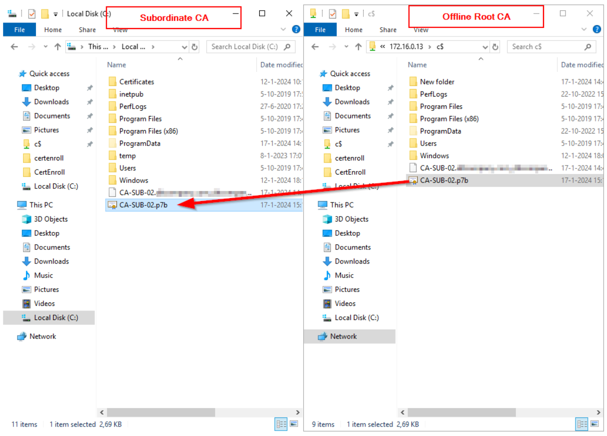
Save As

This PC › Local Disk (C:) ›

Name	Date modified	Type	Size
New folder	17-1-2024 14:46	File folder	
PerfLogs	22-10-2022 15:39	File folder	
Program Files	5-10-2019 17:41	File folder	
Program Files (x86)	5-10-2019 17:41	File folder	
Users	5-10-2019 17:40	File folder	
Windows	12-1-2024 18:00	File folder	

File name: CA-SUB-02

Save as type: PKCS #7 Certificates (*.p7b)



Local Disk (C:)

Subordinate CA

Name	Date modified
Certificates	12-1-2024 10:
inetpub	5-10-2019 17:
PerfLogs	27-6-2020 17:
Program Files	5-10-2019 17:
Program Files (x86)	5-10-2019 17:
ProgramData	17-1-2024 14:
temp	8-1-2023 17:0
Users	5-10-2019 17:
Windows	12-1-2024 18:
CA-SUB-02.[redacted]	17-1-2024 14:
CA-SUB-02.p7b	17-1-2024 15:

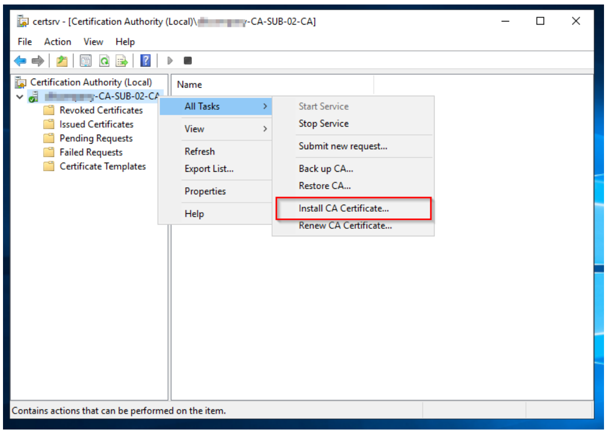
11 items 1 item selected 2,69 KB

c$

Offline Root CA

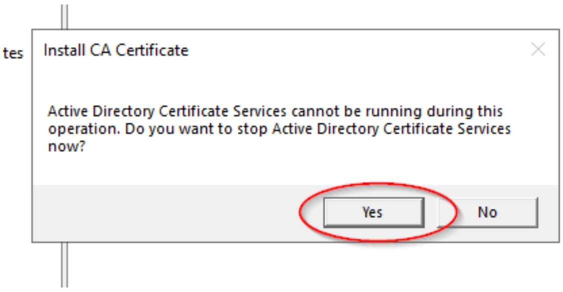
Name	Date modified
New folder	17-1-2024 14:
PerfLogs	22-10-2022 15
Program Files	5-10-2019 17:
Program Files (x86)	5-10-2019 17:
ProgramData	22-10-2022 15
Users	5-10-2019 17:
Windows	12-1-2024 18:
CA-SUB-02.[redacted]	17-1-2024 14:
CA-SUB-02.p7b	17-1-2024 15:

9 items 1 item selected 2,69 KB



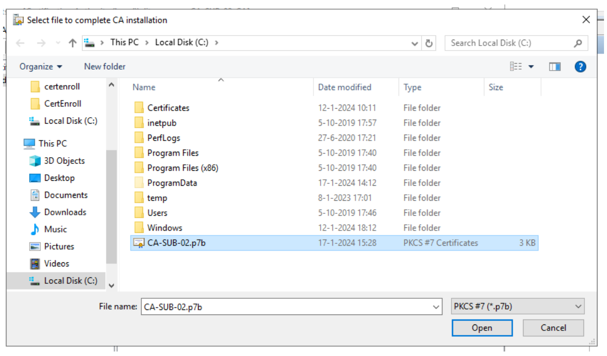
certsrv - [Certification Authority (Local)\[redacted]-CA-SUB-02-CA]

Contains actions that can be performed on the item.



Install CA Certificate

Active Directory Certificate Services cannot be running during this operation. Do you want to stop Active Directory Certificate Services now?

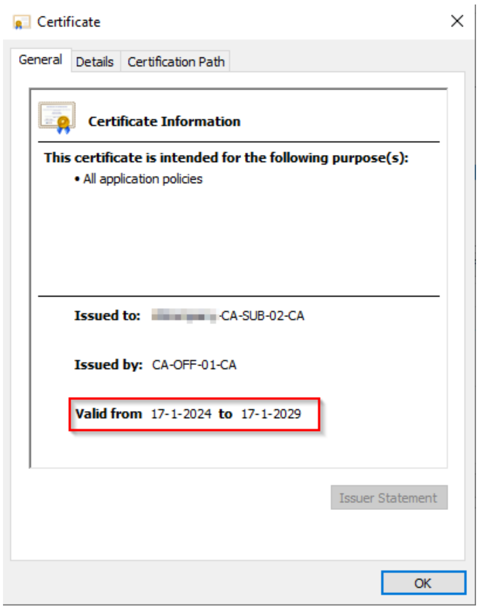


Select file to complete CA installation

Name	Date modified	Type	Size
Certificates	12-1-2024 10:11	File folder	
inetpub	5-10-2019 17:57	File folder	
PerfLogs	27-6-2020 17:21	File folder	
Program Files	5-10-2019 17:40	File folder	
Program Files (x86)	5-10-2019 17:40	File folder	
ProgramData	17-1-2024 14:12	File folder	
temp	8-1-2023 17:01	File folder	
Users	5-10-2019 17:46	File folder	
Windows	12-1-2024 18:12	File folder	
CA-SUB-02.p7b	17-1-2024 15:28	PKCS #7 Certificates	3 KB

File name: CA-SUB-02.p7b

PKCS #7 (*.p7b)



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- All application policies

Issued to: [redacted]-CA-SUB-02-CA

Issued by: CA-OFF-01-CA

Valid from 17-1-2024 to 17-1-2029

”