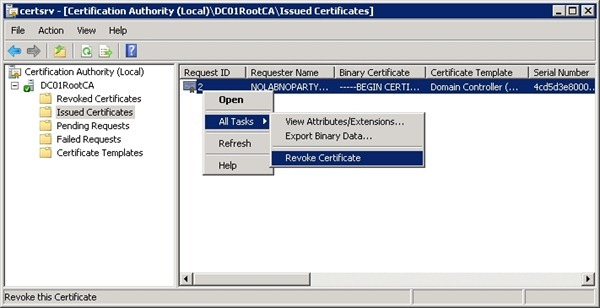
Remove CA from Active Directory

To remove Certification Authority from Active Directory you must follow the correct steps in order to delete the CA objects and services no longer needed.

The procedure helps to properly decommission the CA and clean the Active Directory environment from the objects left during the uninstall process of the AD Certificate Services.

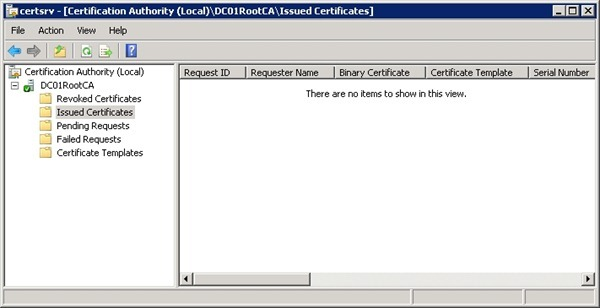
Revoke all issued certificates

Open the Certification Authority, expand the configured CA and navigate to Issued Certificates. In the right pane right click the issued certificates and select **All Tasks > Revoke Certificate** option.

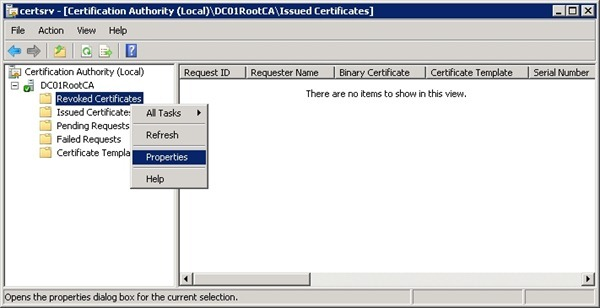
Specify a reason in the Reason code field then click Yes.



The certificate is removed from the list.

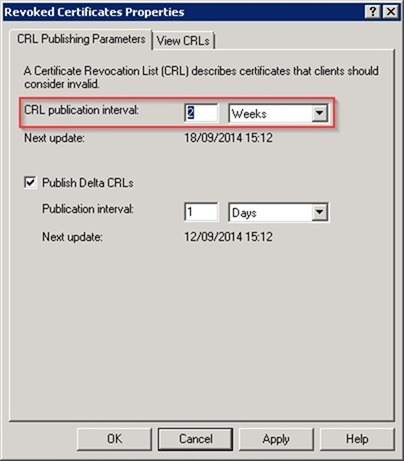


Right click the Revoke Certificates item and select Properties.

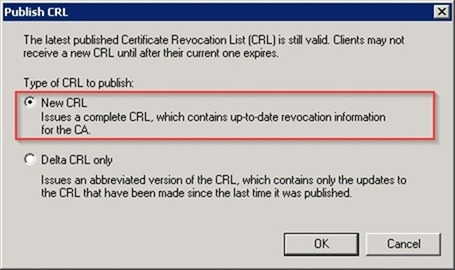


Increase the CRL publication interval by typing a suitably long value then click OK.

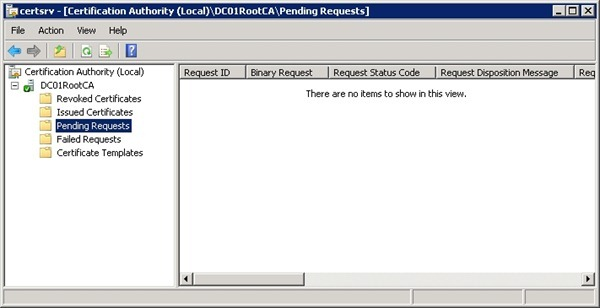
Now right click Revoked Certificates item and select All Tasks > Publish.



Select New CRL option and click OK.



In the Pending Requests folder deny any pending certificate requests right clicking the pending request then selecting All Tasks > Deny Request.

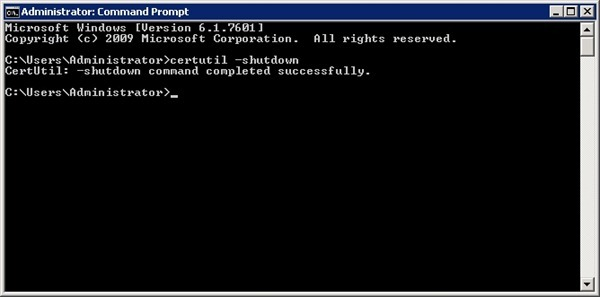


**NOTE: DELETE KEY BEFORE REMOVING ROLES**

Uninstall AD Certificate Services

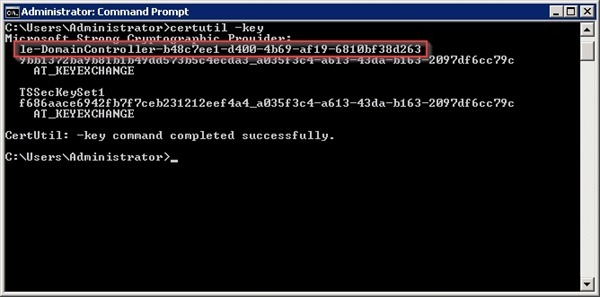
From the server, open the Command Prompt and type the command:

C:\>certutil -shutdown



To list all key stores for the local computer, type in the Command Prompt:

C:\>certutil -key



Delete the private key associated with the CA using the command:

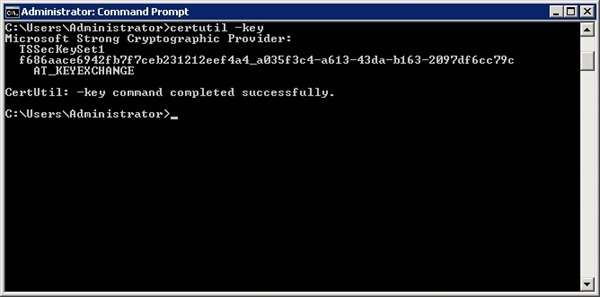
certutil -delkey CertificateAuthorityName

C:\>certutil –delkey le-DomainController-b48c7ee1-d400-4b69-af19-6810bf38d263

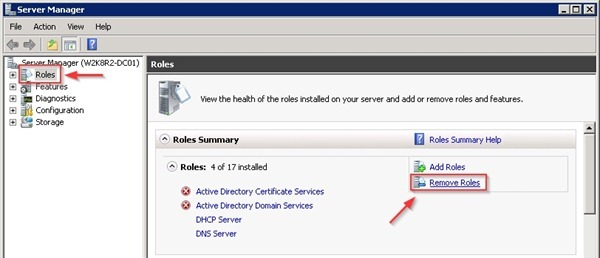


List the key stores once again to check if the CA private key has been removed.

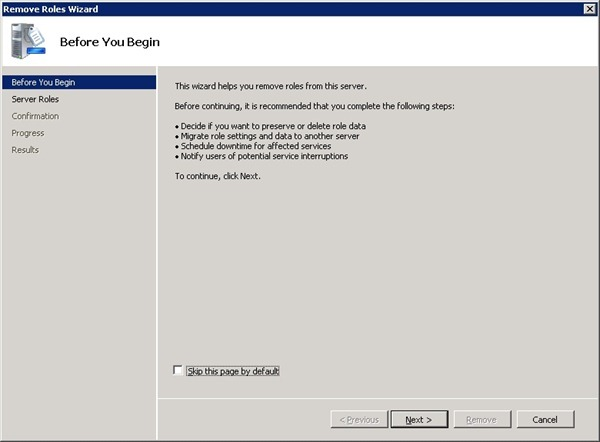
C:\>certutil -key



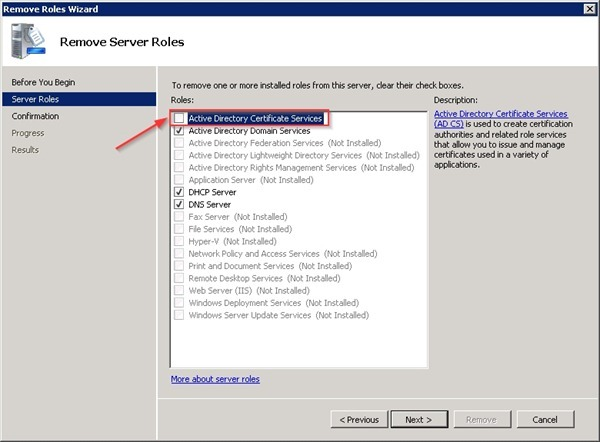
Open the Server Manager, select Roles item and click Remove Roles in the right pane.



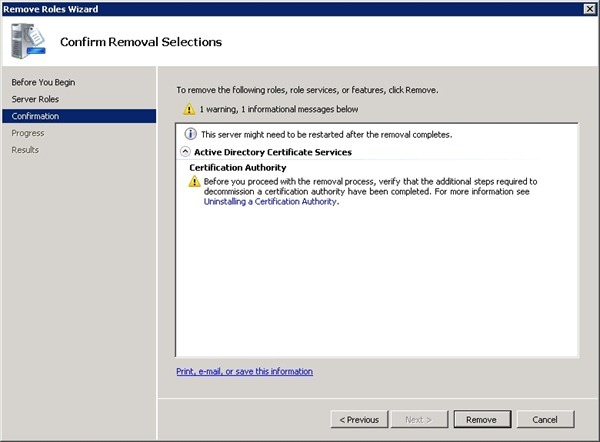
The Remove Roles Wizard opens. Click Next to continue.



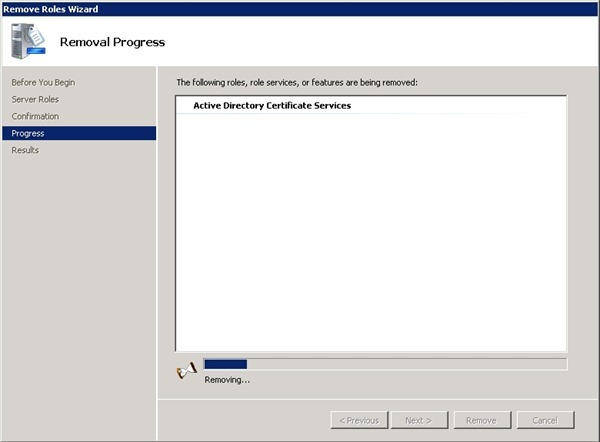
Uncheck Active Directory Certificate Services then click Next.



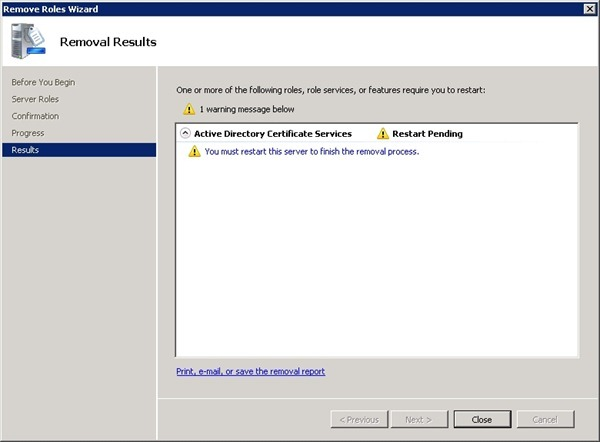
Click Remove to proceed.



The selected role is being removed.



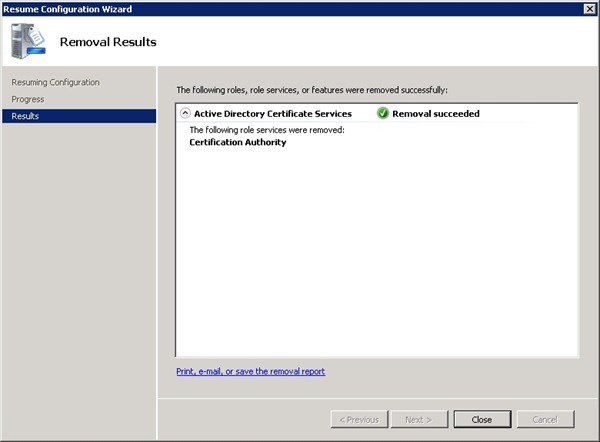
Click Close to exit the wizard.



Click Yes to restart the server.



After rebooting the server, the procedure is complete.

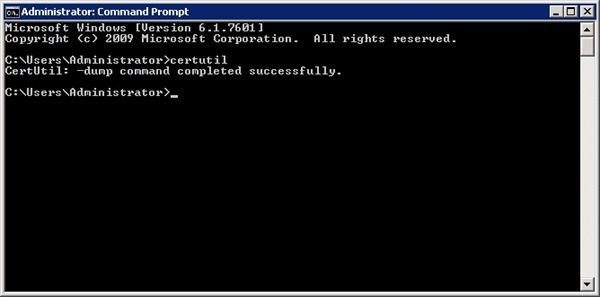


Remove CA objects from Active Directory

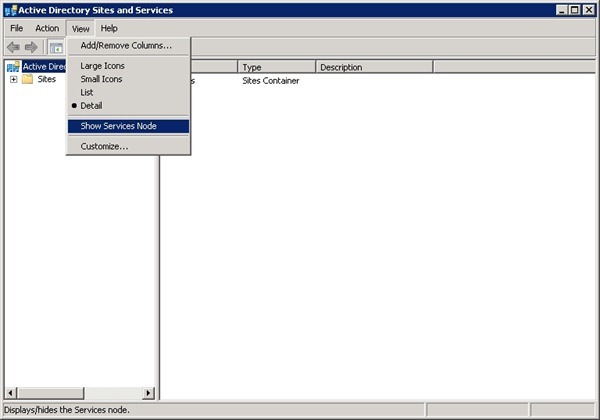
When the CA is installed, several objects are created in the Active Directory but not removed during the uninstalling process. Only pKIEnrollmentService object is removed to prevent clients from trying enroll against the decommissioned CA.

Open the Command Prompt and type the command certutil.

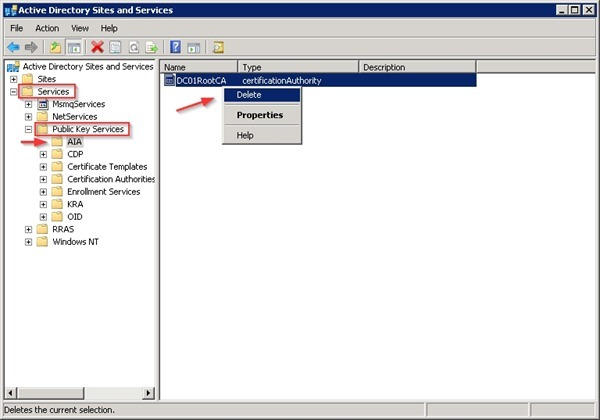
C:\>certutil



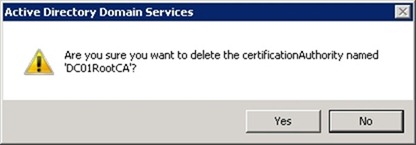
Open the Active Directory Site and Services and select View >Show Services Node.



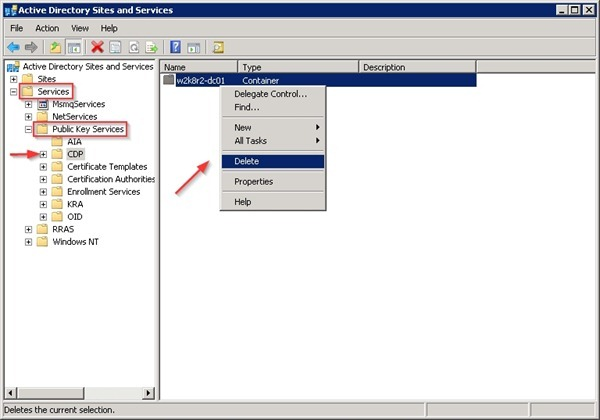
Navigate to Services > Public Key Services > AIA. Right click the CA object and select Delete.



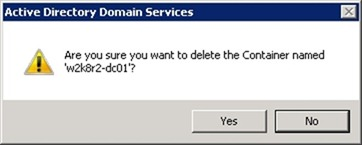
Click Yes to confirm deletion.



Now navigate to Services > Public Key Services > CDP. Right click the container object where Certificate Services is installed and select Delete.



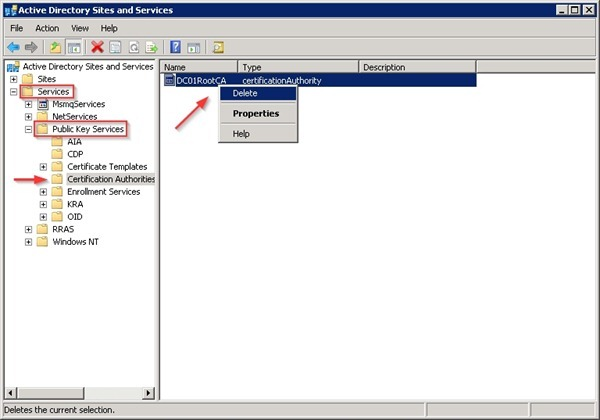
Click Yes to confirm deletion.



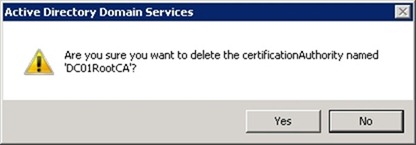
Click Yes to confirm.



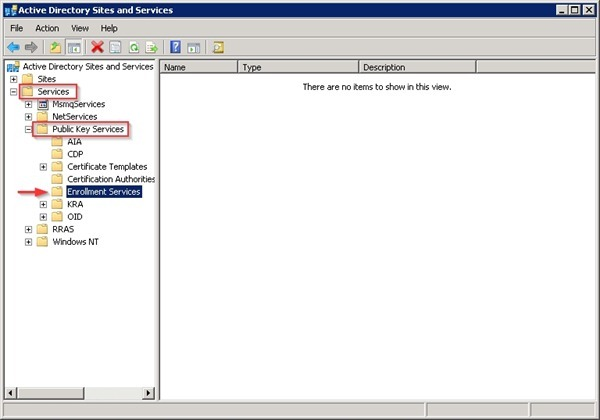
Navigate to Services > Public Key Services > Certification Authorities. Right click the CA object and select Delete.



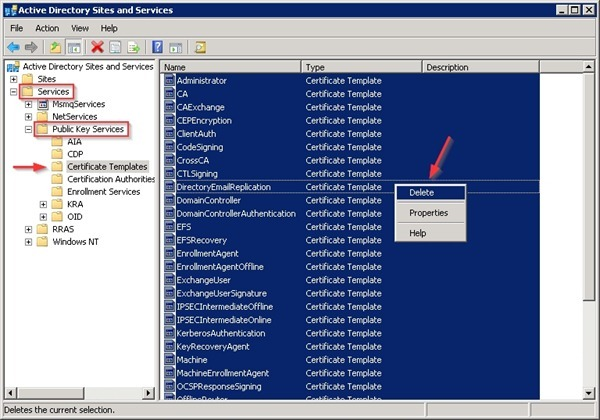
Click Yes to confirm deletion.



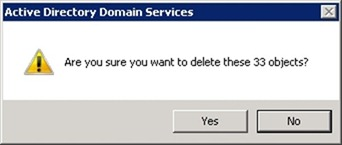
Navigate to Services > Public Key Services > Enrollment Services. In the right pane verify that the pKIEnrollmentService object has been removed during the CA uninstall process. If the object is not deleted, right click the object, select Delete and click Yes to confirm.



Navigate to Services > Public Key Services > Certificate Templates. In the right pane select a certificate and press CTRL+A to select all templates. Right click and select Delete.



Click Yes to confirm deletion.

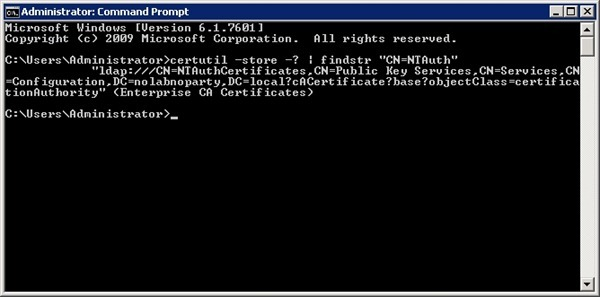


Delete certificates published to the NtAuthCertificates object

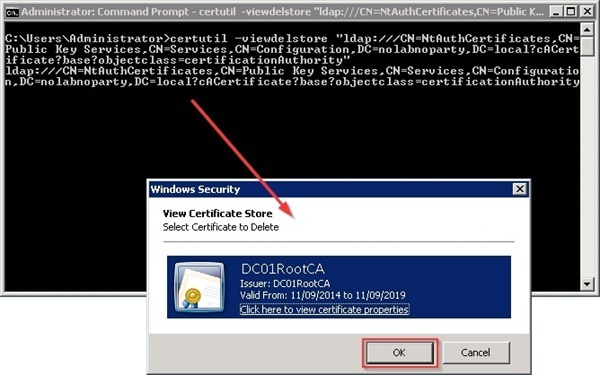
When CA objects are deleted, also the CA certificates published to the NtAuthCertificates object have to be deleted.

With Enterprise Administrator permissions, check the full LDAP path to the NtAuthCertificates object in Active Directory with the following command:

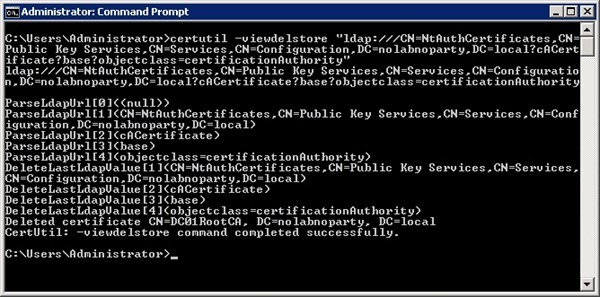
C:\>certutil -store -? | findstr "CN=NTAuth"



C:\>certutil –viewdelstore “ldap:///CN=NtAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=nolabnoparty,DC=local?cACertificate?base?objectclass=certificationAuthority”

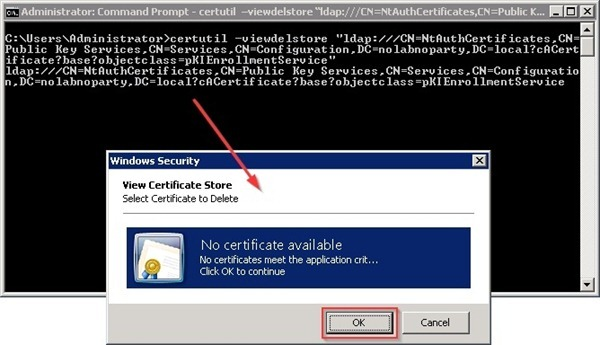


Click OK to delete the certificate.

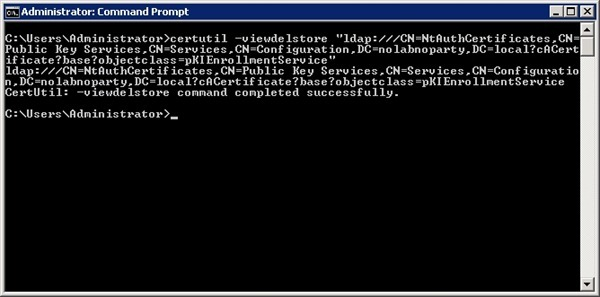


Now run the following command:

C:\>certutil –viewdelstore “ldap:///CN=NtAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=nolabnoparty,DC=local?cACertificate?base?objectclass=pKIEnrollmentService”

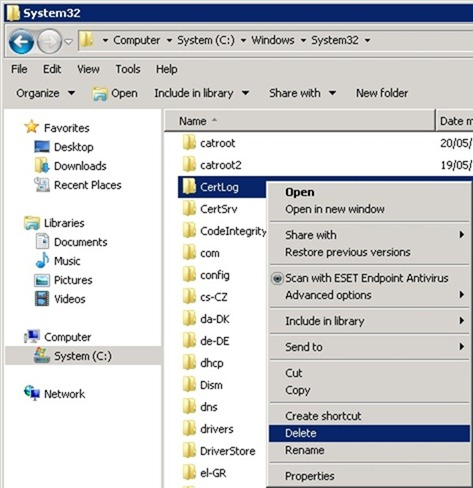


Click OK to delete the certificate.



Delete the CA database

Since the database is not removed during the Certification Services uninstall process, to remove the database delete the %systemroot%\System32\Certlog folder.



Remove certificates from DCs

Also the certificates that were issued to Domain Controllers must be removed.

On a Domain Controller, open the Command Prompt and type the command:

C:\>certutil -dcinfo deleteBad



Certutil tries to validate all the DC certificates that are issued to the domain controllers. Certificates that do not validate are removed. The Active Directory Certificate Services has been removed from the Active Directory successfully.

notes:certutil –delkey le-DomainController-b48c7ee1-d400-4b69-af19-6810bf38d263

you're removing the wrong key - i.e. not the CA private key. You should check the private key name with a command like:

certutil -key -csp "Microsoft Software Key Storage Provider"

and then remove it with

certutil -csp "Microsoft Software Key Storage Provider" -delkey ""