Generating CSR in Exchange 2013 EAC

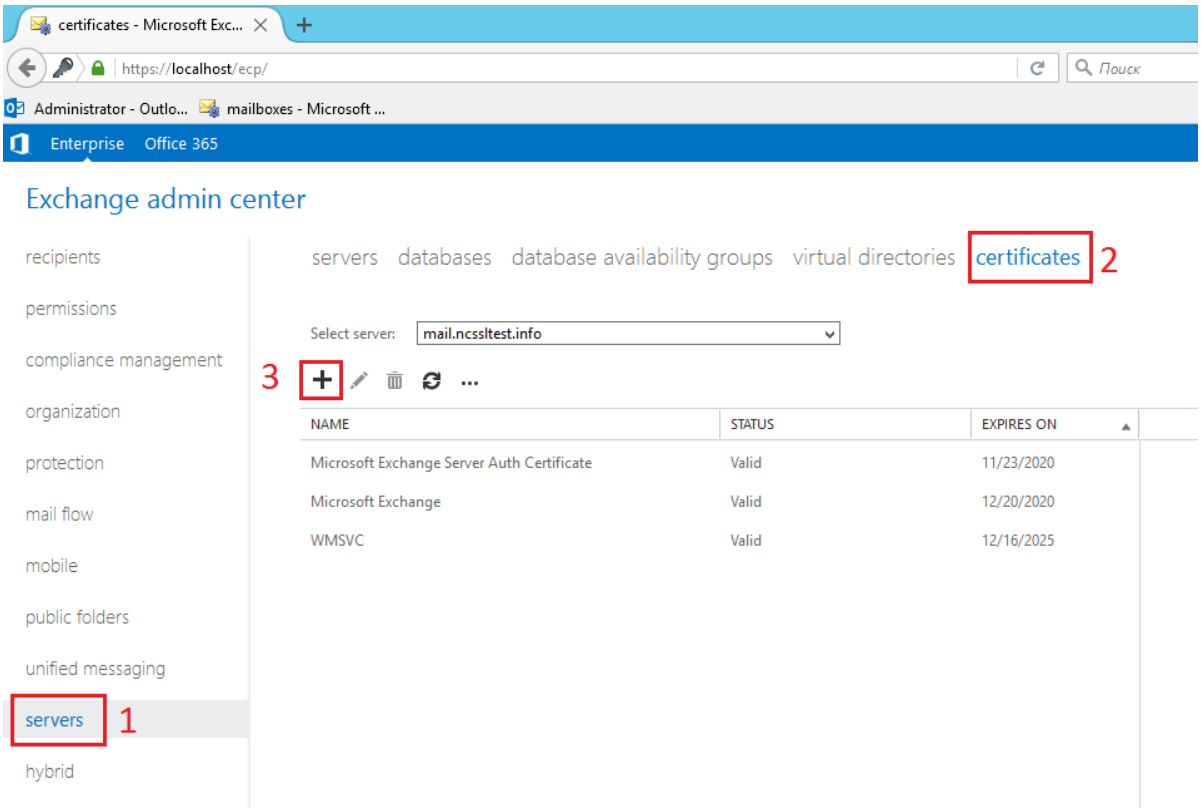
This article will describe the steps needed to generate a CSR in Exchange 2013 using the tools accessible through a browser.

In this example, we are generating the CSR on the server called MAIL for the domains *mail.ncssltest.info*, *ncssltest.info* and *autodiscover.ncssltest.info*.

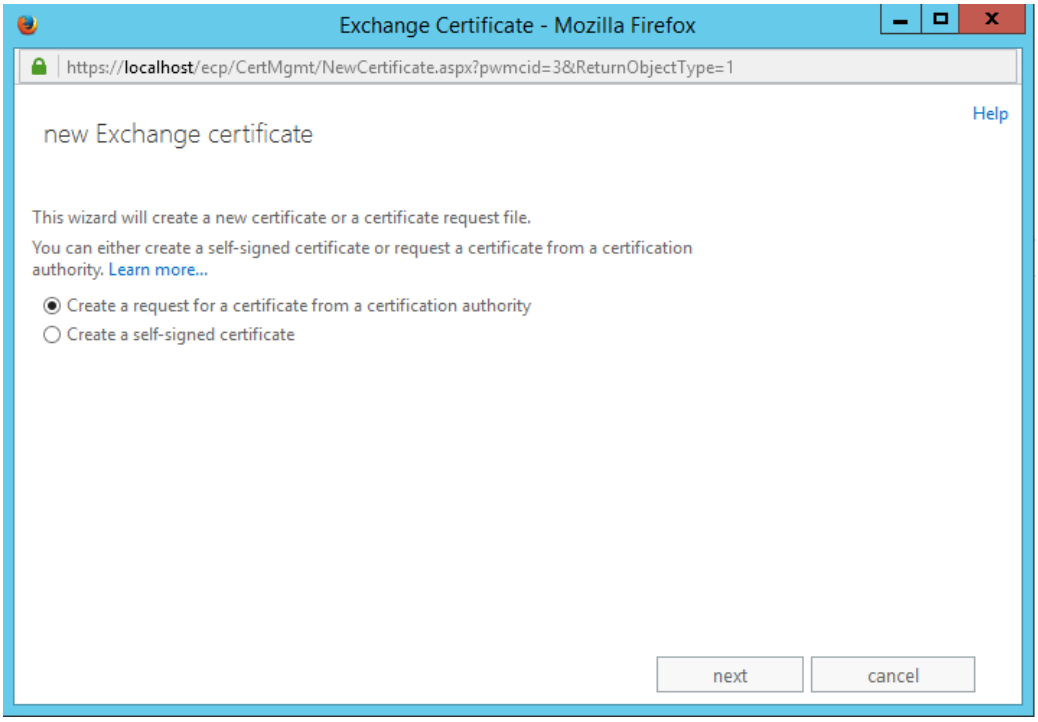
While setting up the Exchange server, you can specify the same subdomain "mail" for most services, such as OWA (Outlook Web Access) or OAB (Offline Address Book). For Autodiscover services, the subdomain "autodiscover" is typically used, and Outlook Anywhere is usually accessible via subdomain "oa".

The Certificate Signing Request is generated in Exchange Administration Center.

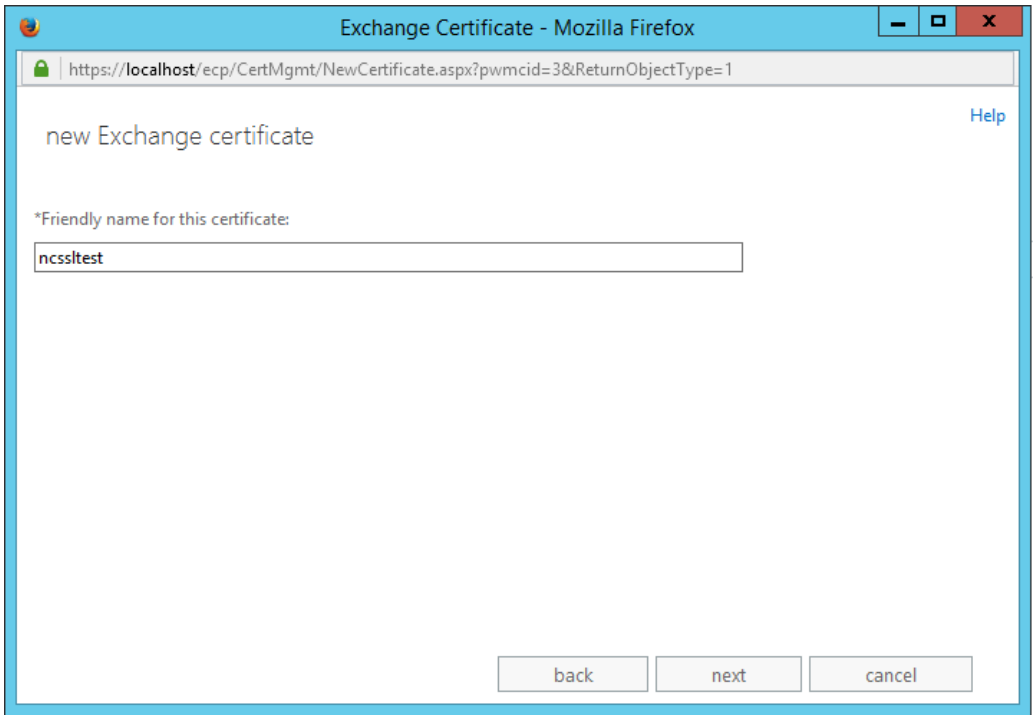
1. First, open your Exchange Administration Center in the web browser (usually done via https://localhost/ecp) and navigate to **Servers** > **Certificates**. Then click on the "+" button to open the Exchange certificate wizard.



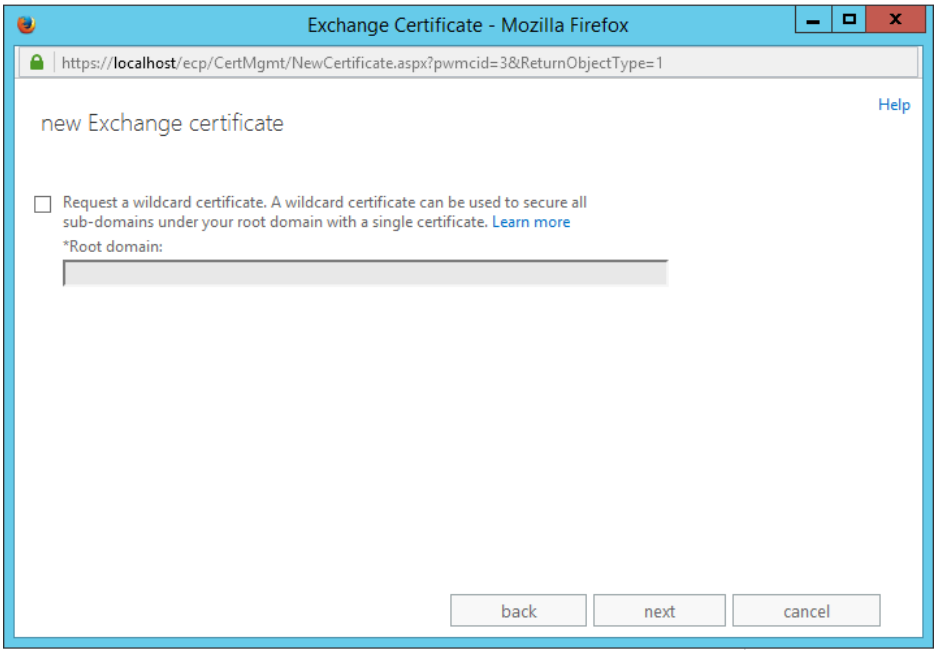
2. Choose "**Create a request for a certificate from a certification authority**" and click Next.



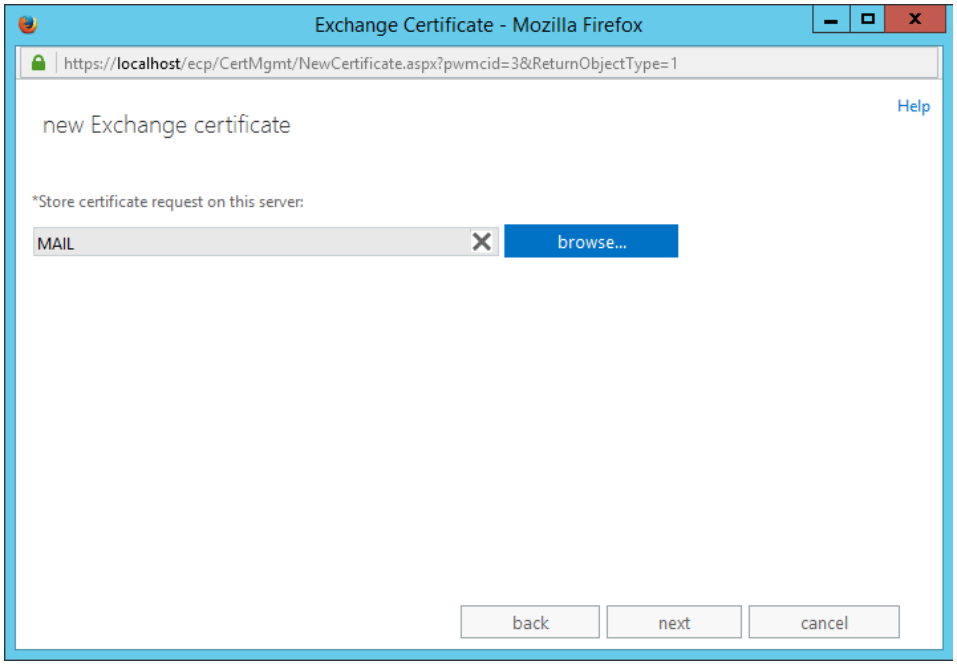
3. Give your certificate a **Friendly name** and click Next to continue. The friendly name is created for the server administrator to identify the certificate later. It is not the domain name itself.



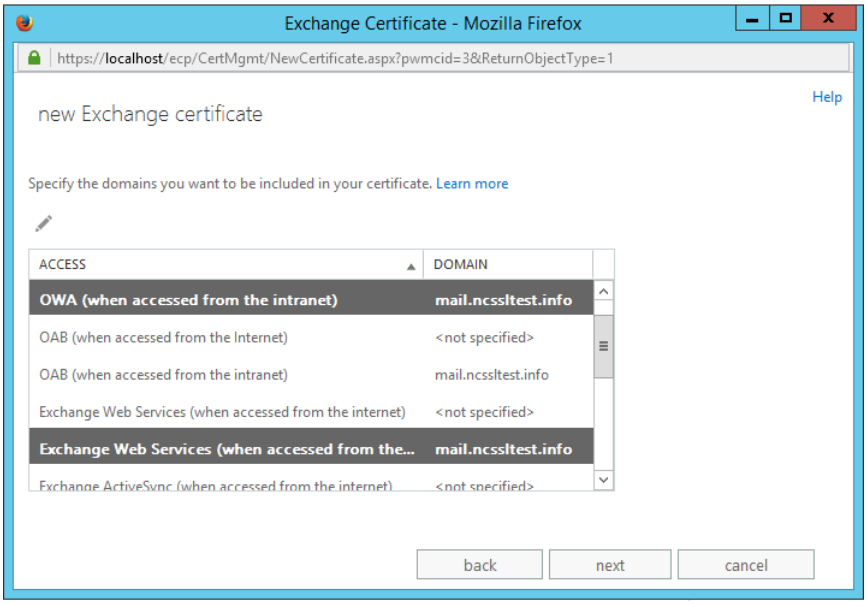
4. In the next step, you will be given the option to create a CSR for a **Wildcard** domain. Although Wildcard certificates are accepted and supported by Exchange 2013, they are not recommended as they may be not compliant with other server products which do not support them. If you are using a multi-domain (aka other names - SAN or UCC) certificate, you can skip this step by clicking **Next**.



5. Click **Browse** and select the **Exchange server** where the pending CSR will be stored on, then click **Next**.

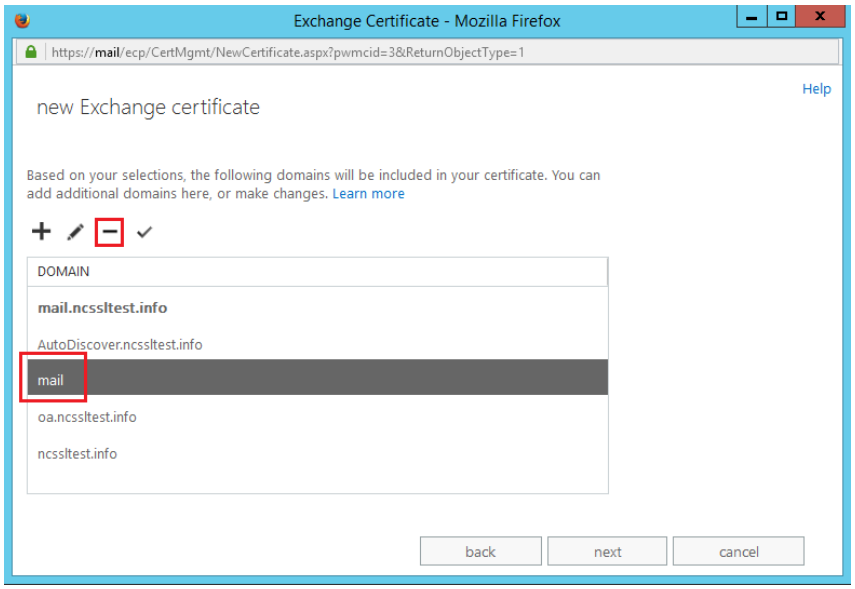


6. From the list, select the **services** to be secured with the certificate using Ctrl+Click. The step should be omitted for Wildcard certificates.

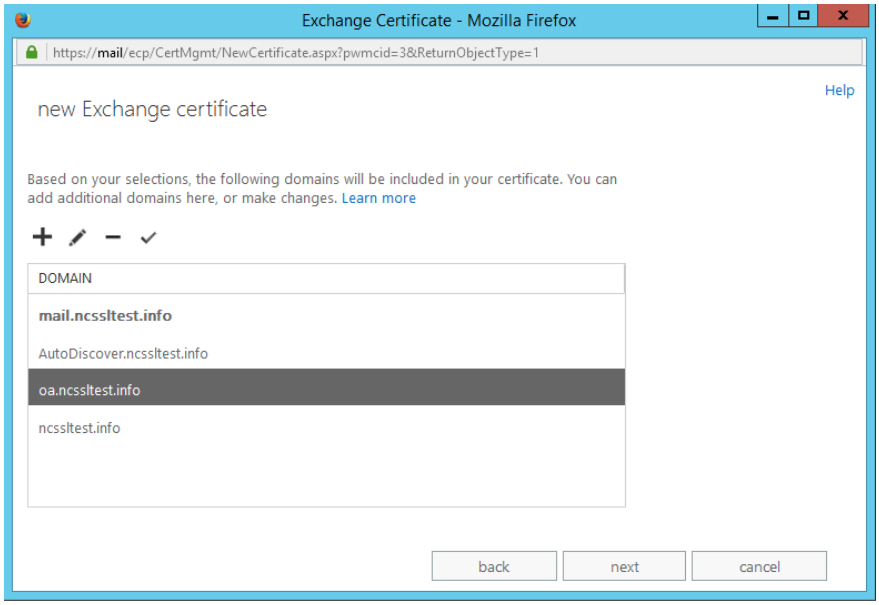


7. On the next screen, you can review the **list** of domains/subdomains which will be included in your certificate. If different services are using the same subdomain, it will be shown in the list only once. Extra domains can be added using the "+" button if needed.

Note: The server internal name is added to the list by the server. Various other names may also appear, depending on how the previous step was completed. Due to the restrictions of CA/Browser forum, the Certificate Authorities do not issue certificates for internal/local domain names. Remove the internal domain name from the list using the "-" button.

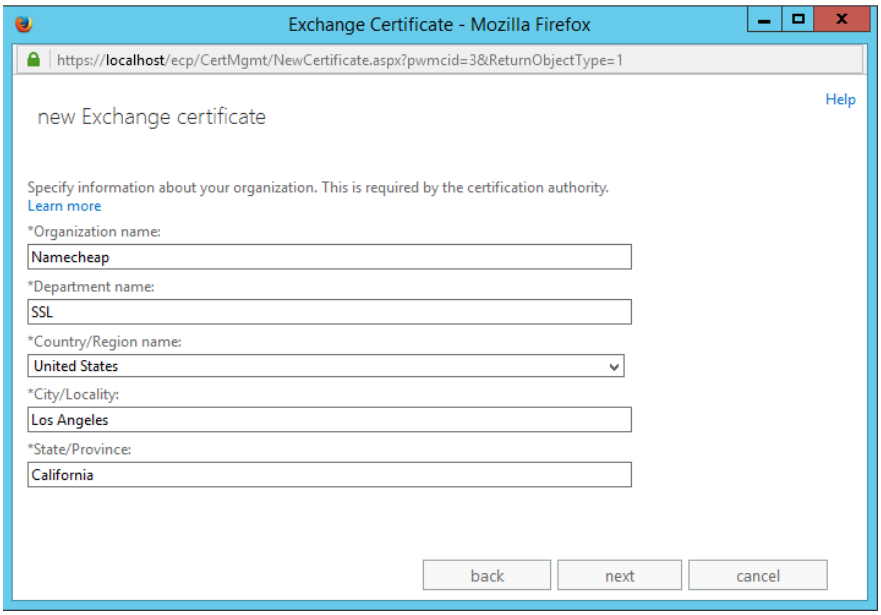


8. After the list of names has been reviewed and edited according to your preferences, click **Next**.

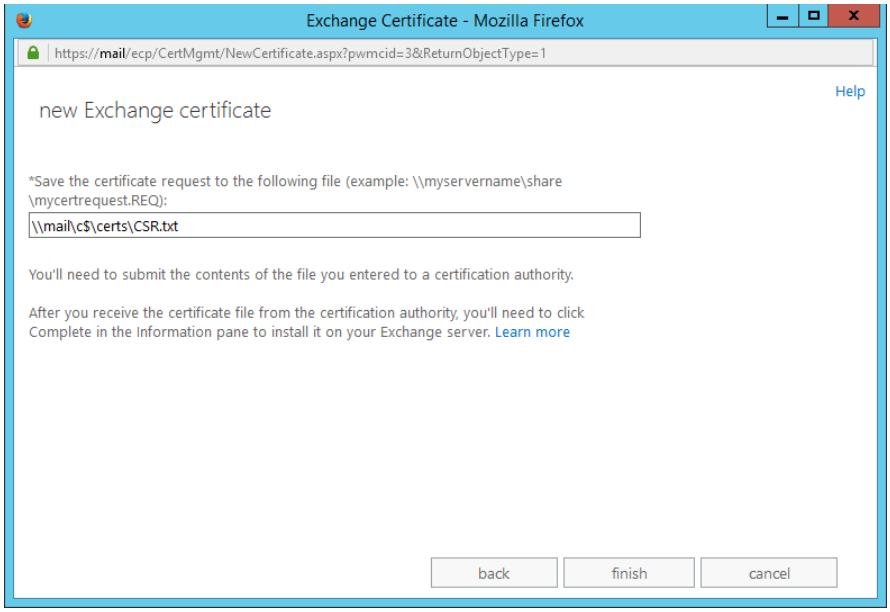


9. In this step, you will fill in the **organization** details. Short descriptions of these fields are listed below:
    - *Organization name*: the name of your company. If the certificate is not being used for a company or organization, you may enter "NA". In most cases, domain-validated certificates are sufficient for the Exchange server so this will not cause any issues.
    - *Department name*: the department within your organization. "NA" can be also used here if there is no department in your company.
    - *Country/Region name*: select your country from the drop-down list. This field refers to the country in which your domain is registered/operating.
    - *City/Locality*: the full name of your city.
    - *State/Province*: the full name of your state or province. You may re-enter the city name if there are no states or other regional identifiers in your country.

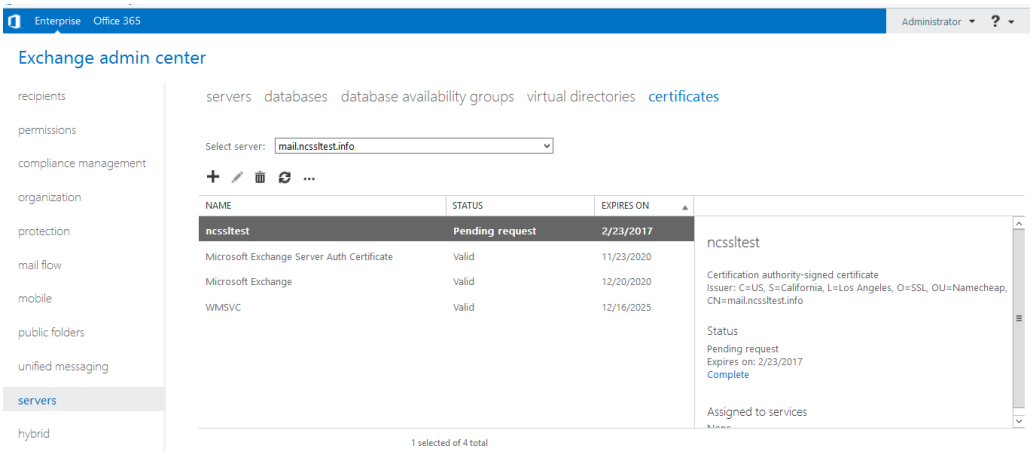
Note: All fields should contain only alphanumeric symbols (A-Z, a-z, 0-9); special characters ("&", "/", "^", "â", etc.) are not allowed.



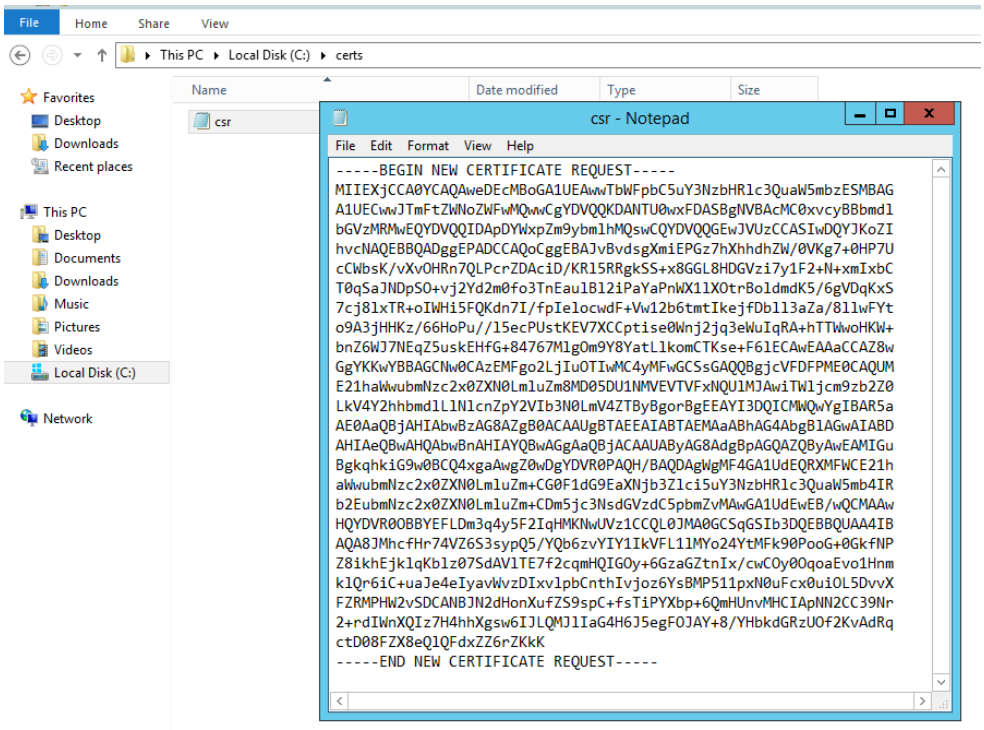
10. Enter a **path** to the folder on your computer in which the CSR will be saved. In this example, the file will be saved in the "certs" folder on the disk C://. **Note**: the destination folder should be created in advance. The system offers to save the file with .req extensions; however you will need only its text, so you are free to use .txt extension.



11. After clicking **Finish**, you will see your **pending** certificate request in the Certificates menu.



12. The file can then be found in your computer using the path that was specified in the step 10. Please use the whole text (including Begin and End headers) for certificate activation.



13. After the certificate is issued by the Certificate Authority, you will be able to install it using this guide.