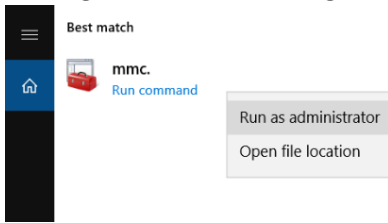
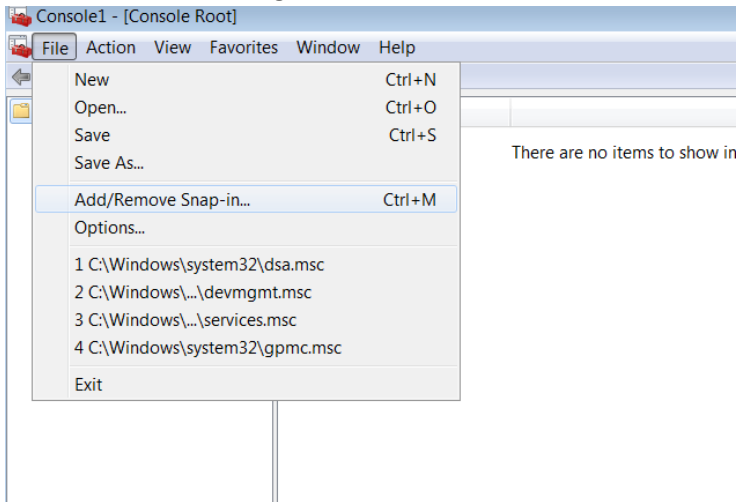


How to Generate a Certificate Signing Request on a Windows Server

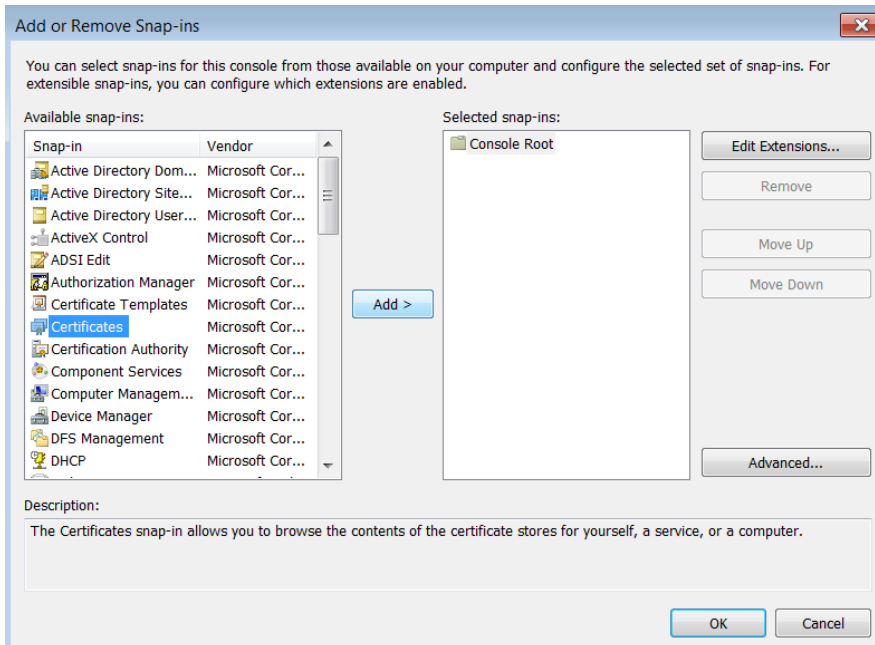
1. Launch the Microsoft Management Console (MMC) by clicking the Start button, typing “mmc.”, right-clicking **mmc.**, and selecting Run as administrator:



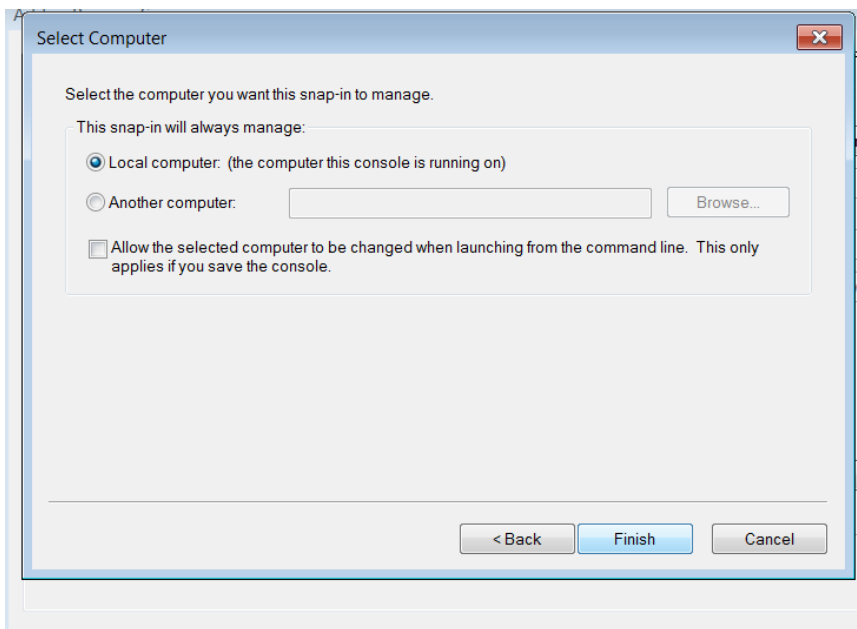
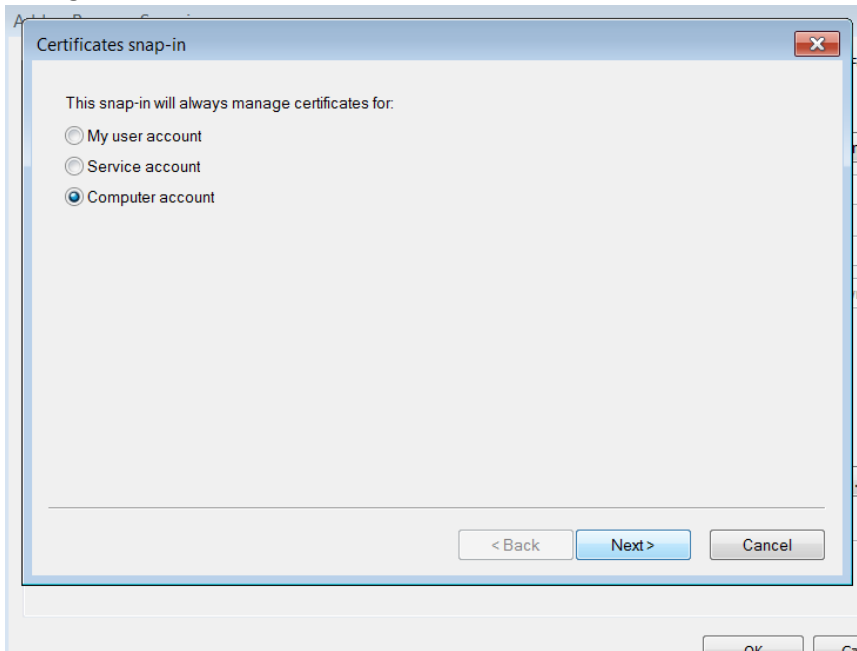
2. In the Microsoft Management Console, select File and then Add/Remove Snap-in...



3. Select Certificates from the list on the left and click Add in the center

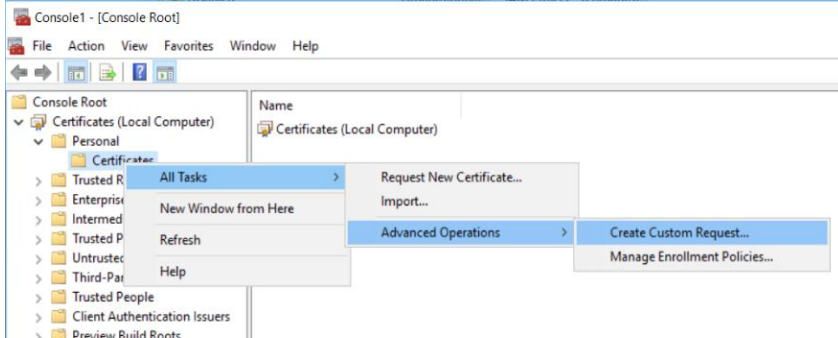


4. In the next Dialog Box select Computer account, click Next, and Finish for Local Computer on the next Dialog Box.

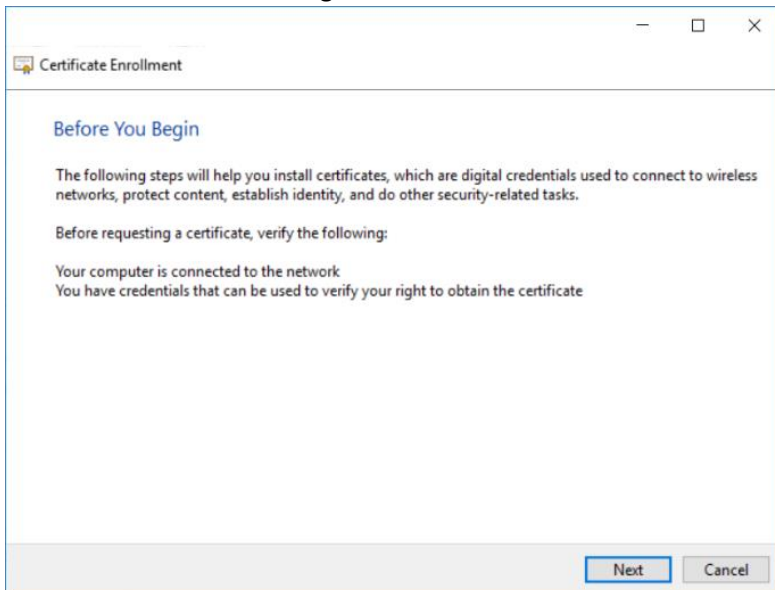


5. Finally click OK to close the Add or Remove Snap-ins Dialog Box.

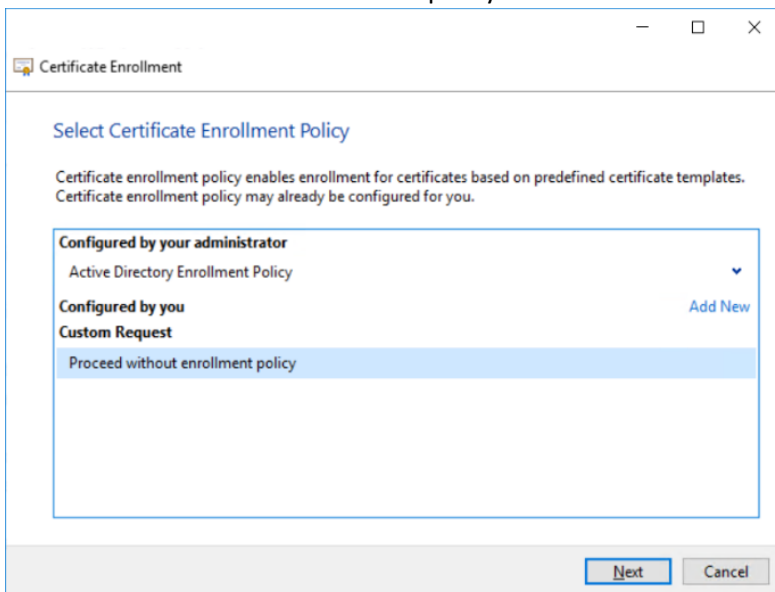
6. Expand Certificates and Personal on the left pane and then right-click Certificates under Personal. Select All Tasks, Advanced Operations, and Create Custom Request...:



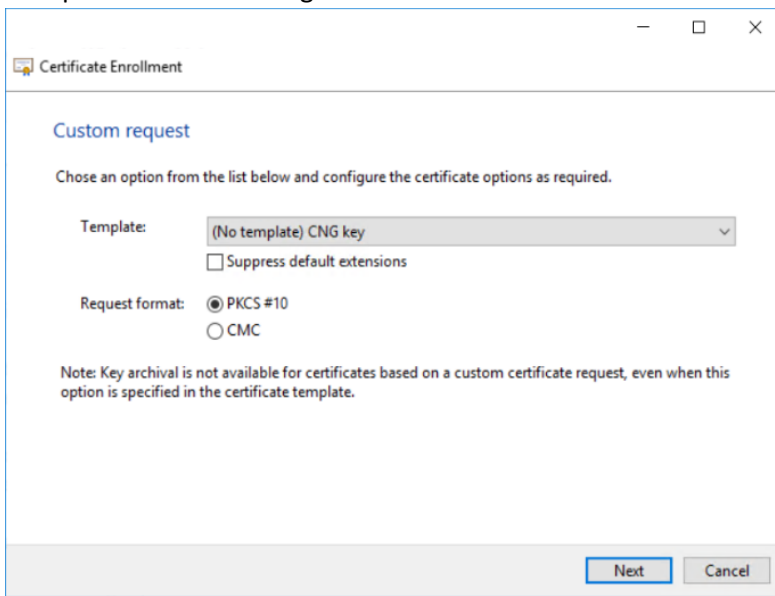
7. Click Next in the first Dialog Box for the Certificate Enrollment Wizard:



8. Select Proceed without enrollment policy and click Next:

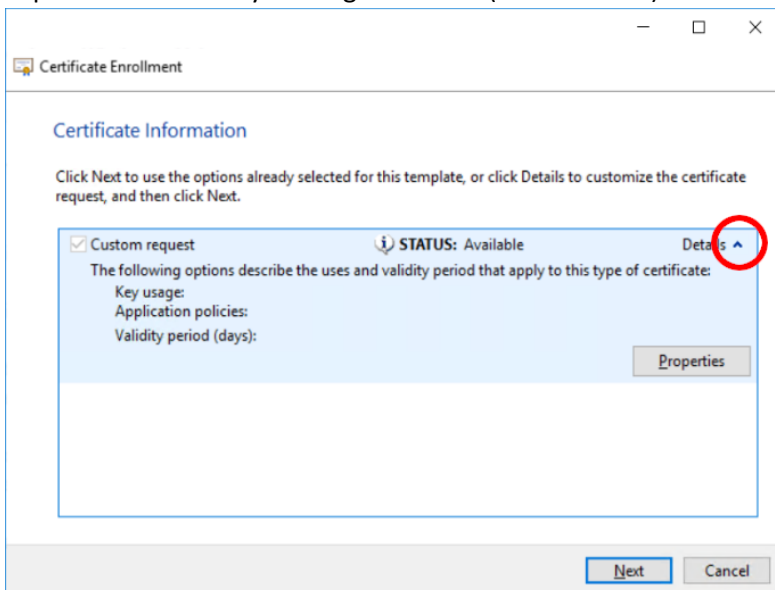


9. Accept the default settings and click Next:



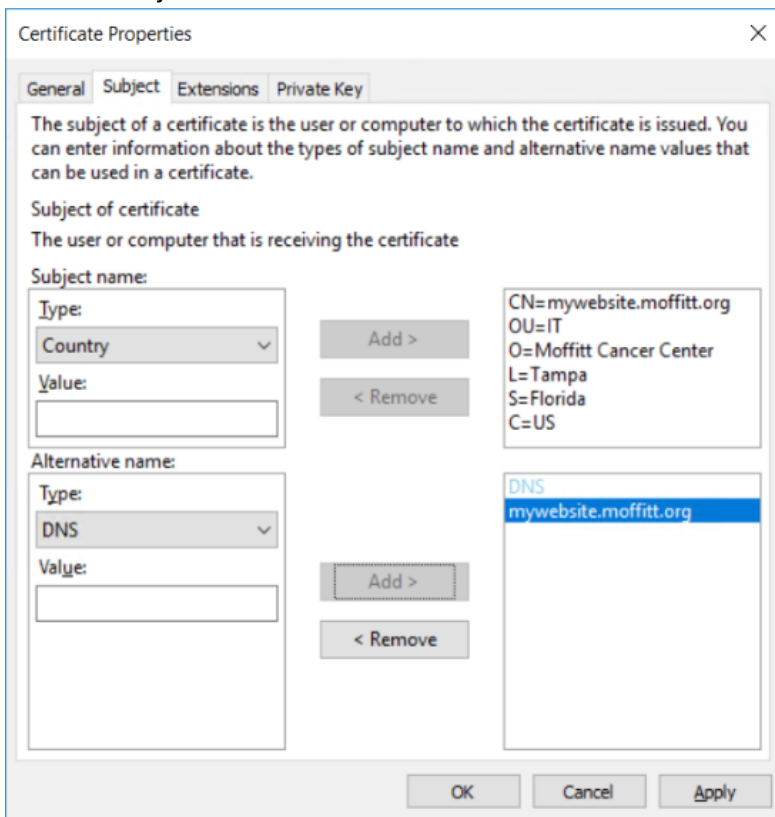
The dialog box is titled "Certificate Enrollment" and contains a section titled "Custom request". Below this title, it says "Chose an option from the list below and configure the certificate options as required." There are two main settings: "Template:" with a dropdown menu showing "(No template) CNG key" and a checkbox "Suppress default extensions" which is unchecked; and "Request format:" with two radio buttons, "PKCS #10" (which is selected) and "CMC". A note at the bottom states: "Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template." At the bottom right, there are "Next" and "Cancel" buttons.

10. Expand the Details by clicking the arrow (circled in red) and then click Properties:



The dialog box is titled "Certificate Enrollment" and contains a section titled "Certificate Information". It says "Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next." Below this, there is a blue-bordered box containing a checked checkbox "Custom request", a status icon and text "STATUS: Available", and a "Details" link with a small upward-pointing arrow (circled in red). Below the "Details" link, it says "The following options describe the uses and validity period that apply to this type of certificate:" followed by three lines of text: "Key usage:", "Application policies:", and "Validity period (days):". A "Properties" button is located to the right of this text. At the bottom right of the dialog, there are "Next" and "Cancel" buttons.

11. Click the Subject Tab and fill out the fields as below:



The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate
The user or computer that is receiving the certificate

Subject name:

Type: Country
Value:

Alternative name:

Type: DNS
Value:

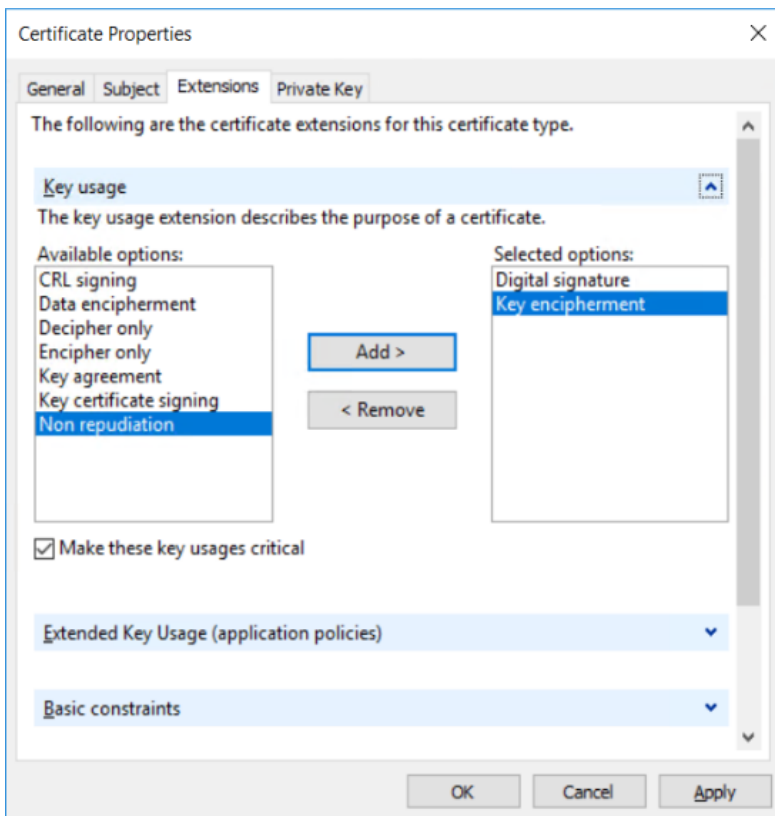
Add > < Remove

CN=mywebsite.moffitt.org
OU=IT
O=Moffitt Cancer Center
L=Tampa
S=Florida
C=US

DNS
mywebsite.moffitt.org

OK Cancel Apply

12. Click the Extensions Tab and fill out the fields as below:



The following are the certificate extensions for this certificate type.

Key usage
The key usage extension describes the purpose of a certificate.

Available options:

CRL signing
Data encipherment
Decipher only
Encipher only
Key agreement
Key certificate signing
Non repudiation

Add > < Remove

Selected options:

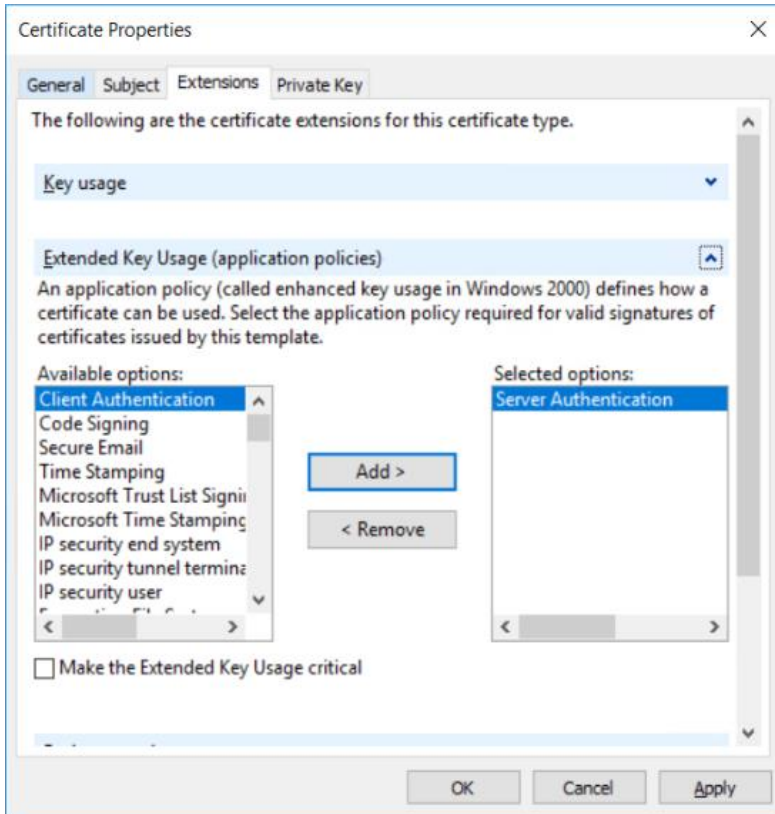
Digital signature
Key encipherment

☒ Make these key usages critical

Extended Key Usage (application policies)

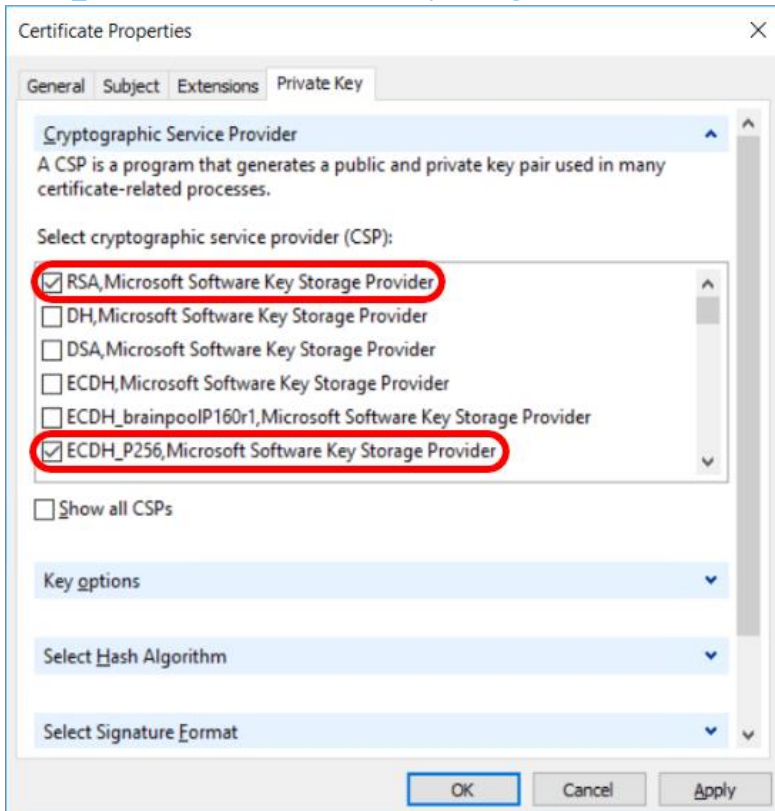
Basic constraints

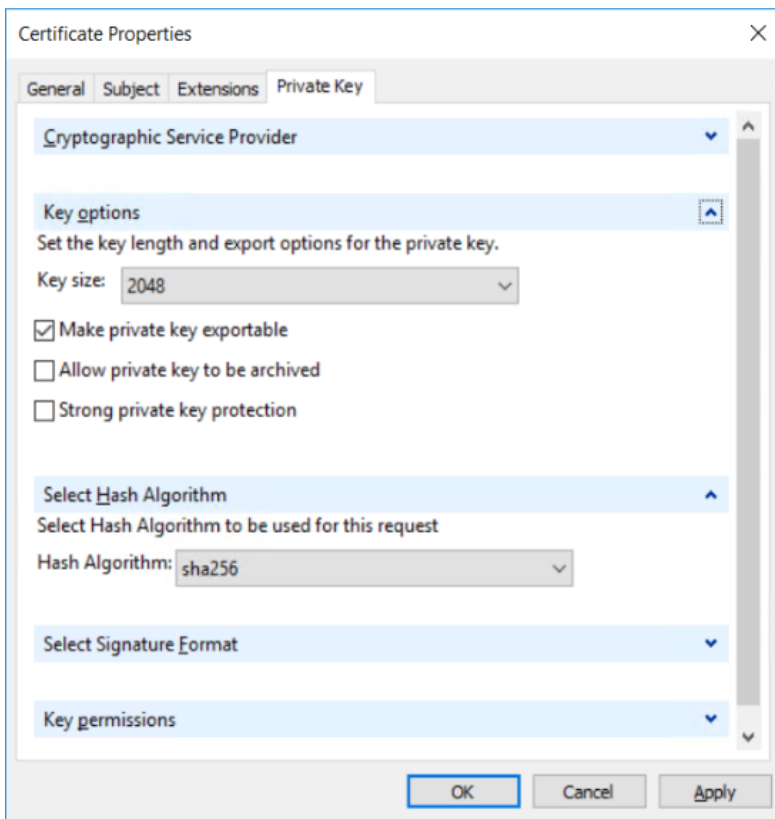
OK Cancel Apply



13. Click the Private Key Tab and fill out the fields as below:

Cryptographic Service Provider should be [RSA, Microsoft Software Key Storage Provider](#) (preferred) **OR** [ECDH_P256, Microsoft Software Key Storage Provider](#):





14. Click OK to accept the settings. Click Next in the Certificate Enrollment Wizard. Select the location to store the file and give it a name, accept the other defaults settings and click Okay.
15. Create a ticket in ServiceNow and attach the generated file. Assign the ticket to Unified Communications.