# Create a CSR with SHA256 signature algorithm

imkottees

As all security partners have already made SHA-256 the default for all new SSL Certificates issued, and strongly recommends that all customers re-key their SHA-1 certificates to avoid possible warnings online due to the phase out of SHA-1 trust by Microsoft, Google, and Mozilla.

I had to submit a CSR file for renewing my Exchange 2010 internal CAS servers. But when I created a certificate request using Exchange PowerShell it creates with SHA1 by default. Then found a way to create a CSR with SHA256 using certificate management console. Just thought of sharing with you!

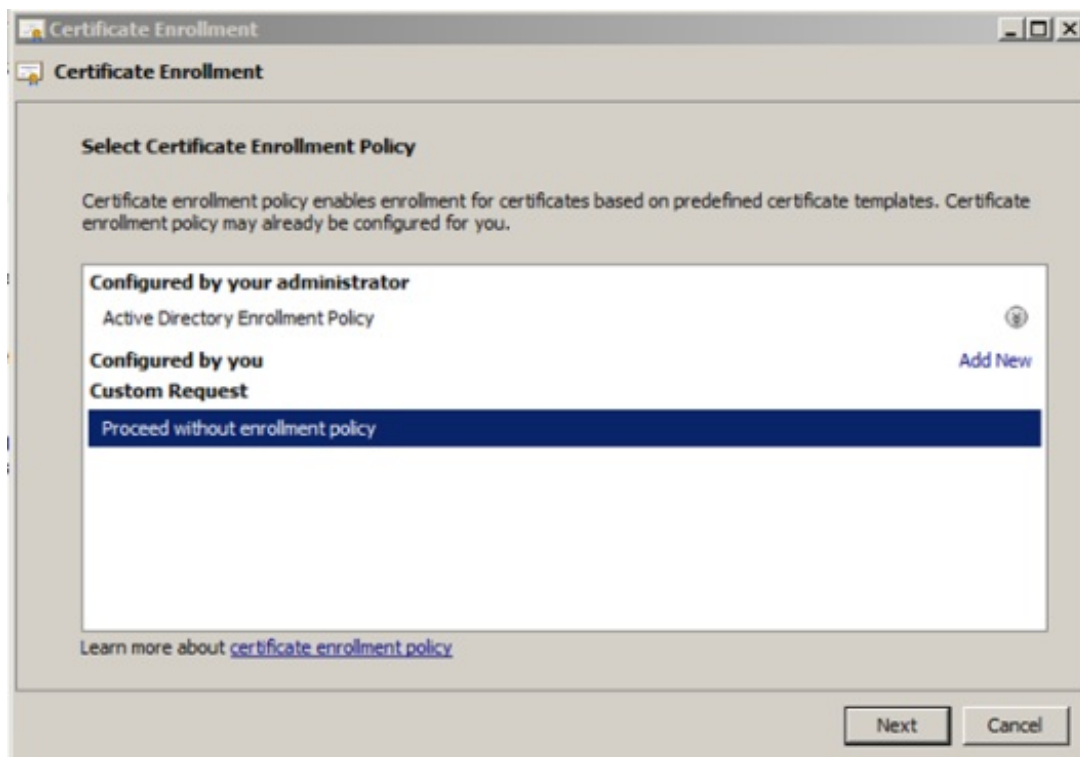You can use any windows machine to create this request, steps are below.

Go to start à Run à MMC à File à Add / Remove Snap-In à Certificates à Right Click à All Tasks à Advanced Operations à Create Custom Request
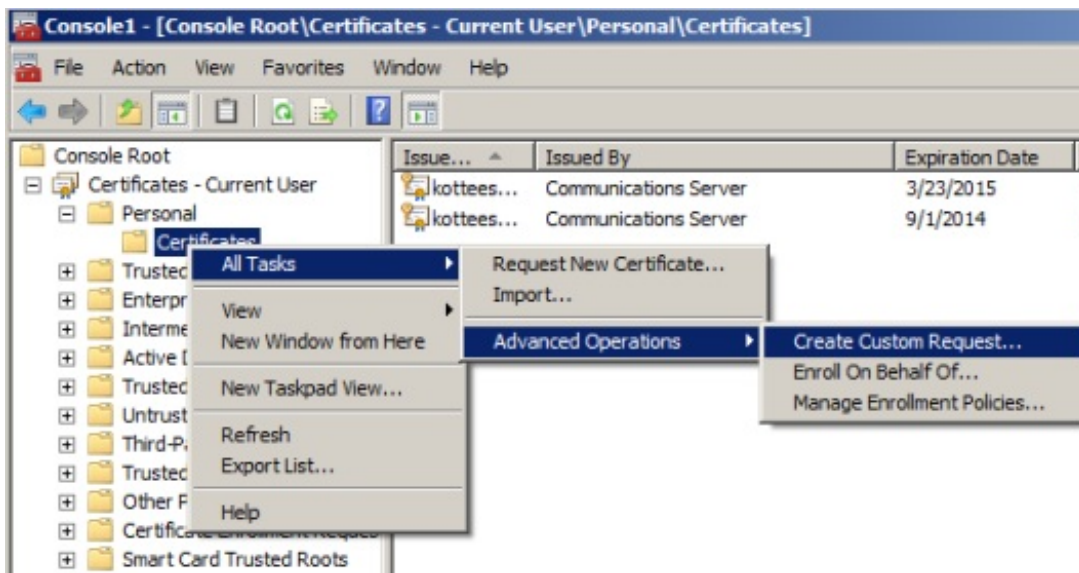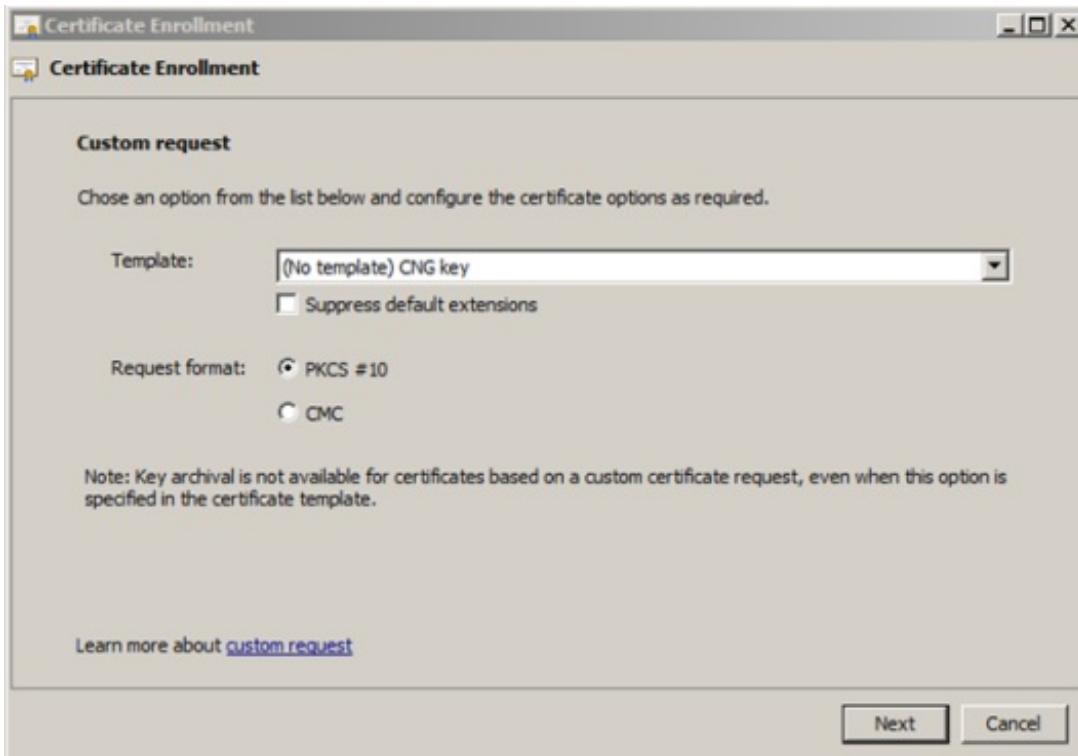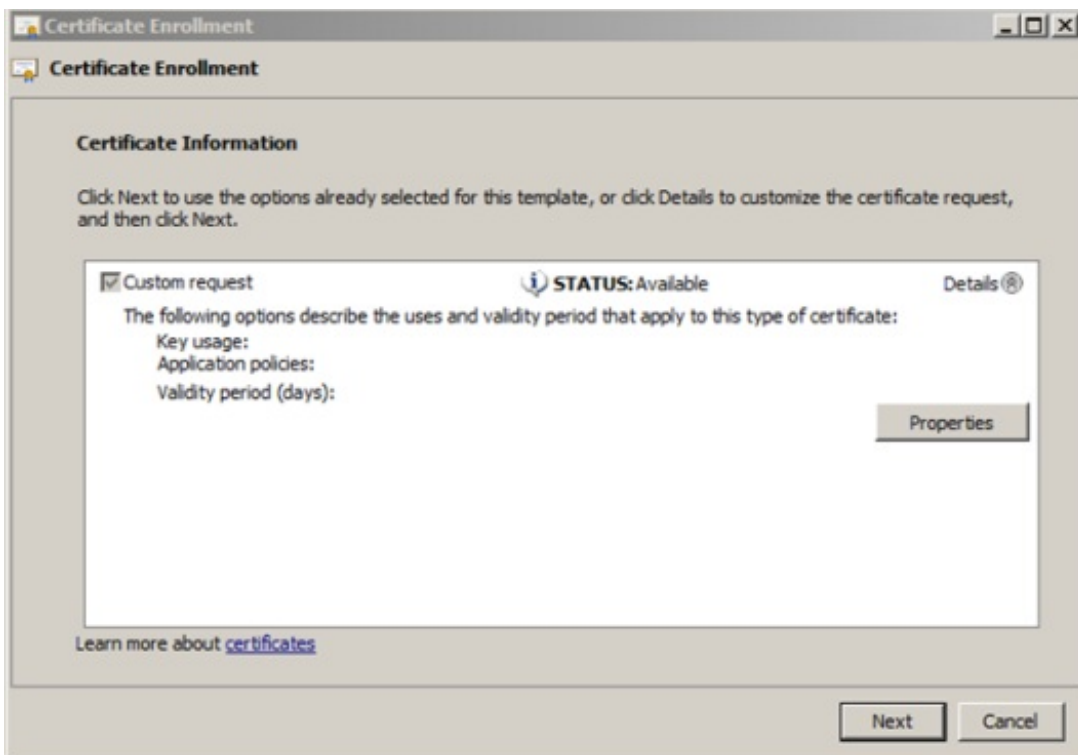

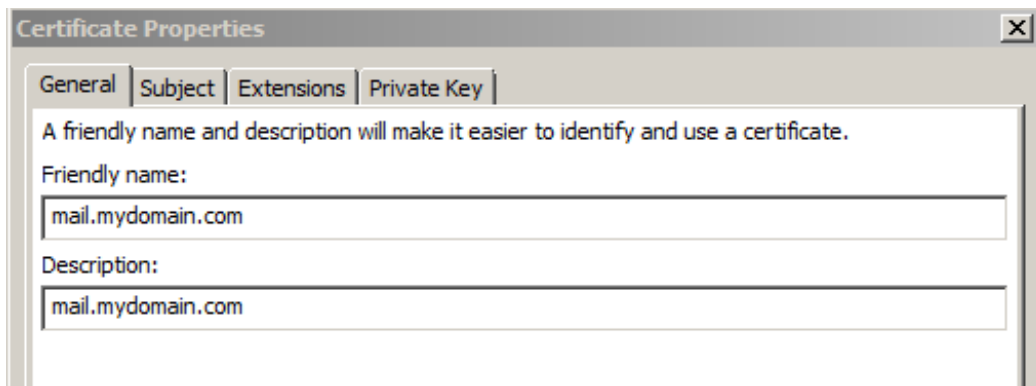Click Next à
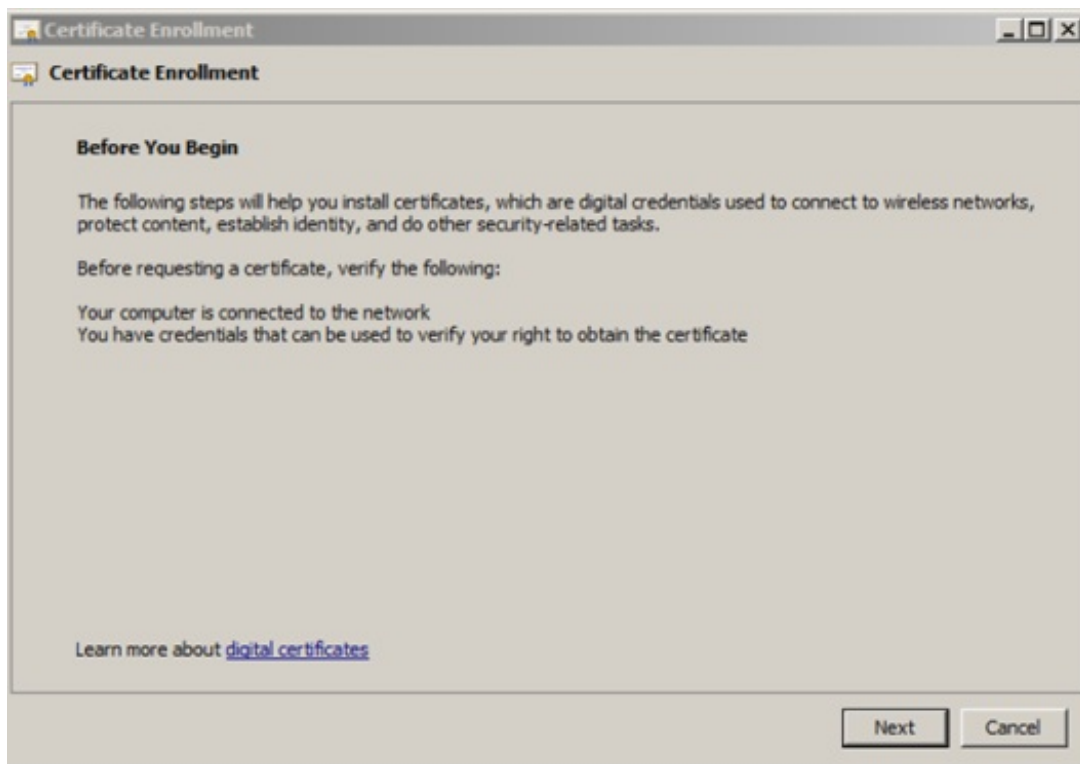
Select Custom Request à Next à
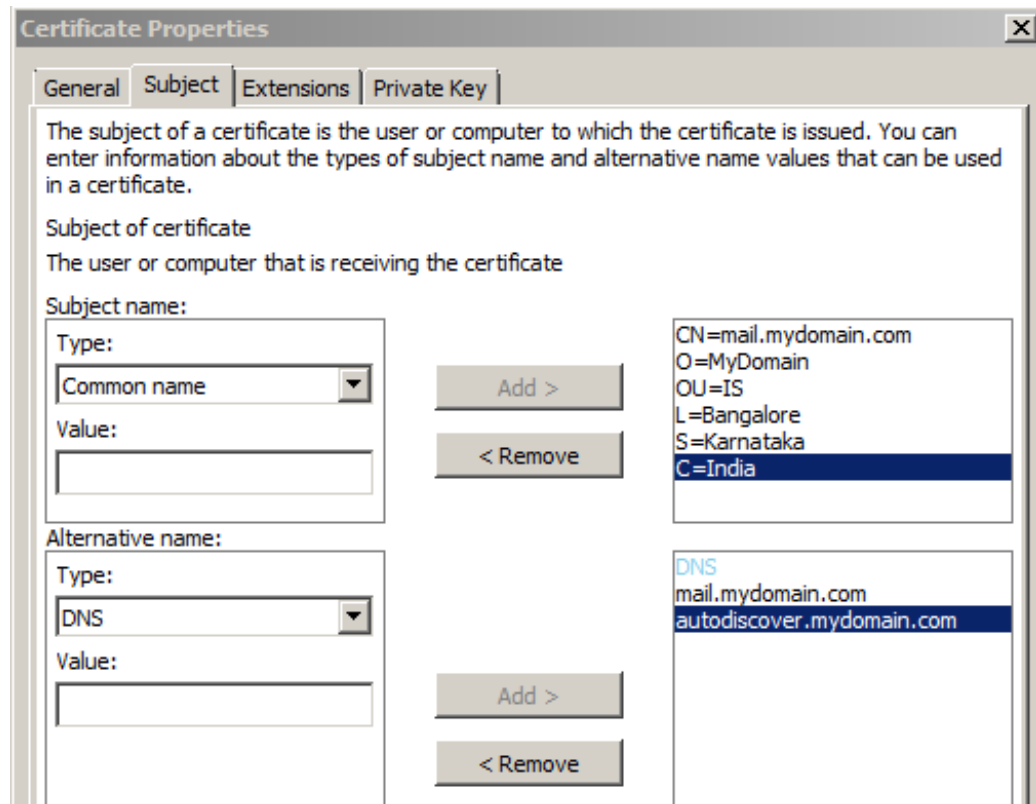
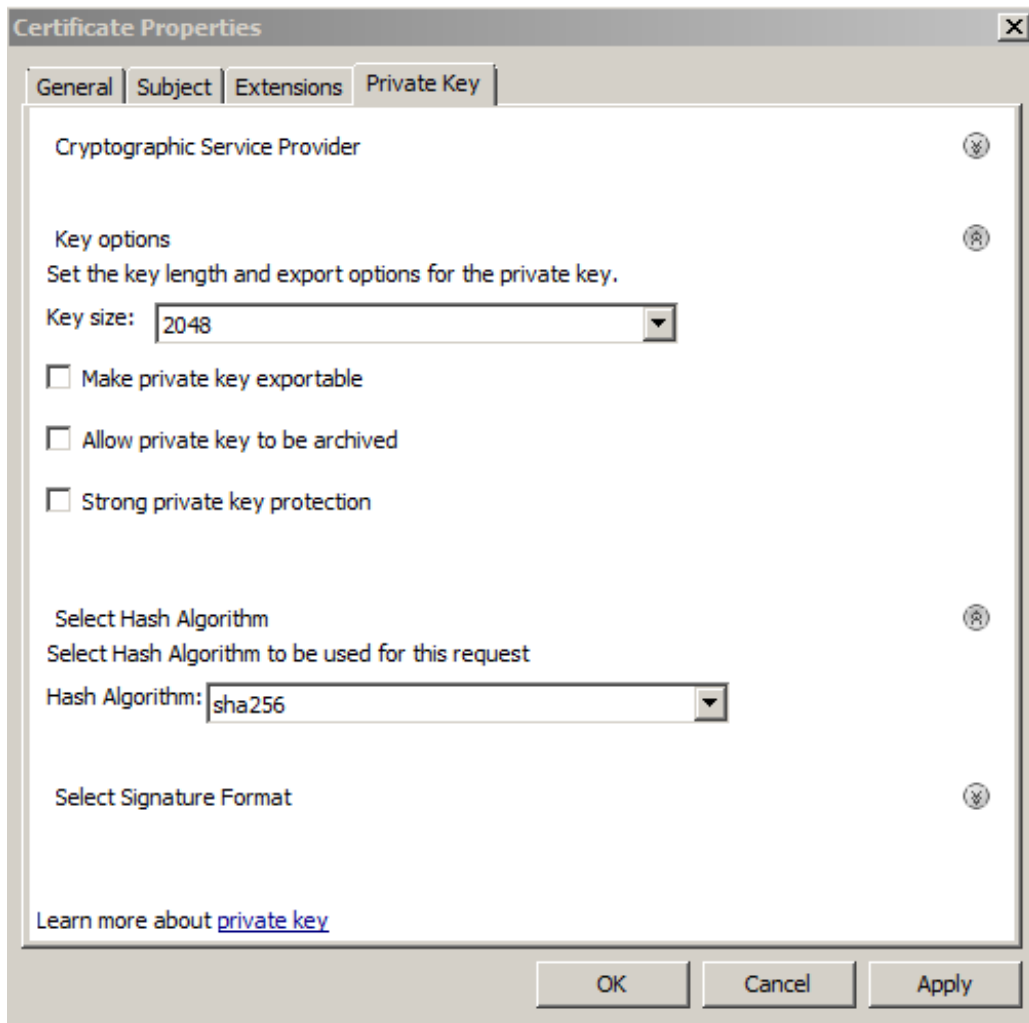

Choose PKCS #10 à Next

Click on Properties à Next

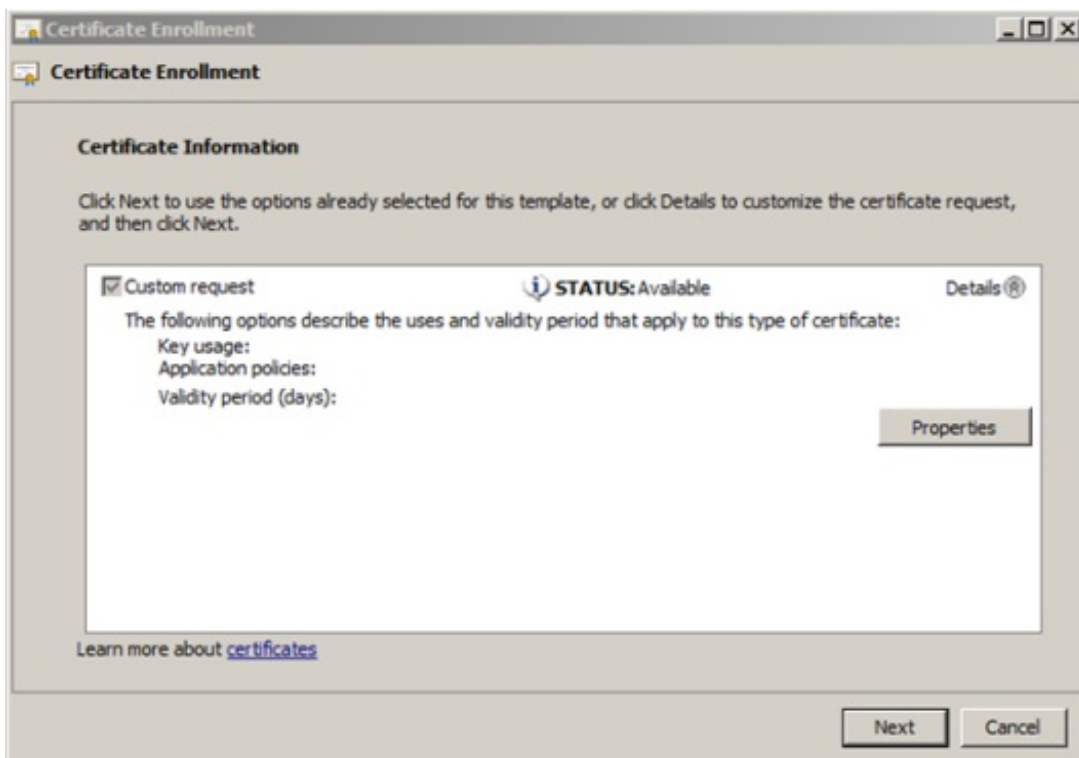Type your friendly name under general tab

Under subject tab add your Common Name, Organization, Organizational Unit, State, Country and SAN based on your need. Additional SAN names should be listed under DNS.
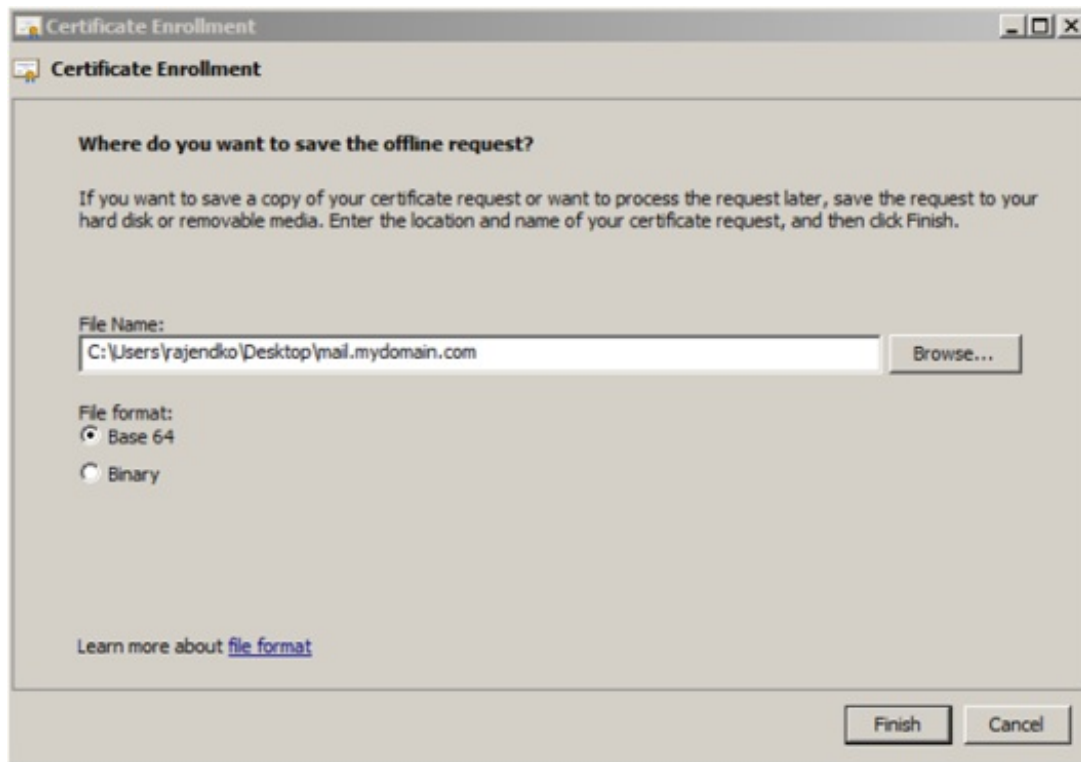

Under Private Key tab, choose Key size to 2048 and Signature Algorithm to SHA256 à Apply àOk

Next à

Choose path to save certificate request file à Finish

To verify the signature algorithm you can use below site.

https://ssltools.websecurity.symantec.com/checker/views/csrCheck.jsp

I hope you would have enjoyed this!!!

Signature algorithm: SHA256
Key algorithm: RSA
Key size: 2048