

How to request custom certificates using the MMC snapin

By Jakob Østergaard Nielsen | 2016-02-04

0 Comment

A common misundersand is that creating a Certificate Signing Request (CSR) can only be performed using tools like *Internet Information Service* (IIS) or the *Exchange Admin Center* console.

On any Windows computer, you can use the *Certificates* MMC snap-in to create custom certificate signing requests, including wildcard and multi-SAN certificates for web server authentication.

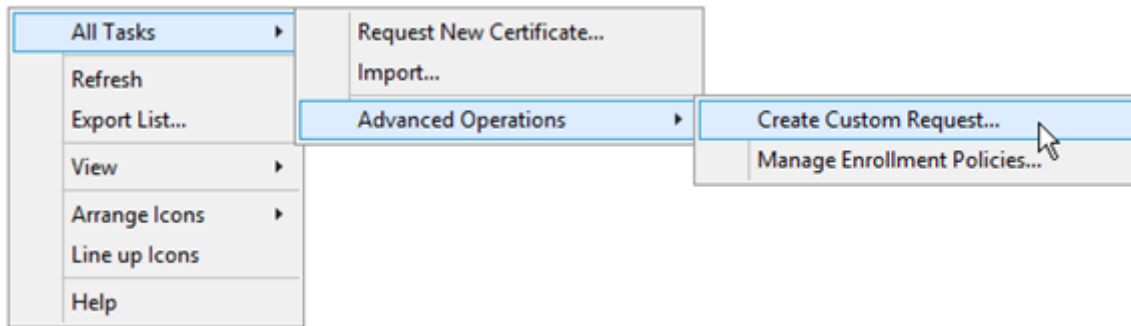
How do make a custom certificate signing request

First open the *Certificates* MMC snap-in:

1. Log on to any Windows computer, with an account that is a member of the local Administrators group.
2. Click **Start**.
3. In the **Search programs and files** box, type **mmc.exe**, and press **ENTER**.
4. On the **File** menu, click **Add/Remove Snap-in** or use the shortcut **Ctrl+M**.
5. In the list of available snap-ins, click **Certificates**, and then click **Add**.
6. Click **Computer account**, and click **Next**.
7. Click **Local computer**, and click **Finish**.
8. Click **OK**.
9. In the console tree, double-click **Certificates (Local Computer)**, and then double-click **Personal**.

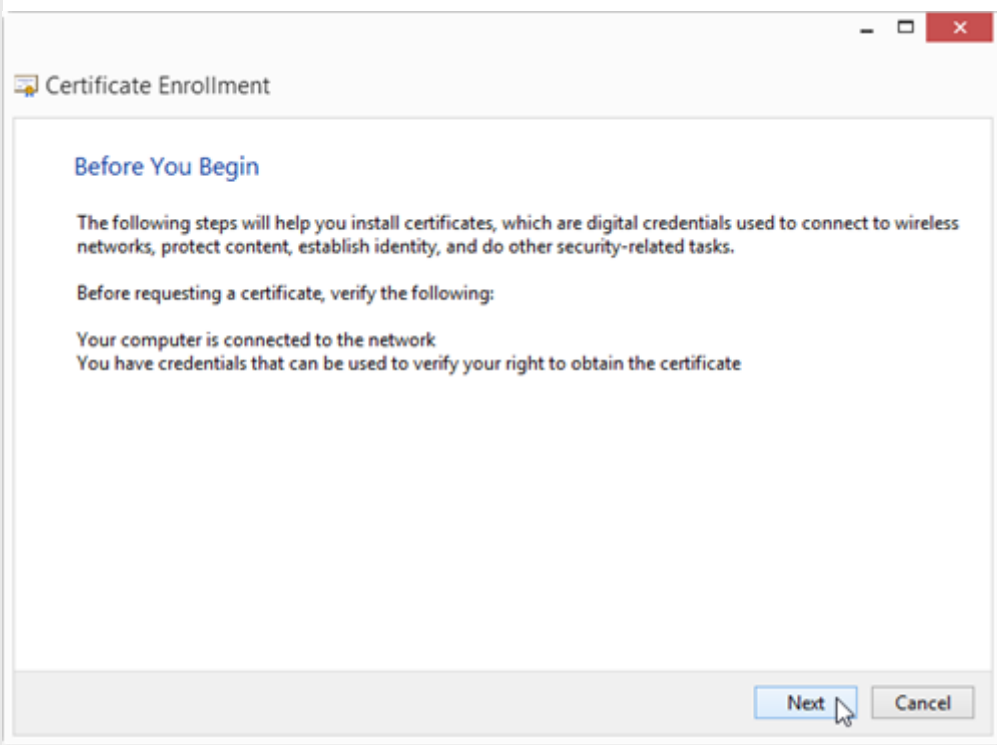
After you have added the *Certificates* snap-in for your local computer store, you can create a custom certificate request :

Right-click **Personal**, point to **All Tasks**, select **Advanced Operations** and click **Create Custom Request**

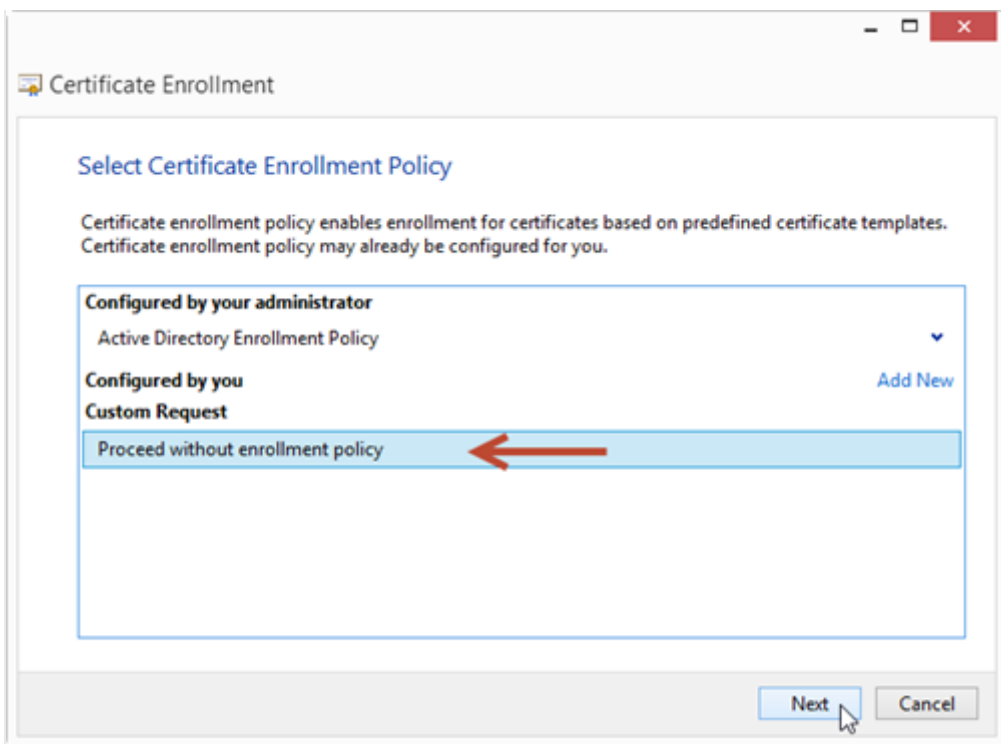


The *Certificate Enrollment* wizard now start.

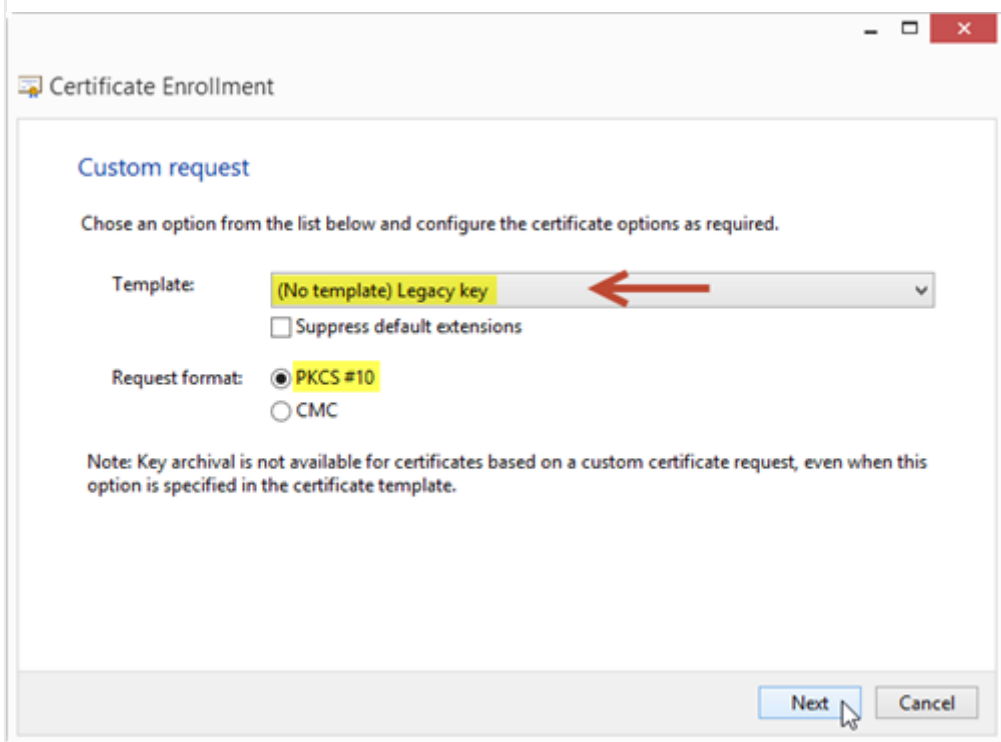
On *Before You Begin* page click **Next**



On the *Select Certificate Enrollment Policy* select **Custom Request, (Proceed without enrollment policy)** and click **Next**.



On *Custom Request* page under the *Template* options select **(No template) Legacy key** and select the **PKCS #10** request format option:



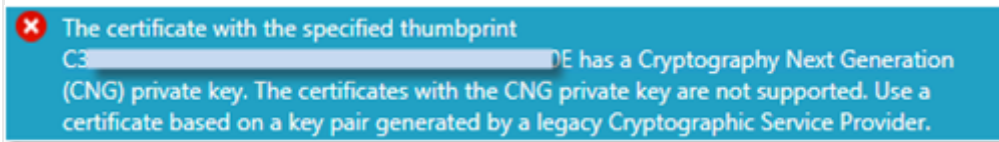
NOTE:

A range of systems and services does not support CNG based certificates, but require certificates to be based on a legacy CSP.

This website may use cookies for statistical purposes. By continuing to use this website, you agreed to this. [Cookie Policy](#)

Close and accept

ADFS:



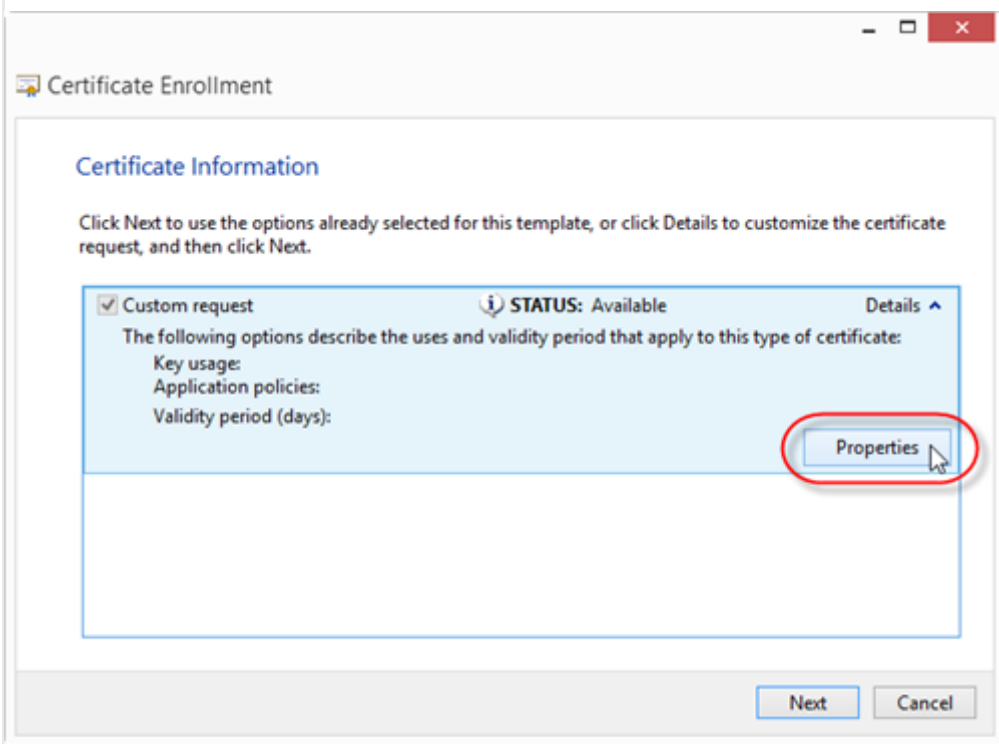
TMG:

Forefront TMG does not support the use of certificates created using CNG (Certificate New Generation) based templates for Web listeners or as client certificate authentication in Web publishing or Web chaining rules.

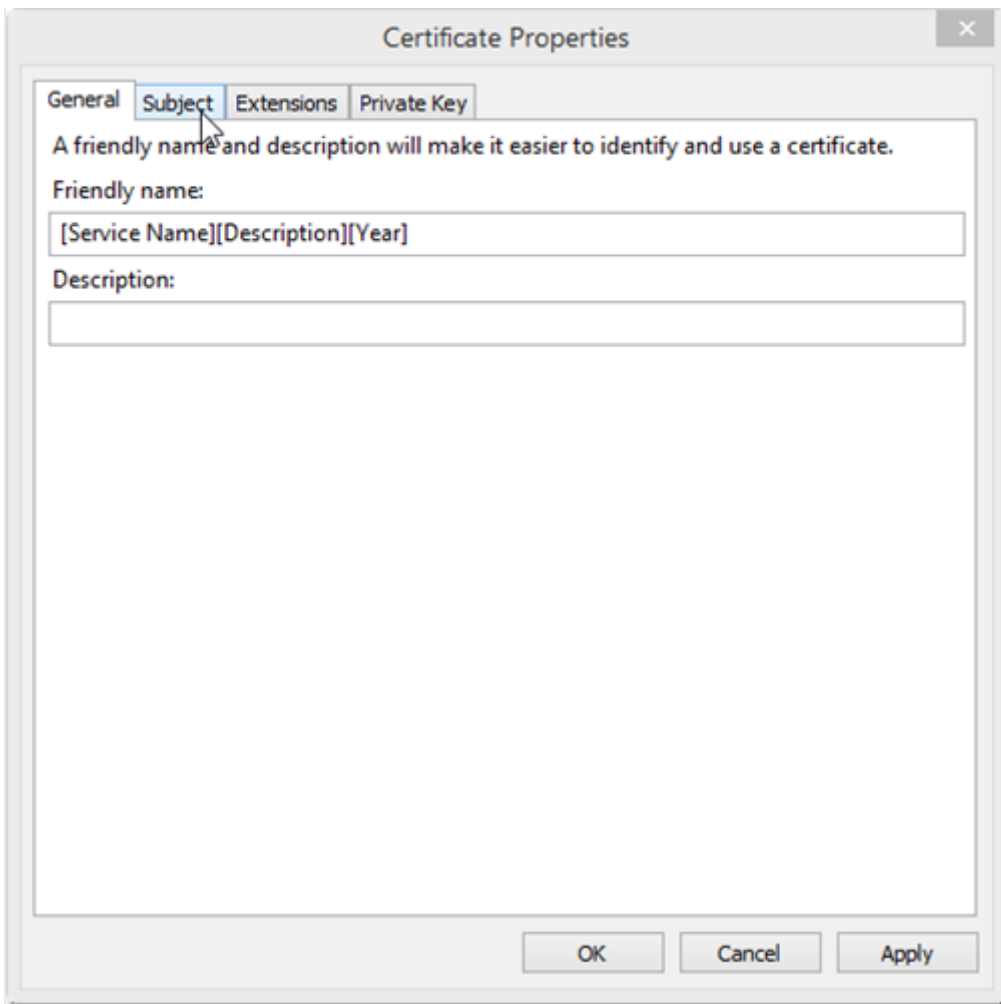
Microsoft Support statement on Forefront Threat Management Gateway (TMG):

<https://technet.microsoft.com/en-us/library/ee796231.aspx#dfg9o9i8uuy6tre>

On *Certificate Information* click **Details** and click **Properties** :



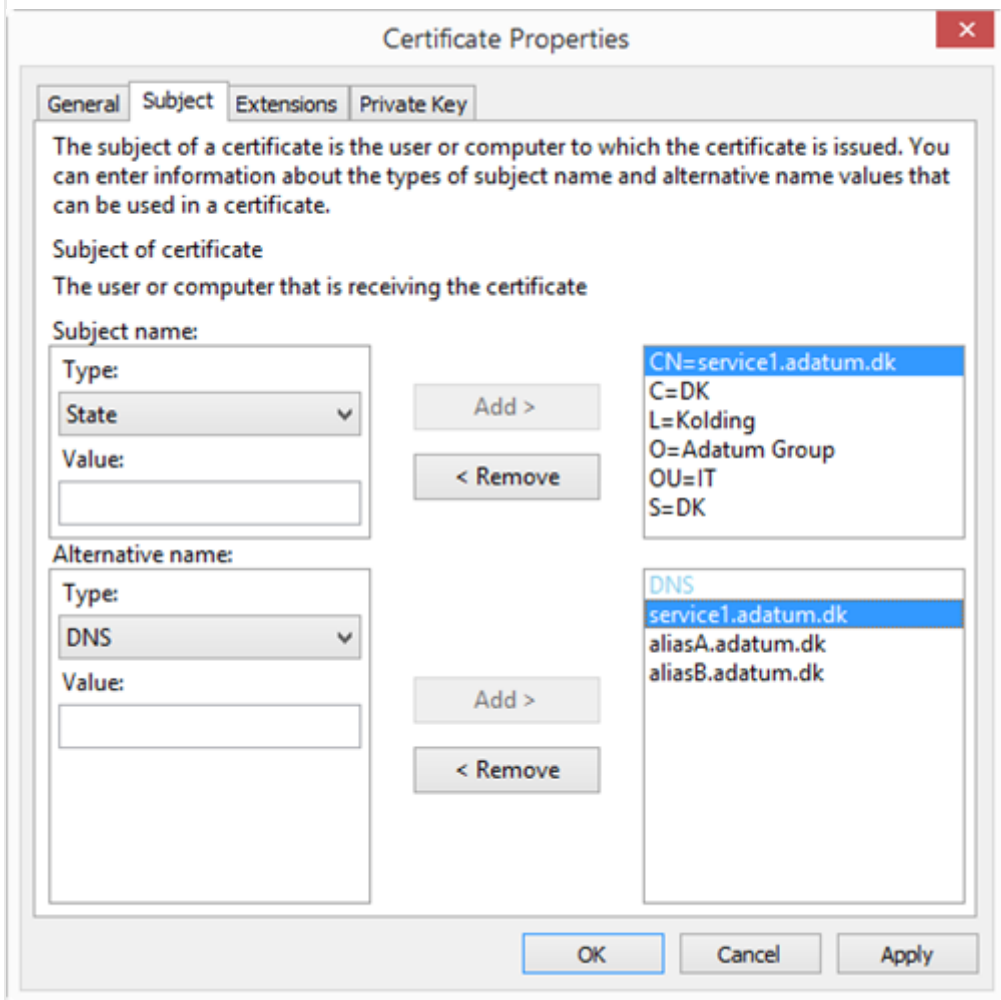
Enter the **Friendly name** for the certificate and select the **Subject** tab



On **Subject** tab add the relevant **Subject names** and **Alternative names** for the certificate.

Most Public CAs require additional information in certificate request, including **Country**, **Locality**, **Organization**, **Organization Unit** and **State**:

Standard SAN certificate:



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: State

Add >

< Remove

Value:

CN=service1.adatum.dk
C=DK
L=Kolding
O=Adatum Group
OU=IT
S=DK

Alternative name:

Type: DNS

Add >

< Remove

Value:

DNS
service1.adatum.dk
aliasA.adatum.dk
aliasB.adatum.dk

OK Cancel Apply

Unified Messaging certificate:

Certificate Properties

General Subject Extensions Private Key

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:
State ▼

Add >

Value:
[Empty text box]

< Remove

CN=dialin.adatum.dk
C=DK
L=Kolding
O=Adatum Group
OU=IT
S=DK

Alternative name:

Type:
DNS ▼

Add >

Value:
[Empty text box]

< Remove

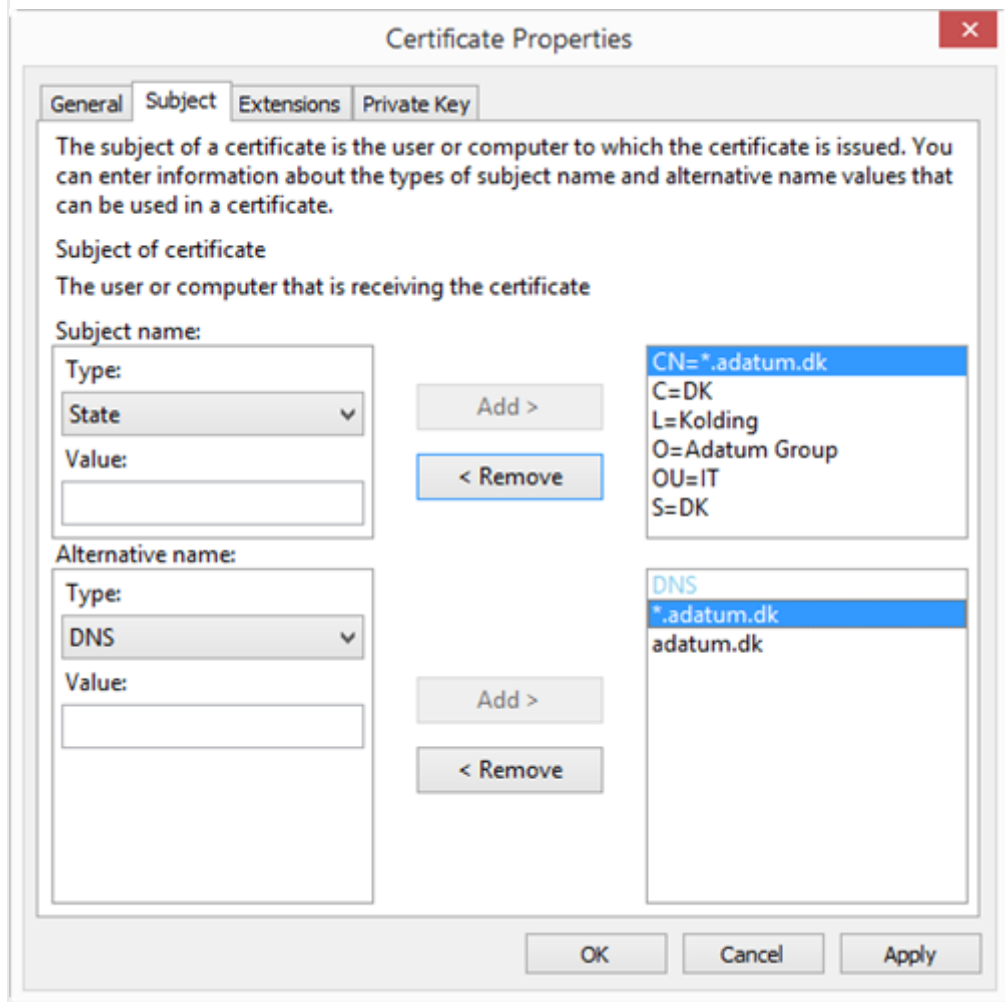
DNS
dialin.adatum.dk
meet.adatum.dk
lyncdiscover.adatum.dk
lsweb-ext.adatum.dk
wac.adatum.dk
lsrp.adatum.dk

OK Cancel Apply

This website may use cookies for statistical purposes. By continuing to use this website, you agreed to this. [Cookie Policy](#)

Close and accept

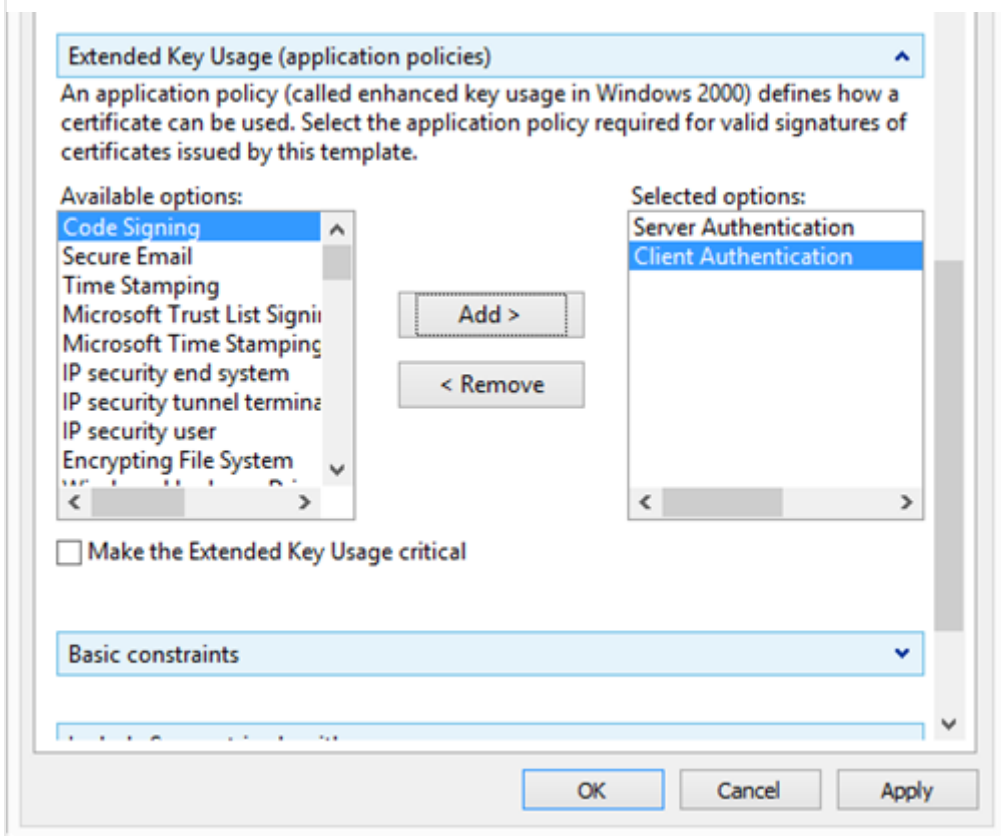
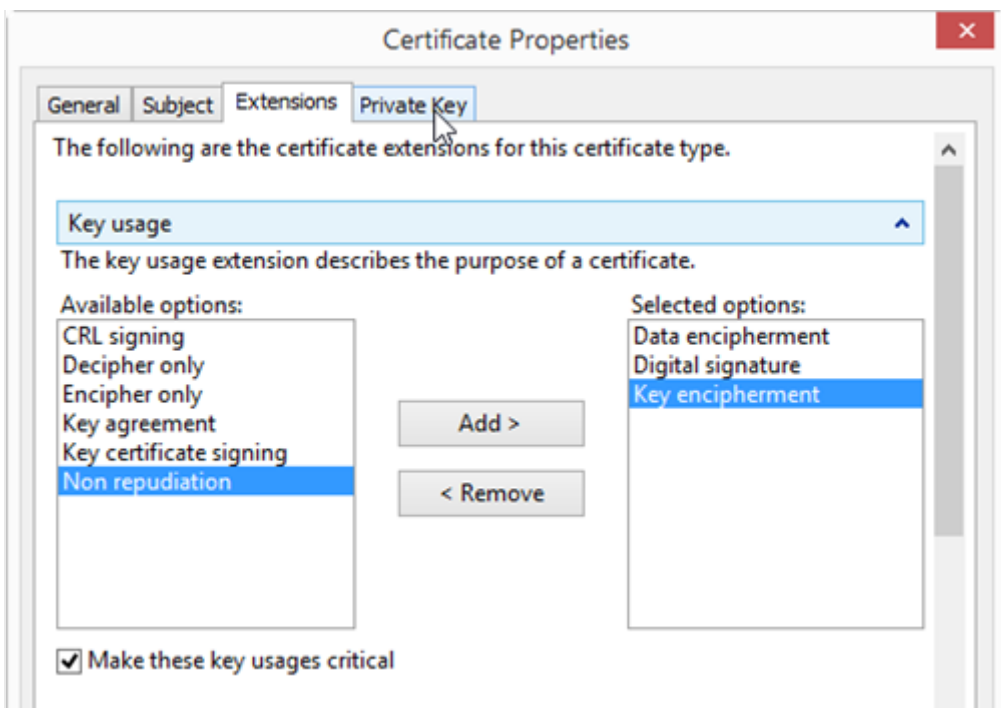
Wildcard certificate:



On the **Extensions** tab:

Select **Key Usage** and add **Data encipherment**, **Digital signature**, **Key encipherment**

Select **Extended Key Usage (application policies)** and add **Server Authentication** and **Client Authentication**



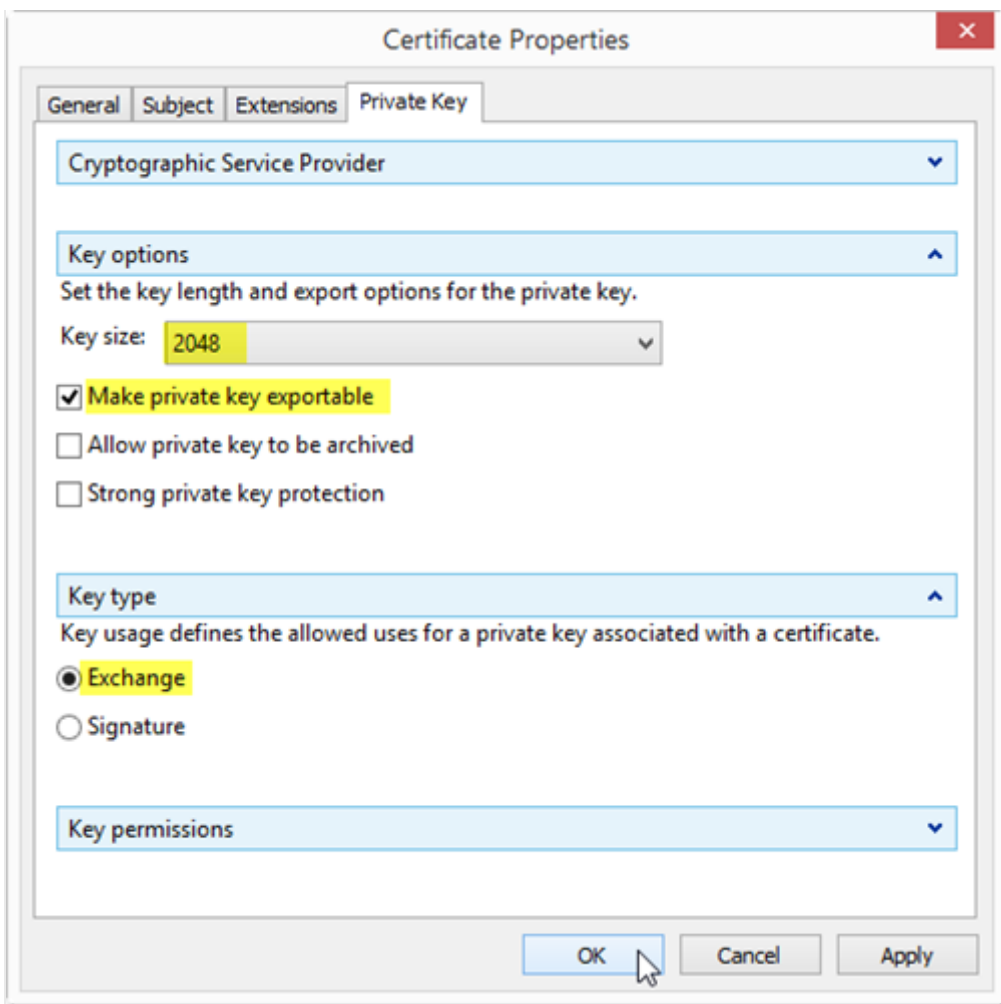
On **Private Key** tab:

Select **Key options** and set **Key size** to **2048** (or higher) and enable the **Make private key exportable** option.

Select **Key type** and set to **Exchange**

This website may use cookies for statistical purposes. By continuing to use this website, you agreed to this. [Cookie Policy](#)

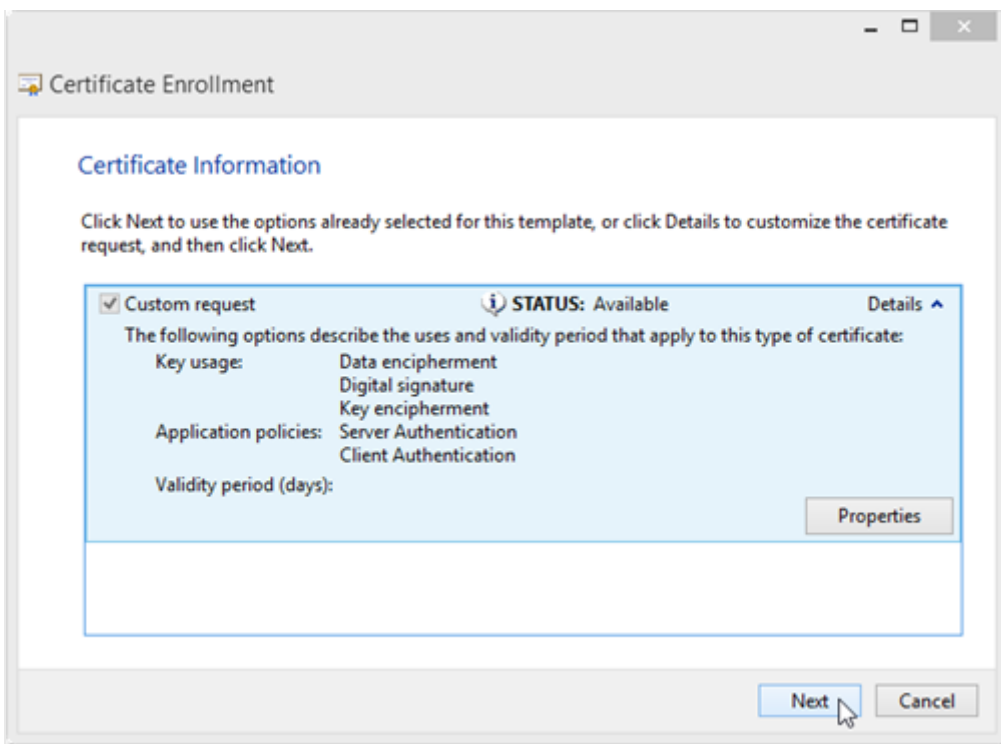
Close and accept



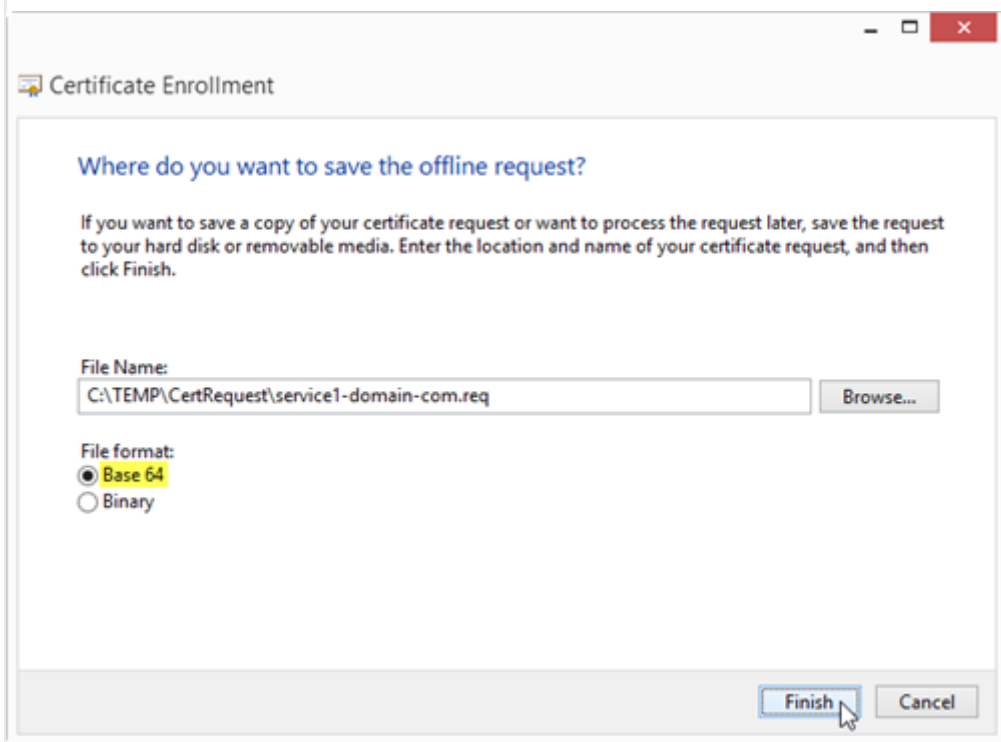
NOTE

If you at this point switch to another tab, without first pressing **Apply**, the **Key size** value will be reverted to the default (1024) !

Click **OK** to go back to wizard page and click **Next**:



Enter the full path to save the request file and ensure that **File format** is set to **Base 64**, and click **Finish**.



After finishing the wizard, you will have a CSR in BASE 64 format which you can forward to an external or internal certificate authority for signing.

Note that the private key is not included in the CSR, and there is no risk of compromising the private key while

This website may use cookies for statistical purposes. By continuing to use this website, you agreed to this. [Cookie Policy](#)

Close and accept

After importing the signed public key, the private key and the imported public key must automatically merge and create a complete, working certificate with an associated private key, ready for deployment on your web site or service.

Category: PKI Tags: Certificates, PKI

You must [log in](#) to post a comment.
This site uses Akismet to reduce spam. [Learn how your comment data is processed](#).

Iconic One Theme | Powered by Wordpress

This website may use cookies for statistical purposes. By continuing to use this website, you agreed to this. [Cookie Policy](#).

Close and accept