

[< Previous](#)[Next >](#)

Certificate Signing Request

In order to get an SSL certificate for your website, you need to generate and submit a Certificate Signing Request (CSR) to the CA (Certificate Authority).

What is a CSR?

A CSR is an encoded message submitted by an applicant to a CA to get an SSL certificate. In other words, it is a request from an applicant to a CA to get a digital certificate.

A CSR contains a public key and the applicant's information such as FQDN (Fully Qualified Domain Name), organization name and address. The CA validates the applicant's information and issues an SSL certificate with the public key included in the CSR.

Generally, a CSR is generated using the web server where the SSL certificate is going to be installed. However, it can also be generated using SSL tools or a modern browser such as Chrome or Firefox. The most common format for CSRs is the [PKCS #10 specification](#).

A CSR is a Base64 ASCII encoding message starting with "-----BEGIN NEW CERTIFICATE REQUEST-----" and ending with "-----END NEW CERTIFICATE REQUEST-----". The following is a sample CSR:

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIERzCCAY8CAQAwZzELMAkGA1UEBhMCVVMxCzAJBgNVBAGMAk5ZMREwDwYDVQQH
DAhuZXcgeW9yazEPMA0GA1UECgwGbkXkb3JnMQswCQYDVQQLDAJJVDEaMBGGA1UE
AwwRd3d3Lm15d2Vic2l0ZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCfVbkuJwMiw0wgvRAV1XS/HZFGH0I6/p2NyOn7onb8uEV3cMFf4iCzBN6Z
KJD92qVtmZSBpH9IQrYiEohTxkgJ2c/dyX06eDVS7nE53etPOZCM8VvJ0q/7PD0+
7Kvy6jhQVU7Rb1mQrFcrU0GVOQWwqtpHwbeKPFJ3mR1PNzygmXAUxkv0XdstQPm
b5sVx965SGoIgrRUDp1+UNUcE198AVPEiDUg1VqY+mUmyOcvCk0153UtxDUMoocg
S5Wlfd83We35a7I6+FAvDKKk31gv6Jxfs/EzZ6D0iiytDMAWNRwDvaYcu0608Ye/
rt9mFF90XsMMn7xi0cuCaLzG7JrJAgMBAAAgggGZMBoGCisGAQQBgjcNAgMxDBYK
Ni4xLjc2MDEuMjA1BgkrBgEEAYI3FRQxKDAmaGFEADkZWxsLVBDdAtkZWxsLVBD
XERldgwLSW5ldE1nci5leGUwYmYyYBBAGCNw0CAjFkMGICAQEeWgBNAGkAYwBy
AG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBzACAAQwByAHkAcAB0
AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgMBADCBzwYJKoZIhvcN
AQkOMYHBMIG+MA4GA1UdDwEB/wQEAwIE8DATBgNVHSUEDDAKBggrBgEFBQcDATB4
BgkqhkiG9w0BCQ8EazBpMA4GCCqGSIb3DQMCAGIAgDA0BggqhkiG9w0DBAICAIaw
BAEFMAcGBSs0AwIHAoGCCqGSIb3DQMHB0GA1UdDgQWBBS4T+amOyNS+ECWfIwx
eBUR+XRv+TCTfXvFRiQ35T960o79JqJZpad+PS9HNghqS051dsrA/p/n/1rG9T+n
1a6jTj6BEwOLaTfUWlq8KtkkYiROOC9LqhQCn84PQu03L9c1LrsV//1C4hGkFUBG
-----END NEW CERTIFICATE REQUEST-----

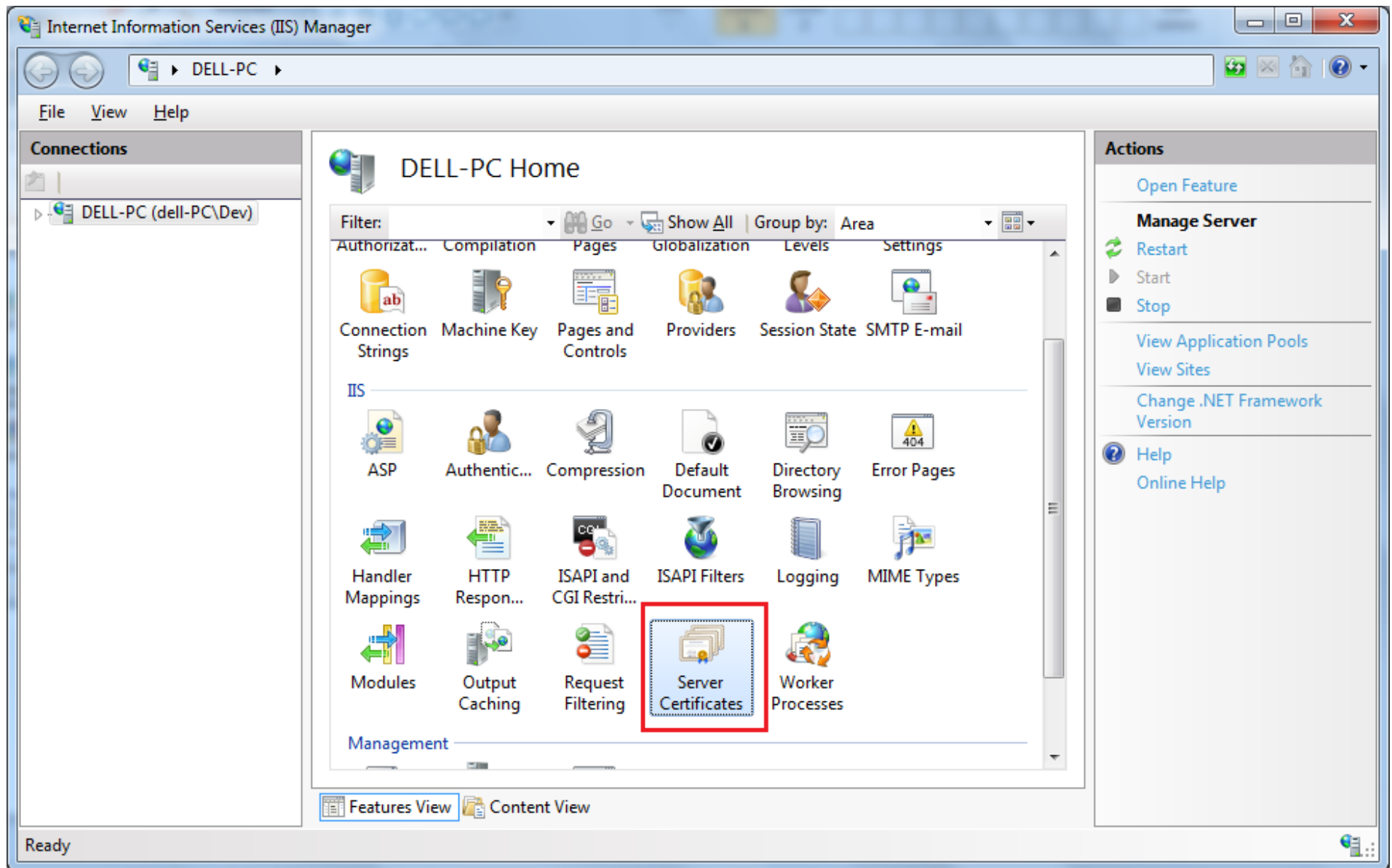
```

Generate a CSR

A CSR can be generated using any web server. Here, we are going to generate a CSR from IIS 7.

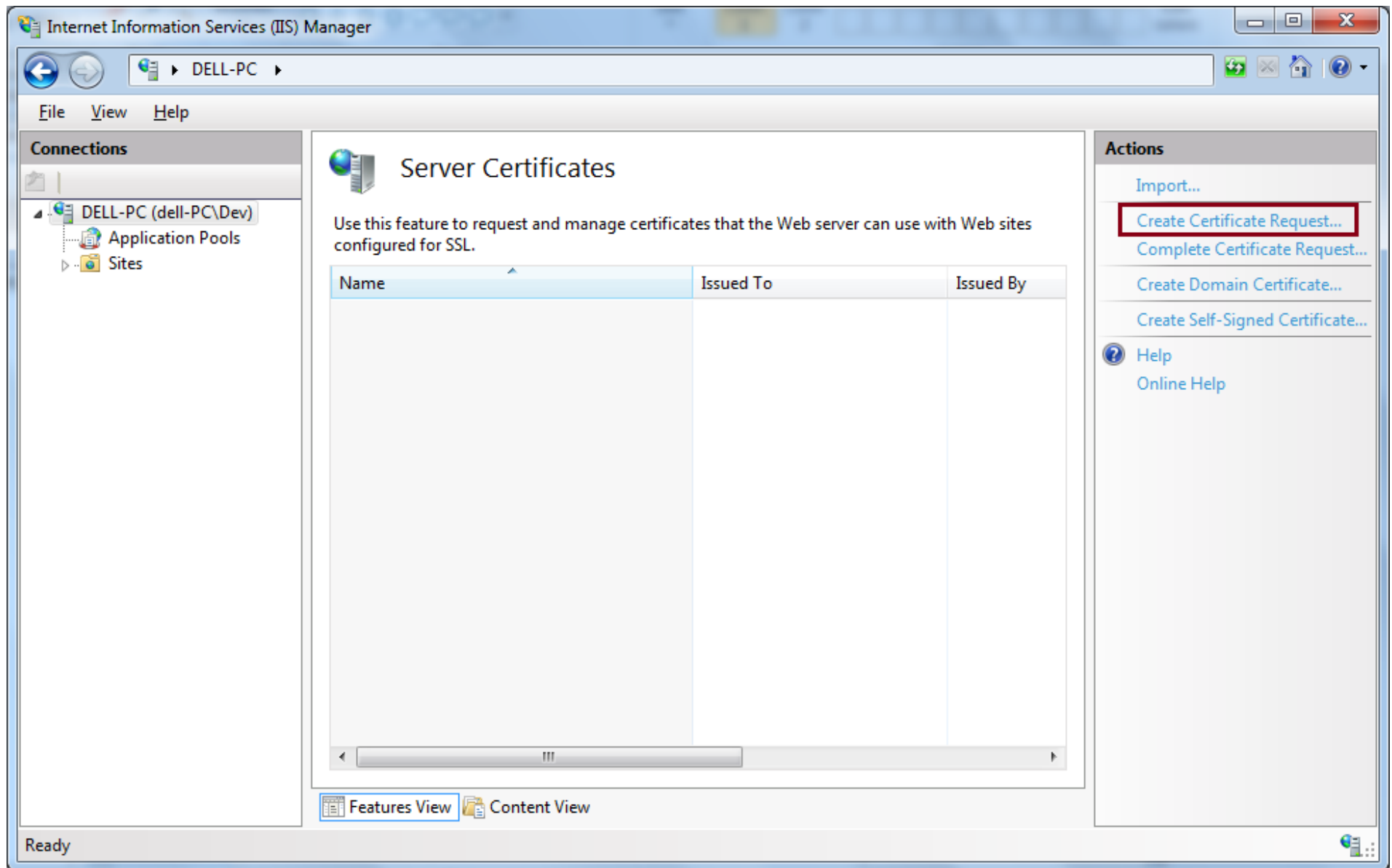
Click **Start** -> **All Programs** -> **Administrative Tools** -> Internet Services Manager.

In the Internet Information Services (IIS) Manager window, select your server and double-click **Server Certificates**.



Server Certificates in IIS

From the **Actions** panel on the right, click **Create Certificate Request...**

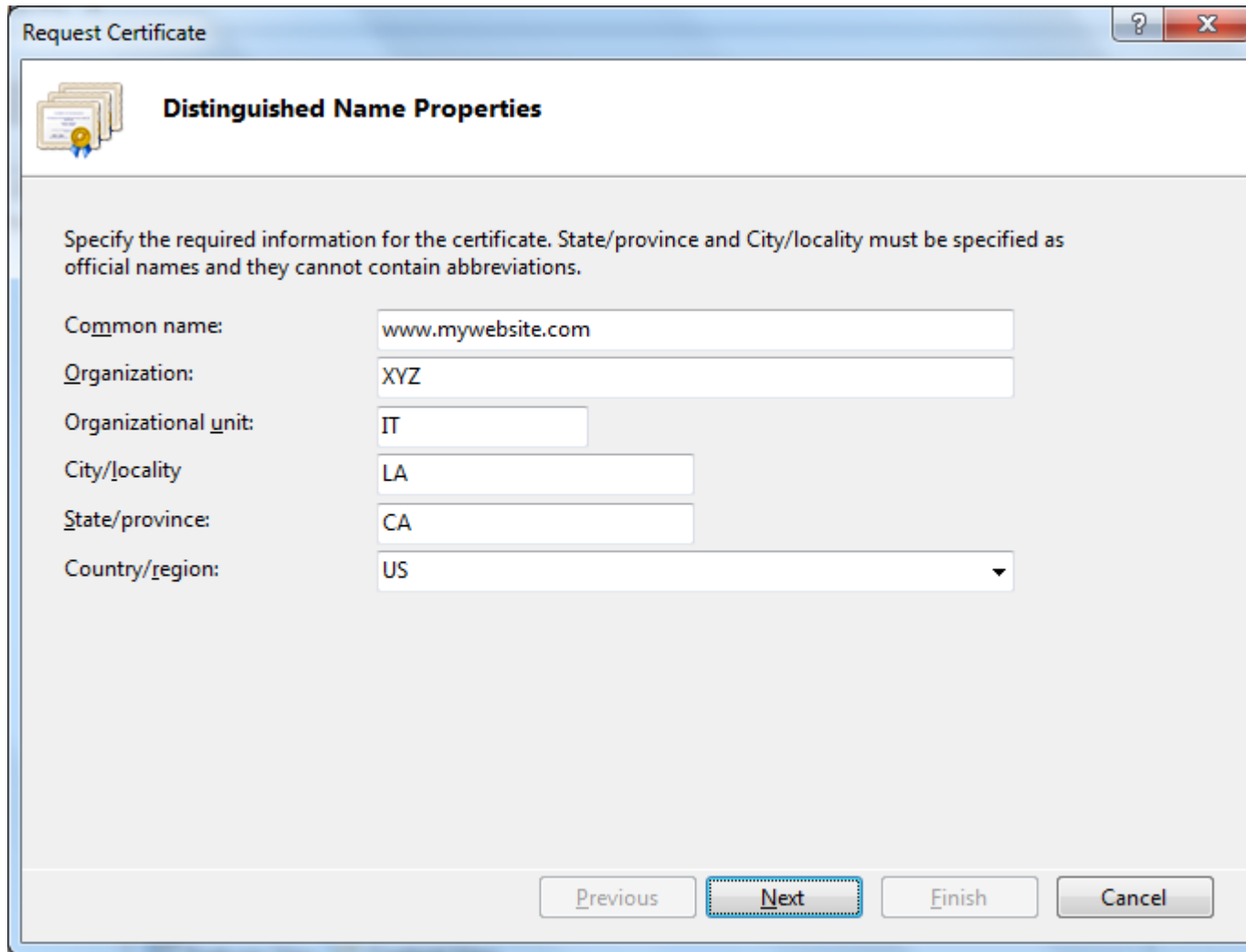


Create CSR

In the **Request Certificate** dialogue box fill in the information specified below and click **Next**.

- > Common name: The fully-qualified domain name (FQDN) (e.g., www.mywebsite.com).

- > Organization: Your company's legally registered name (e.g., My Company).
- > Organizational unit: The name of your department within the organization. This entry will usually be listed as "IT".
- > City/locality: The city where your company is legally located.
- > State/province: The state/province where your company is legally located.
- > Country/region: The country/region where your company is legally located. Use the drop-down list to select your country.



Request Certificate

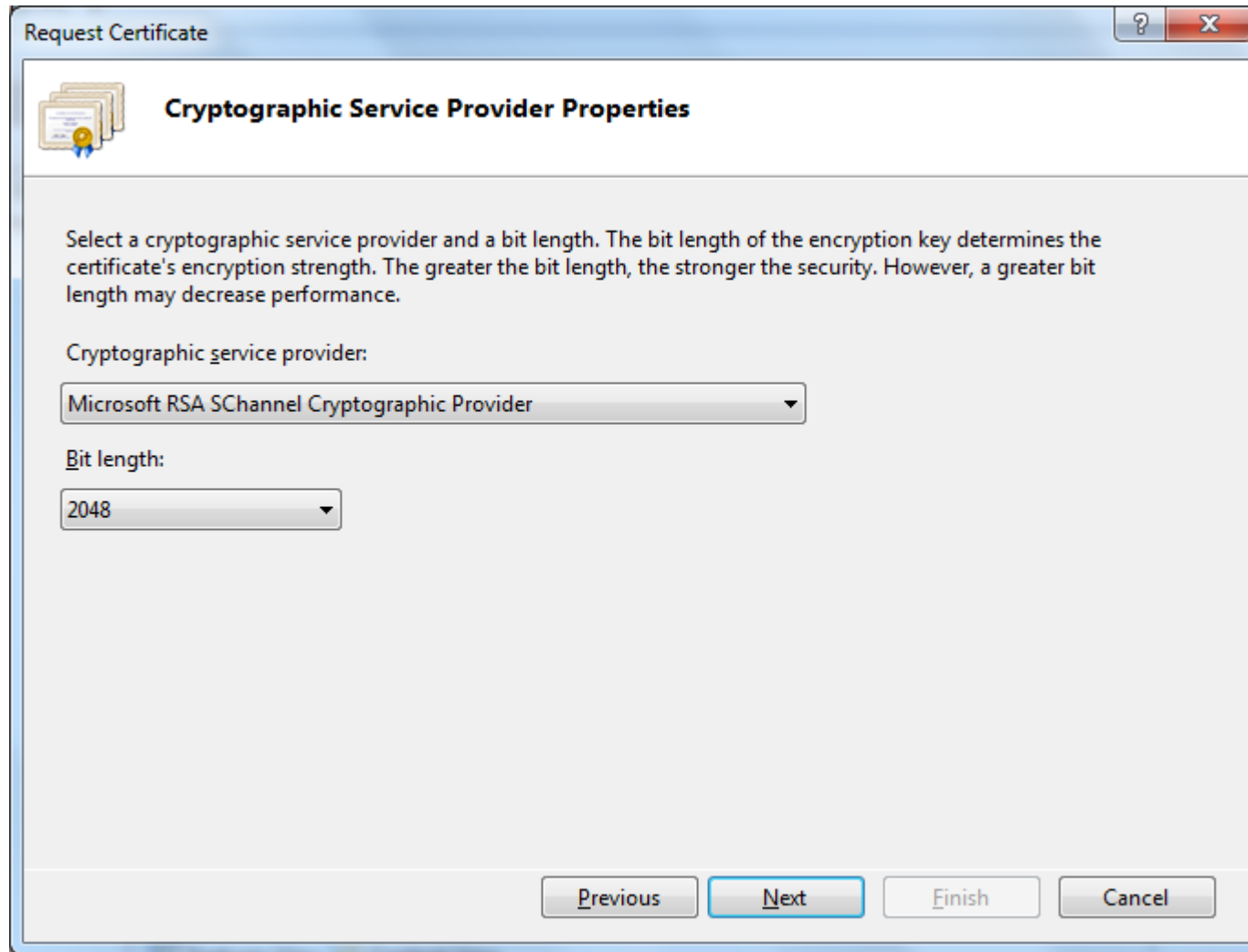
Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	<input type="text" value="www.mywebsite.com"/>
Organization:	<input type="text" value="XYZ"/>
Organizational unit:	<input type="text" value="IT"/>
City/locality:	<input type="text" value="LA"/>
State/province:	<input type="text" value="CA"/>
Country/region:	<input type="text" value="US"/>

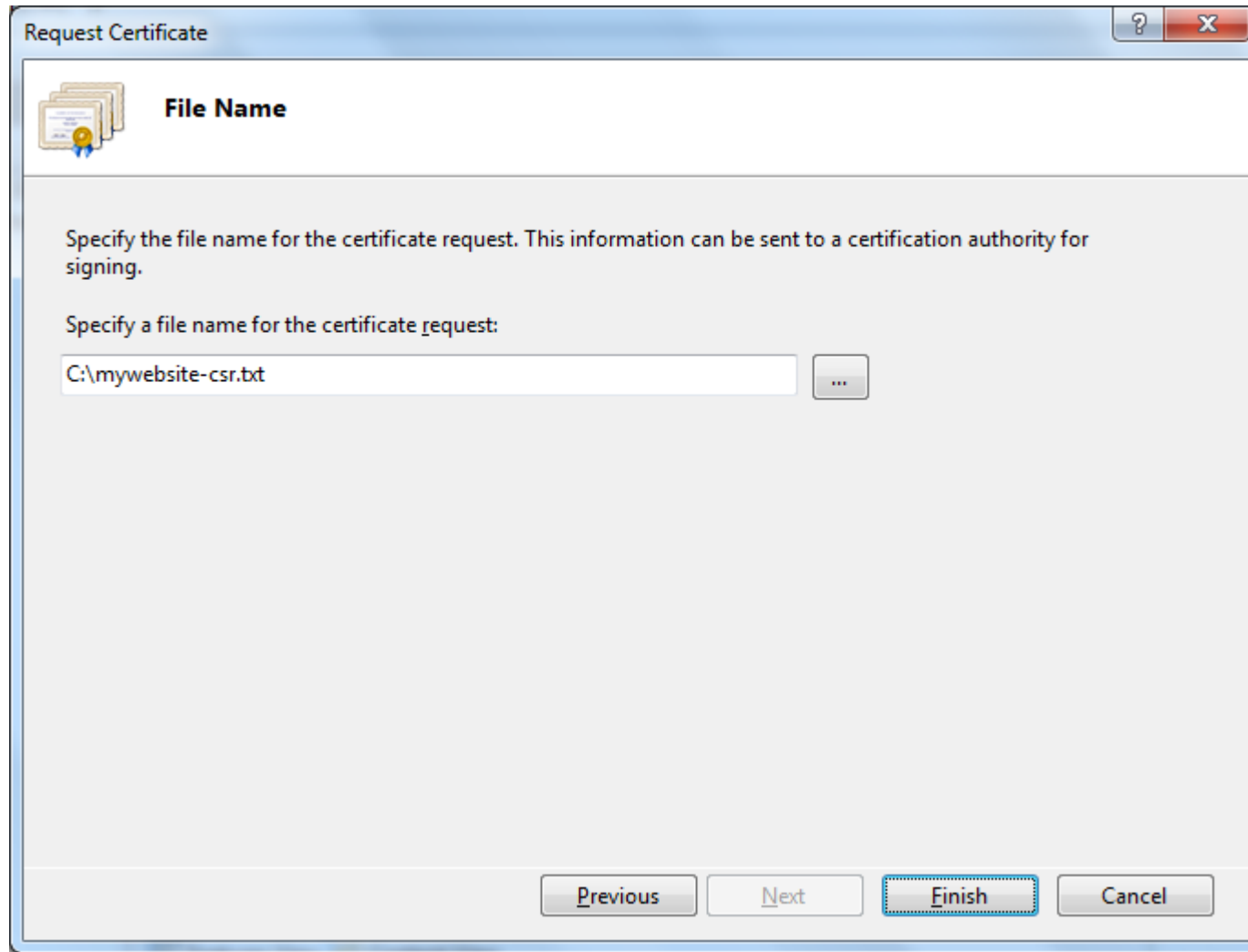
Certificate Signing Request

On the Cryptographic Service Provider Properties page, select **Microsoft RSA SChannel Cryptographic Provider** as the cryptographic service provider and select 2048 Bit length from the dropdown, as shown below. Click **Next**.



Certificate Signing Request

Provide the path and the name of the CSR file. (If you enter a filename without specifying a location, your CSR will be saved to C:\Windows\System32.)



Certificate Signing Request

Click **Finish**. This will generate a CSR in the specified file. The above CSR in the mywebsite-csr.txt looks like below. (It will be different on your local server.)

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIERTCCAY0CAQAwZTElMAkGA1UEBhMCVVMxHzANBgNVBAgMAk5ZMQswCQYDVQQL
DAJ0WTEtBEGA1UECgwKTXkgQ29tZGFueTElMAkGA1UECwwCSVQxGjAYBgNVBAMM
EXd3dy5teXdlYnNpdGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAtZL8bDFANNObNNC9vk7uMzmtWrqh/qnILcew2+bQ0X03aEtHXgZhTJ7MsC+F
yEmkK5Z9fMjFJFAP1XJH5WLyEJWXkH65DxGhncSQhU1oBL2gwENYTPgTupg9l+Ro
j8NV++DSYUZUjAF72GHI3+E/xvudushJ40Qqwdxc0ZJ61TzX5T9VTv4iPMaveN7M
e4yrAG3x28nrkarX8InEDGCojMtKr7wcHmEtz4mED//23X9hDUlnUpBkseB55tgo
AAGRCzrNkidXTwuVDVmQBqA4GAaH1lpIlxD6nd3v3N7GiN0kaxpeT6vqZyFBN5p/
rM0cOnoOH9drKJHKvSuoq7g4GQIDAQAB0IIBmTAAABgorBgEEAYI3DQIDMQwwCjYu
MS43NjAxLjIwNQYJKwYBBAGCNxUUMSgwJgIBBQwHZGVsbC1QQwwLZGVsbC1QQ1xE
ZYMC0luZXRNZ3IuZXh1MHMIGCisGAQQBgjcNAgIxZDBiAgEBH1oATQBpAGMAcGbv
AHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAgAEMAcGB5AHAAdABV
AGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZAB1AHIDAQAwgc8GCsQGSIb3DQEJ
DjGBwTCBvjAOBgNVHQ8BAf8EBAMCBPAwEwYDVR0lBAwwCgYIKwYBBQUHAEwEAYJ
KoZIhvcNAQkPBGswTAOBggqhkiG9w0DAGICAIAwDgYIKoZIhvcNAwQCAgCAMASG
CWGSAF1AwQBKjAlBglghkgBZQMEAS0wCwyYJYIZIAWUDBAECMASGCWGSAF1AwQB
BTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQUAij8Shgv157ZiZLNxt4se
J4FfCwgdQYJKoZIhvcNAQEFBQADggEBAFZ0RtA1q+H+xgdf19ccDzsoxqCA6Nkv
WARhrNG5ryC8+f0VhFSh1N0PyEY1aMEhIZLjP2BDaoPw2G+1xeTa170VzbObk5bw
KTe3LAGWVENDVm03x3bFgX05PfdFYTHMTXyyY6nZCurunFqGsov1CxuNqrQEgCD
5Q9aZ61cT8d2W2epae5bCzZ4WxHCUeHtYeja3hYQfk9eFpaAvQ4KFioBPnGY5L+V
J1H79wda0p4+0kY1aB/PyVKNMZmuSphdeMD045hsKm6UFT+99ewq/ocKDIJX7U7V
V0gQ/53fUmJ3zqUavcg+SxrwFF8wFU59VKPSGYoMBOWEPd/5pb0rGx8=
-----END NEW CERTIFICATE REQUEST-----
```

The above CSR includes a public key and other identity information we provided in the Base64 PEM format.

If you are using a different web server then visit [thesslstore's knowledgebase](#) and click on the link of the web server you are using to know how to generate a CSR for your web server.

Public Key and Private Key

A CSR includes a public key generated by the web server where you are going to install an SSL certificate. The web server generates a key pair, a public key and a private key when the CSR is generated. It includes a public key in the CSR and also stores a private key secretly in the file system. This private key will be used when installing a certificate on the web server.



[< Previous](#)[Next >](#)

TutorialsTeacher.com is optimized for learning web technologies step by step. Examples might be simplified to improve reading and basic understanding. While using this site, you agree to have read and accepted our terms of use and [privacy policy](#).

✉ feedback@tutorialsteacher.com

TUTORIALS

- > [ASP.NET Core](#)
- > [ASP.NET MVC](#)
- > [IoC](#)
- > [Web API](#)
- > [C#](#)
- > [LINQ](#)
- > [Entity Framework](#)
- > [AngularJS 1](#)
- > [Node.js](#)
- > [D3.js](#)
- > [JavaScript](#)
- > [jQuery](#)
- > [Sass](#)
- > [Https](#)

E-MAIL LIST

Subscribe to TutorialsTeacher email list and get latest updates, tips & tricks on C#, .Net, JavaScript, jQuery, AngularJS, Node.js to your inbox.

We respect your privacy.

[HOME](#) [PRIVACY POLICY](#) [TERMS OF USE](#) [ADVERTISE WITH US](#)

© 2020 TutorialTeacher.com. All Rights Reserved.