

[< 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-----
MIIERzCCAY8CAQAwZzELMAkGA1UEBhMCVVMxCzAJBgNVBAGMAk5ZMREwDwYDVQQH
DAhuZXCgeW9yazEPMA0GA1UECgwGbXkgb3JnMQswCQYDVQQQLDAJJVDEaMBGGA1UE
AwwRd3d3Lm15d2Vic2l0ZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCfVbkuJwMiwOwgvRAV1XS/HZFGH0I6/p2NyOn7onb8uEV3cMFF4iCzBN6Z
KJD92qVtmZSBpH9IQrYiEohTxkgJ2c/dyX06eDVS7nE53etPOZCM8VvJOq/7PD0+
7Kvy6jhQVU7Rb1mQrFcrU0GVOQWwqtpHwbeKpfJ3mR1PNzygmXAUXkv0XdstQPm
b5sVx965SGoIgrRUDp1+UNUCe198AVPEiDUg1VqY+mUmyOcvCk0153UtxDUMoocg
S5Wlfd83We35a7I6+FavDKKk31gv6Jxfs/EzZ6D0iiytDMAWNRwDvaYcu0608Ye/
rt9mFF90XsMMn7xi0cuCaLzG7JrJAgMBAAGggGZMB0GcisGAQQBgjcNAgMxDBYK
Ni4xLjc2MDEuMjA1BgkrBgEEAYI3FRQxKDAmaGFEADkZWxsLVBDdAtkZWxsLVBD
XERldgwLSW5ldE1nci5leGUwcgYKKwYBBAGCNw0CAjFkMGICAQEewgBNAGkAYwBy
AG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBzACAAQwByAHkAcAB0
AG8AZwByAGEAcAB0AGkAYwAgAFAAcgBvAHYAaQBkAGUAcgMBADCBzwYJKoZIhvcN
AQkOMYHBMIG+MA4GA1UdDwEB/wQEAWIE8DATBgNVHSUEDDAKBggrBgEFBQcDATB4
BgkqhkiG9w0BCQ8EazBpMA4GCCqGSIb3DQMCAGIAgDAOBggqhkiG9w0DBAICAIaw
BAEFMAcGBSsOAwIHMaoGCCqGSIb3DQMhMB0GA1UdDgQWBBS4T+am0yNS+ECWfIwx
eBUR+XRv+TCTfXvFRiQ35T960079JqJZpaD+PS9HNghqS051dsrA/p/n/1rG9T+n
1a6jTj6BEwOLaTfUwLq8KtkkYiR0OC9LqhQCn84PQu03L9c1LrsV//1C4hGkFUBG
-----END NEW CERTIFICATE REQUEST-----

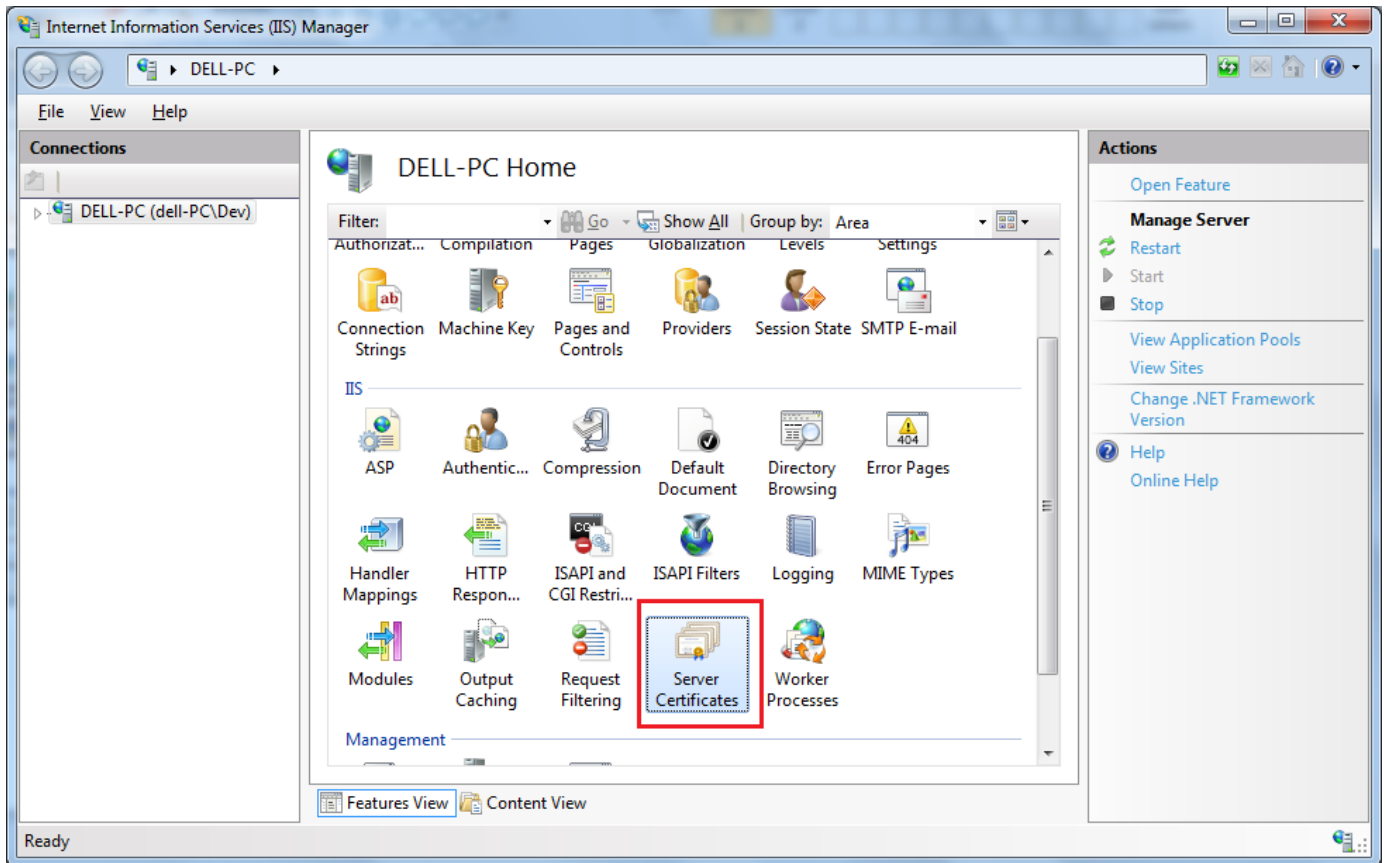
```

## Generate a CSR

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

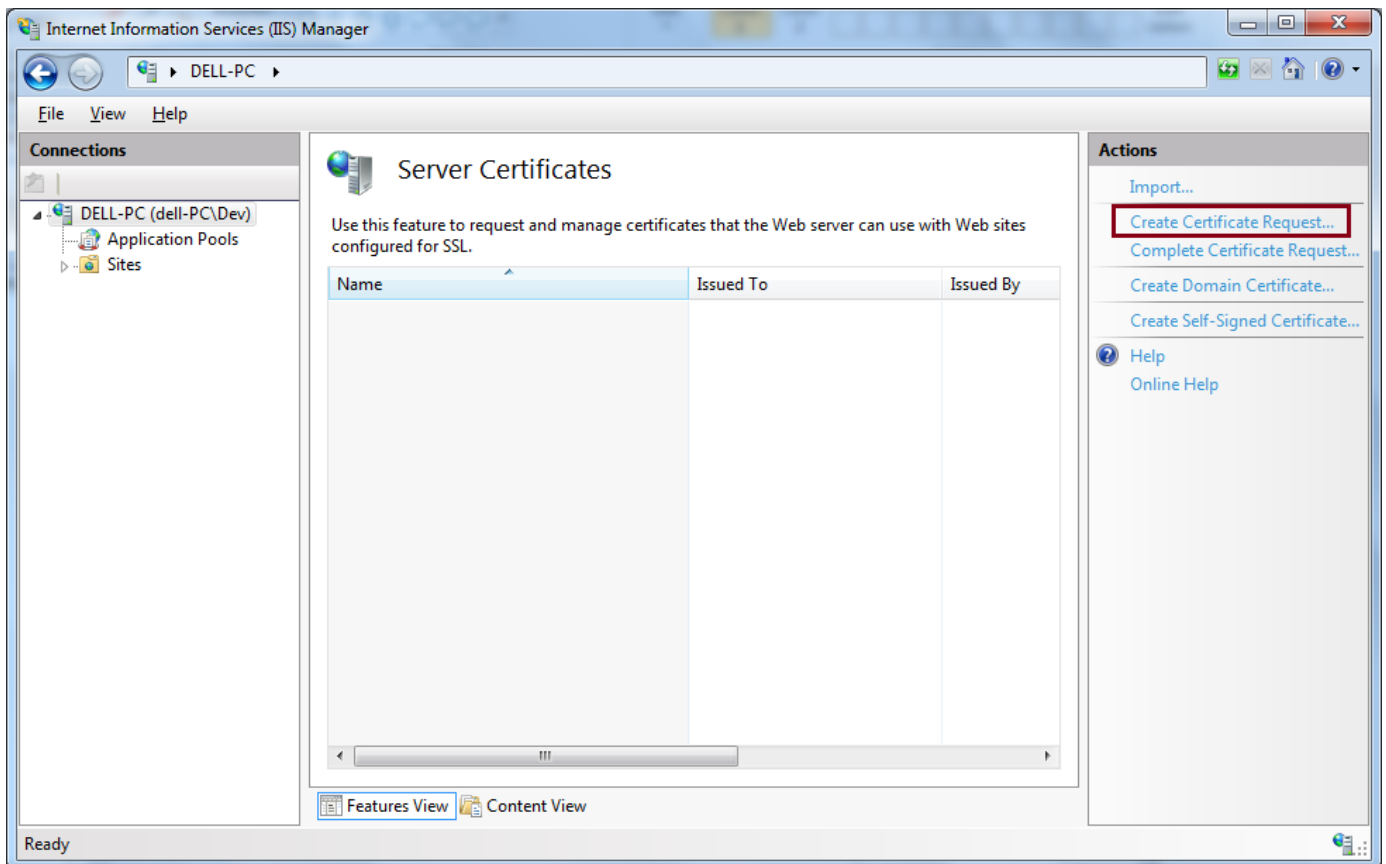
Click **Start** -> **All Programs** -> **Administrative Tools** -> Internet Services Manager.

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



Server Certificates in IIS

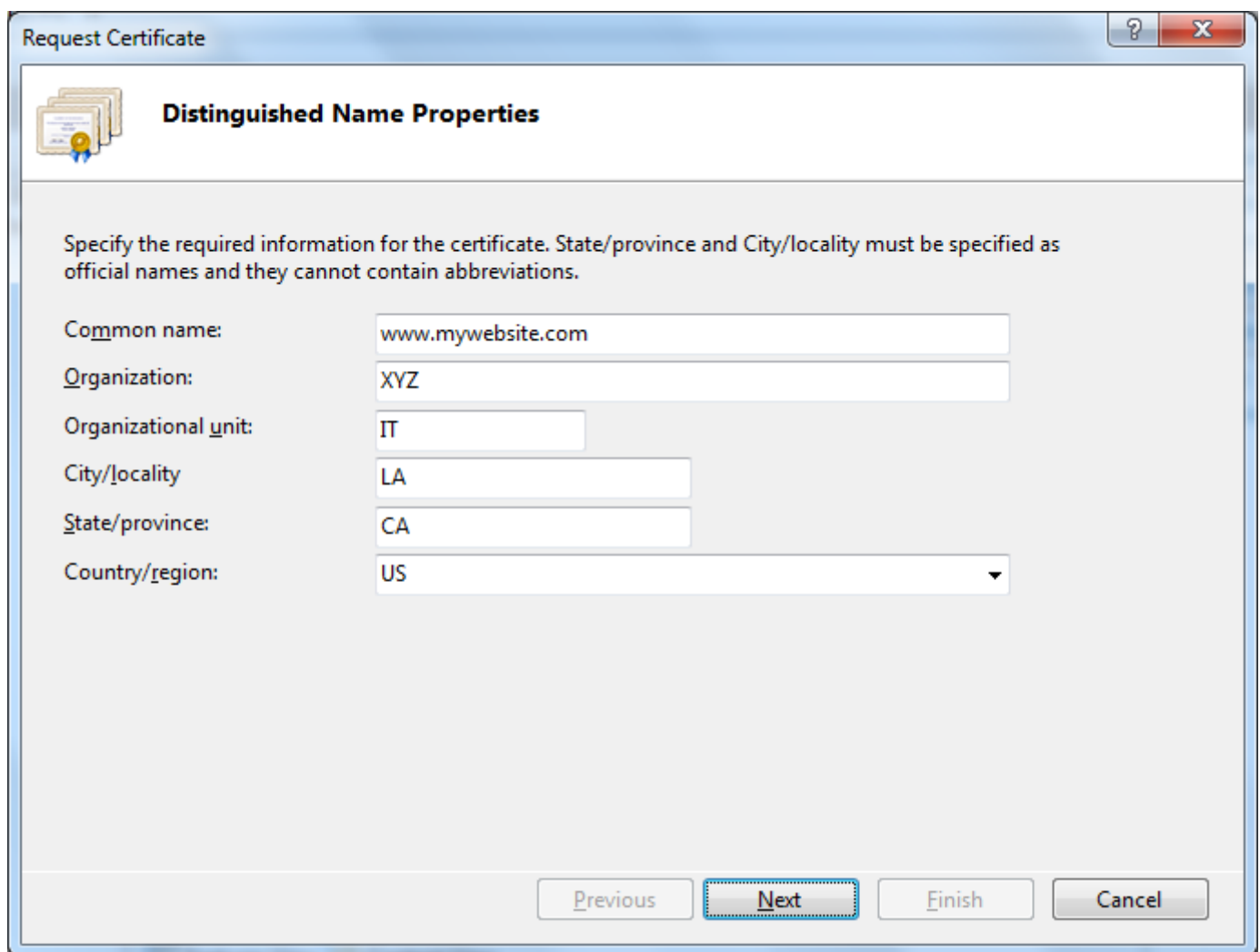
From the **Actions** panel on the right, click **Create Certificate Request...**



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:

Organization:

Organizational unit:

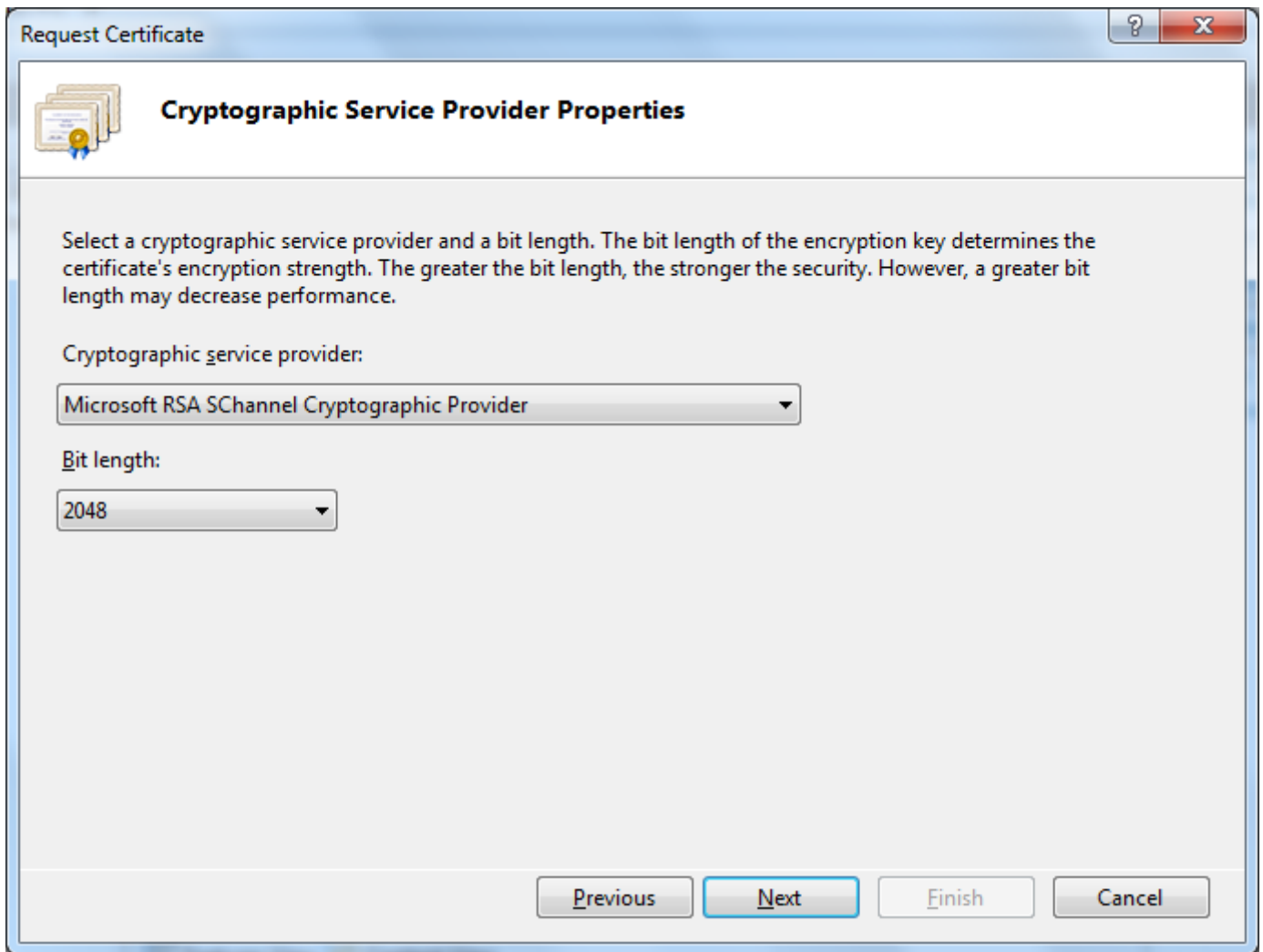
City/locality:

State/province:

Country/region:

### 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**.



Request Certificate

**Cryptographic Service Provider Properties**

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:

Microsoft RSA SChannel Cryptographic Provider

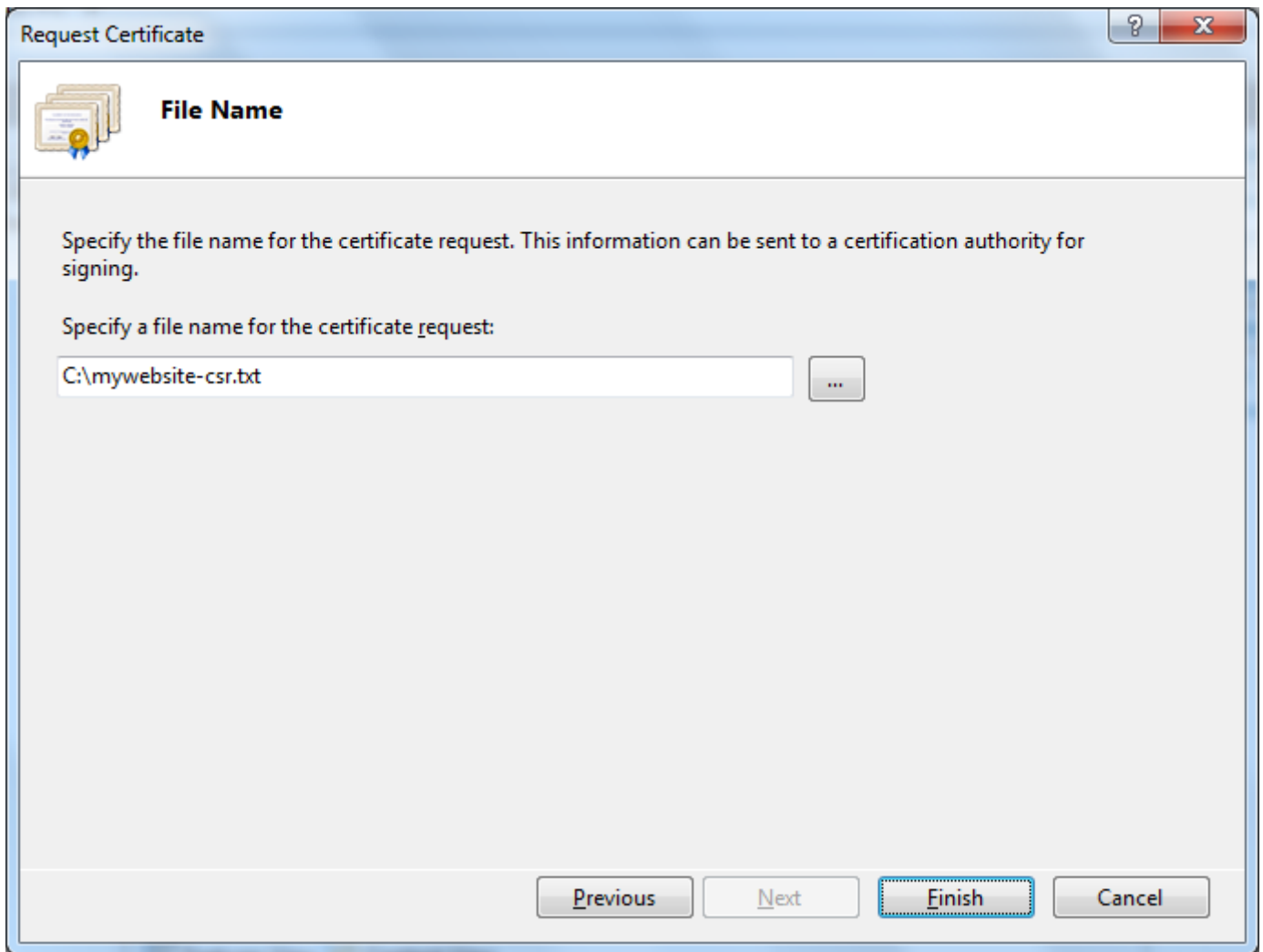
Bit length:

2048

Previous Next Finish Cancel

### 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.)



The image shows a Windows-style dialog box titled "Request Certificate". It has a standard title bar with a question mark icon and a close button (X). The main area is titled "File Name" with a small icon of a certificate. Below the title, there is a text box containing the instruction: "Specify the file name for the certificate request. This information can be sent to a certification authority for signing." Below this, another text box says "Specify a file name for the certificate request:" followed by a text input field containing "C:\mywebsite-csr.txt" and a browse button (three dots). At the bottom of the dialog, there are four buttons: "Previous", "Next", "Finish" (which is highlighted with a blue border), and "Cancel".

### 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-----
MIERTCCAY0CAQAwZTElMAkGA1UEBhMCVVMxCzAJBgNVBAGMAk5ZMQswCQYDVQQH
DAJOWTETMBEGA1UECgwKTXkgQ29tcGFueTElMAkGA1UECwwCSVQxGjAYBgNVBAMM
EXd3dy5teXd1YnNpdGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAtZL8bDFANNOBNNc9vk7uMzmtWrqh/qnILcew2+bQ0X03aEtHXgZhTJ7MsC+F
yEmkK5ZF9mJfJFAP1XJH5WLyEJWXkH65DxGhncSQhU1oBL2gwENYTPgTupg91+Ro
j8NV++DSYZUjAfff72GHI3+E/xvudushj40QqwdxcoZJ61Tzx5T9VTv4iPMAveN7M
e4yrAG3x28nrkarX8InEDGCojMtKr7wcHmEtz4mED//23X9hDU1nUpBkseBs5tgo
AAgRCzrNkidXTWuVDVmQBqA4GAaH1pI1xD6nd3v3N7GiN0kaxpeT6vqZyFBN5p/
rM0c0no0H9drKJHKvSuoq7g4GQIDAQABoIIBmTAABgorBgEEAYI3DQIDMQWwCjYu
MS43NjAxLjIwNQYJKwYBBAGCNxUUMSgwJgIBBQwHZGVsbC1QQWwLZGVsbC1QQ1xE
ZXYMC0luZXRnZ3IuZXh1MHIGCisGAQQBgjcNAgIxZDBiAgEBHloATQBpAGMAcGBv
AHMAbWBMaHQAIABSAFMAQQAgAFMAQWBoAGEAbgBuAGUAbAAgAEMAcGB5AHAAdABv
AGcAcgBhAHAaAABpAGMAIABQAHIAbWB2AGkAZABIAHIDAQAwwc8GCSqGSIb3DQEJ
DjGBwTCBvjA0BgNVHQ8BAf8EBAMCBPAwEwYDVR0lBAwwCgYIKwYBBQUHAWeweAYJ
KoZIHvcNAQkPBGswaTA0BgqgqhkiG9w0DAgICAIAwDgYIKoZIHvcNAwQCAgCAMAsG
CWCGSAFlAwQBKjAlBglghkgBZQMEAS0wCwYJYIZIAWUDBAECMA5GCWCGSAFlAwQB
BTAHBgUrDgMCMCBZAKBgqgqhkiG9w0DBzAdBgNVHQ4EFgQUAja8Shgvl57ZiZLNxt4se
J4FfCwgwDQYJKoZIHvcNAQEFBQADggEBAFZ0RtA1q+H+xgdf19ccDzsoxqCA6NKV
WARhrNG5ryC8+f0VhFSH1NOPyEY1aMEhIZLJp2BDaoPw2G+1xeTa170Vzb0bk5bw
KTe3LAGWVENDVqm03x3bFgX05PfdFYTHMtXyyY6nZCurunFqGsov1CxCuNqrQEgCD
5Q9aZ61cT8d2W2epae5bCzZ4WxHCUEHtYeja3hYQfk9eFpaAVq4KFIoBPnGY5L+V
J1H79wda0p4+0kY1aB/PyVKNMZmuSphdeMD045hsKm6UFT+99ewq/ocKDIJX7U7V
VOgQ/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.



Share



Tweet



Share