# Generating a MultiSAN/Multi-Domain CSR using Doc.It Certificate Tools

On the Doc.It server, download the Doc.It Certificate tool package if you haven't already: [http://docs.docitcloud.com/pub/CertificateTools.zip](http://docs.docitcloud.com/pub/CertificateTools.zip)

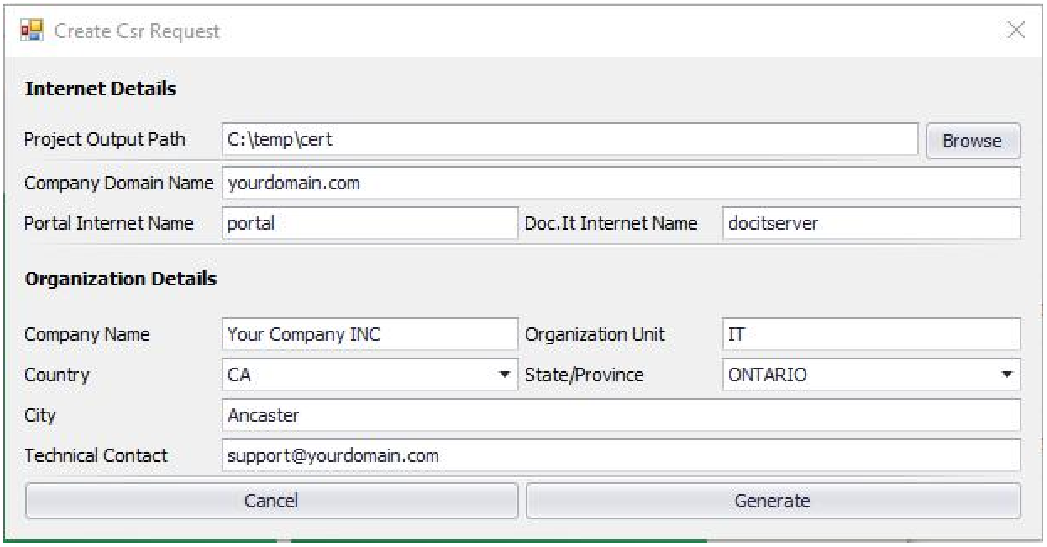
Extract the zip file and run CertificateTools.exe. Click Generate CSR.

Fill out the form as such:

Project Output Path: Click browse to select where the generated files will be created.
Company Domain Name: [yourdomain.com] -your primary root domain.
Portal Internet Name: [portal] -the subdomain portion of your primary portal domain.
Doc.It Internet Name [docitserver] -the subdomain portion of your secondary subdomain.

Company Name: [the name of your Organization]
Organizational Unit: IT
City: [your organization's city/main place of business]
State/Province: [your organization's State or Province]
Country: [your organization's country, usually US or CA]
Technical Contact: [your IT support email address]

Click Generate when you're done.



Internet Details

Project Output Path: C:\temp\cert

Company Domain Name: yourdomain.com

Portal Internet Name: portal

Doc.It Internet Name: docitserver

Organization Details

Company Name: Your Company INC

Organization Unit: IT

Country: CA

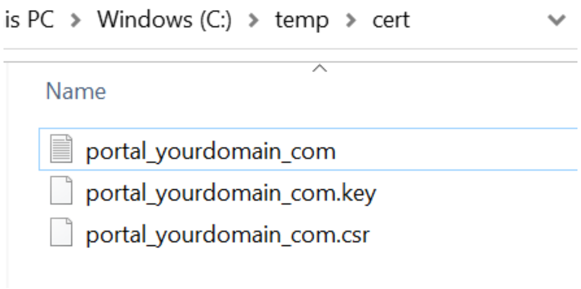
State/Province: ONTARIO

City: Ancaster

Technical Contact: support@yourdomain.com

A prompt will confirm success and the directory you specified will now contain a .csr file, a .key file and a .txt file.

**IMPORTANT**: Do not delete or modify the .key file as it is required to complete the certificate when you receive it from the Certificate Authority.

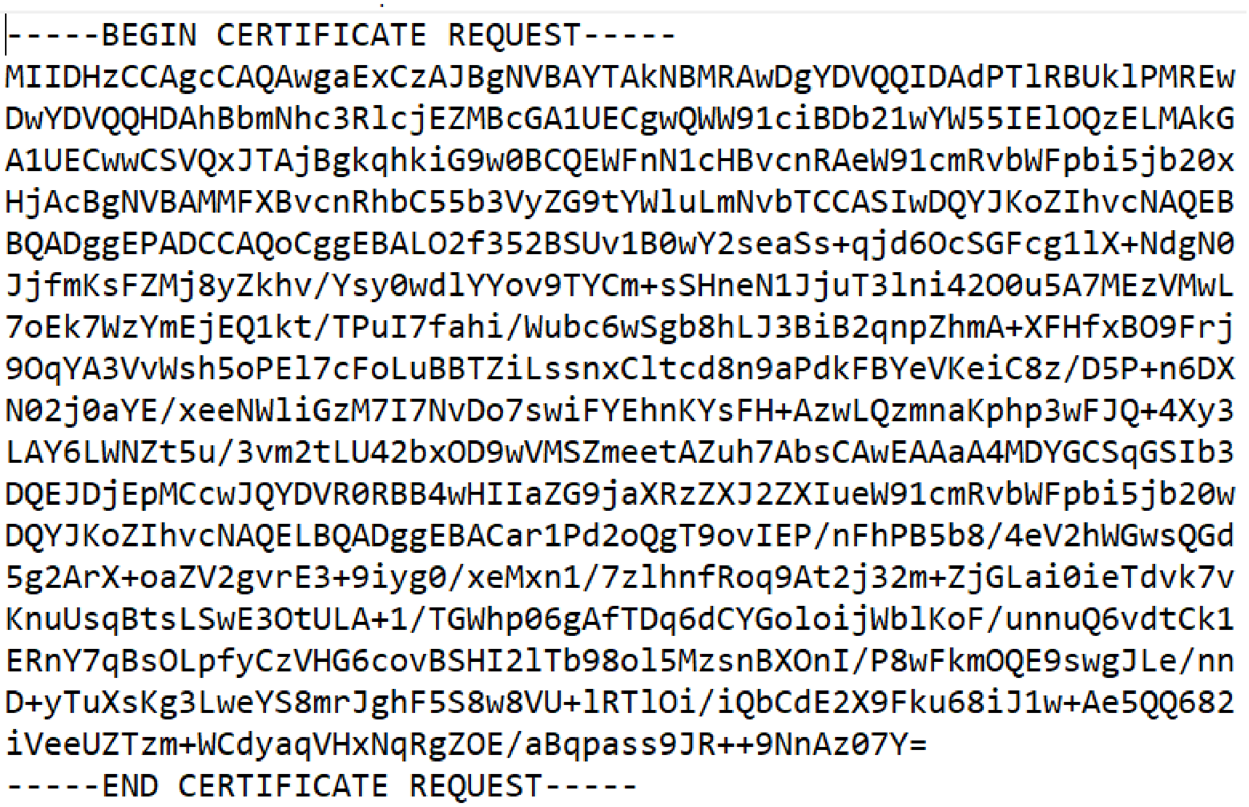


portal_yourdomain_com

portal_yourdomain_com.key

portal_yourdomain_com.csr

The resulting CSR file will look like this:

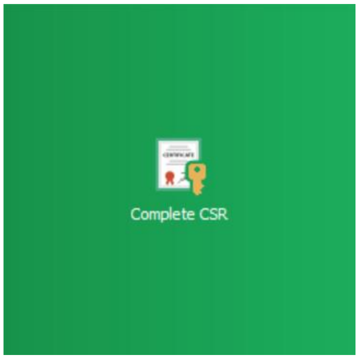


```
-----BEGIN CERTIFICATE REQUEST-----
MIIDHzCCAgcCAQAwgaExCzAJBgNVBAYTAkNBMRAwDgYDVQQIDAdPTlRBUklPMREw
DwYDVQQHDAhBbmNhc3RlcjEZMBcGA1UECgwQWW91ciBDb21wYW55IElOQzELMAkG
A1UECwwCSVQxJTAjBgkqhkiG9w0BCQEWFnN1cHBvcnRAeW91cmRvbWFpbi5jb20x
HjAcBgNVBAMMFXBvcnRhbC55b3VyZG9tYWluLmNvbTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALO2f352BSUv1B0wY2seaSs+qjd6OcSGFcg1lX+NdgN0
JjfmKsFZMj8yZkhv/Ysy0wdlYYov9TYCm+sSHneN1JjuT3lni42O0u5A7MEzVMwL
7oEk7WzYmEjEQ1kt/TPuI7fahi/Wubc6wSgb8hLJ3BiB2qnpZhmA+XFHfxBO9Frj
9OqYA3VvWsh5oPEl7cFoLuBBTZiLssnxCltcd8n9aPdkFBYeVKeiC8z/D5P+n6DX
N02j0aYE/xeeNWliGzM7I7NvDo7swiFYEhnKYsFH+AzwLQzmnaKphp3wFJQ+4Xy3
LAY6LWNZt5u/3vm2tLU42bxOD9wVMSZmeetAZuh7AbsCAwEAAaA4MDYGCSqGSIb3
DQEJDjEpMCcwJQYDVR0RBB4wHIIaZG9jaXRzZXJ2ZXIueW91cmRvbWFpbi5jb20w
DQYJKoZIhvcNAQELBQADggEBACar1Pd2oQgT9ovIEP/nFhPB5b8/4eV2hWGwsQGd
5g2ArX+oaZV2gvrE3+9iyg0/xeMxn1/7zlhnfRoq9At2j32m+ZjGLai0ieTdvk7v
KnuUsqBtsLSwE3OtULA+1/TGWhp06gAfTDq6dCYGoloijWblKoF/unnuQ6vdtCk1
ERnY7qBsOLpfyCzVHG6covBSHI2lTb98ol5MzsnBXOnI/P8wFkmOQE9swgJLe/nn
D+yTuXsKg3LweYS8mrJghF5S8w8VU+lRTlOi/iQbCdE2X9Fku68iJ1w+Ae5QQ682
iVeeUZTzm+WCdyaqVHxNqRgZOE/aBqpass9JR++9NnAz07Y=
-----END CERTIFICATE REQUEST-----
```

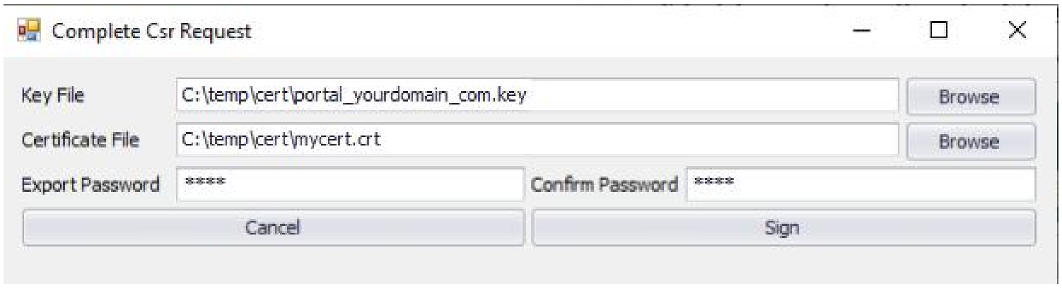
Once you have the CSR, upload it to your Certificate Authority when requesting a new certificate or renewing one. For the latter option, ensure that you select the option to renew with a new private key or re-key of the certificate. Follow your Certificate Authority's guides on how to do this, or request support. Doc.It personnel may be able to assist via screensharing session, if you are logged into the Certificate Authority's portal.

## Completing the CSR

Copy the certificate you downloaded from the CA to the directory you saved your .key and .CSR files. Run CertificateTools.exe. Click Complete CSR.



Point the tool to your .key file and the certificate (.crt) file you downloaded from the Certificate Authority.

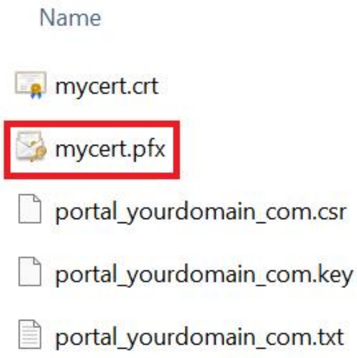

Complete Csr Request

Key File C:\temp\cert\portal_yourdomain_com.key

Certificate File C:\temp\cert\mycert.crt

Export Password **** Confirm Password ****

Enter an export password. This will be used to import the resulting file into the Local Computer's Personal Certificate store. Click Sign. A .pfx file is now generated in the same directory as your .key and .CSR files. This is the file you will import into the Local Machine's Personal Certificate Store.


Name

mycert.crt

mycert.pfx

portal_yourdomain_com.csr

portal_yourdomain_com.key

portal_yourdomain_com.txt