Generating CSR in Exchange 2013 Shell

The Exchange Management provides a command-line interface for Exchange server 2013. In fact, when you perform any actions in EAC, the Shell is doing the work behind the scenes.

The Certificate Signing Request (CSR) can be generated both in EAC and by using the command line. In this article, we will explain the commands used to create the CSR for the main domain *mail.ncssltest.info* and one additional domain *autodiscover.ncsstest.info* using Exchange Shell.

Open the Exchange Management **Shell** and type the following command:

New-ExchangeCertificate -GenerateRequest -RequestFile “path_to_csr.txt” -FriendlyName “friendly_name” -SubjectName “c=Country,s=State,l=Locality,o=Organization,ou=Organizational_Unit,cn=Common_Name” -DomainName additional.domain.com -PrivateKeyExportable $true

Here is a short description of the commands:

- **RequestFile**: the path to the folder where the .txt or .req file with the text of the CSR will be stored. In our example, we saved the file to the disc C://, folder “certs”.
- **FriendlyName**: this field is used by the server administrator to identify the CSR later.
- **SubjectName**: these details will be checked by the Certificate Authority before CSR issuance.
- **Country**: two-digit code of the country your domain is operating/registered in.
- **State**: the full name of the state/province/region inside the country. If there are no states or regions in your country, you can use the city name in this field.
- **Locality**: the full name of the city.
- **Organization**: the full registered name of your organization. You can enter NA here if you do not have a company, as Certificate Authorities do not verify the company for domain-validated (DV) certificates. Usually, it is enough to use the domain-validated certificate to secure Exchange services.
- **Organizational Unit**: the name of the department inside the company. If there is no department in your company, you may enter NA.
- **Common Name**: the domain name you need to secure. This will become the primary domain of your multi-domain certificate.
- **DomainName**: any additional domain(s) which will take one of the slots in your certifiacate.
- **PrivateKeyExportable $true**: this part of the command means that you allow exporting the private key from the server. It should be used if you are going to export the certificate later and install it on the other server. Using “$false” here or excluding this part from the command will not allow the private key to be exported and will cause issues with using the certificate on other servers.

Note: use only alphanumeric letters and digits and avoid using any special characters like “/”, “&”, “å”, etc.

```
[PS] C:\Windows\system32>New-ExchangeCertificate -GenerateRequest -RequestFile "C:\certs\mailshellcsr.txt" -FriendlyName
 "mailshell" -SubjectName "c=US,s=California,l=Los Angeles,o=Namecheap,ou=SSL,cn=mail.ncssltest.info" -DomainName autodi
scover.ncssltest.info -PrivateKeyExportable $true
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEIzCCAwsCAQAweDEcMBoGA1UEAwwTbWFpbC5uY3NzbHRlc3QuaW5mbzEMMAoG
A1UECwwDU1NMMRIwEAYDUQQKDAlOYW1lY2hlYXAxFDASBgNVBAcMC0xvcyBBbmdl
bGVzMRMwEQYDUQQIDApDYWxpZm9ybmlhMQswCQYDUQQGEwJUUzCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAM895MmNwlfRnXIjj8RWFATbvP4yPDZIXNFm
KsWHd0meufWcegQSbL1ljF7s9VlBHrWnWoSuN33eKDoID0int0KmHRoiAbHanDn+
AXK2LhdHoQhCg/ssLyNW4LytvrSZgGZ3hciyodE+3cxWA7L2Z8UdRq7BKCF86B2v
dkvZ/M5weUSlvvK+O1z7YSxn01ueTi1bu7MI4w+kGRH3UYTOk5AqqpQFB+d3RlzY
hQ6dd3YvhM/8EbtKni0YwnaEh7ogxiV1slv/8nXQtstv8cn7aNypc4NelZnCQuiC
DxAJEfzEUNIxflwd83okIItxDyDQu8JXaKOVRK728YEdlpW6ef8CAwEAAaCCAWQw
GgYKKwYBBAGCNw0CAzEMFgo2LjIuOTIwMC4yMFwGCSsGAQQBgjcVFDFPME0CAQUM
E21haWwubmNzc2x0ZXN0LmluZm8MD05DU1NMUEVTUFxNQUlMJAwiTWljcm9zb2Z0
LkV4Y2hhbmdlLlNlcnZpY2VIb3N0LmV4ZTByBgorBgEEAYI3DQICMWQwYgIBAR5a
AE0AaQBjAHIAbwBzAG8AZgB0ACAAUgBIAEEAIABIAEMAaABhAG4AbgBlAGwAIABD
AHIAeQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBpAGQAZQByAwEAMHQG
CSqGSIb3DQEJDjFnMGUwDgYDVR0PAQH/BAQDAgWgMCYGA1UdEQQfMB2CG2F1dG9k
aXNjb3Zlci5uY3NzbHRlc3QuaW5mbzAMBgNVHRMBAf8EAjAAMB0GA1UdDgQWBBSn
yNiFyuVDEEuwM/r2uTCceyVImTANBgkqhkiG9w0BAQUFAAOCAQEAmGts3pzbUT+A
dMcqM0qAFOGJYPPFYinW8bYwfgY8qvdcitb4GCNhq+Fq85k6Up6lwZgbuHw2xza4
jR+GheCgmnaSrQ0eMJPPu6dMv1nfnW2dwi/5XQkeaLjlfGw4SvBdVIU9eDuEZhyD
IpDuFrKzMAu7sUfmJkDJcpi8DznH5FkP3WsWGU03tcqQ4EnIzqA4+pxoqDb1Ryfj
bmxAJ0UY6DWYEjLiijwn367K0z3223mw8/iszXblOyn+JKz82Xxb/2QMxrsfmZD3
CXFMpS0aROQK/lBNUqVuEt9ywiGUbFjfn8Tk2HjgmnKXB82+rFpvonl+qSHNwC2d
wM8jpEA+aQ==
-----END NEW CERTIFICATE REQUEST-----
```

The file is stored on your computer in the folder you specified in the “-RequestFile” command.
You may now activate your certificate using the CSR text. Remember that it is necessary to use the whole text, including Begin and End lines.