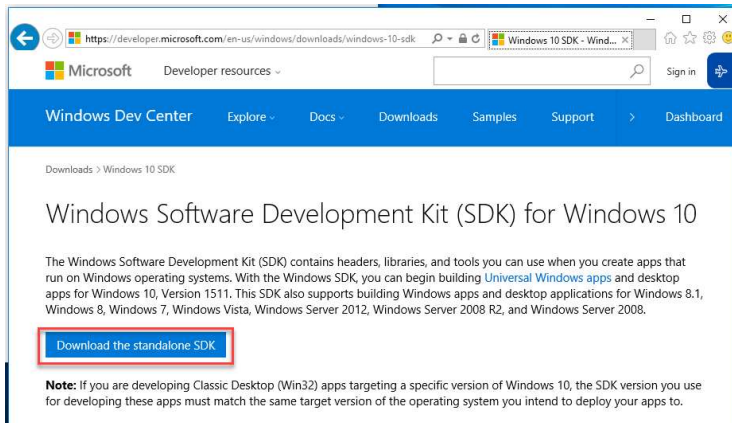# To create a self-signed root certificate
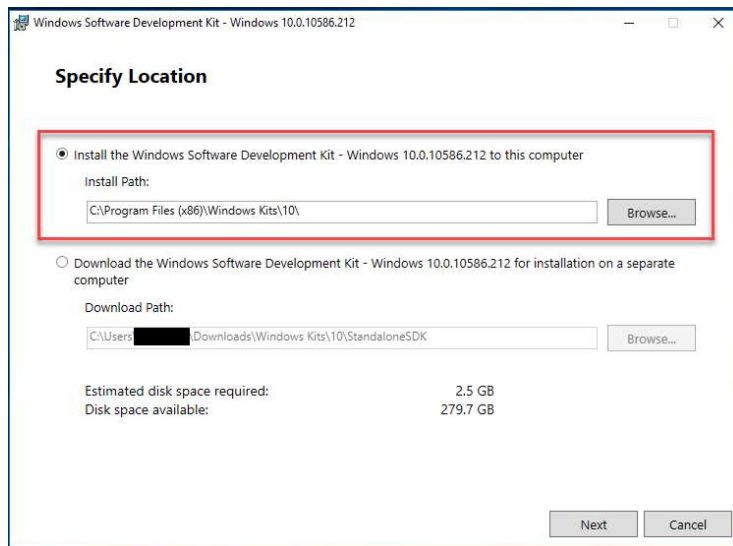
Tuesday, July 19, 2016   4:10 PM

For instructions to create a self-signed root certificate using *makecert*, see Working with self-signed root certificates for Point-to-Site configurations.
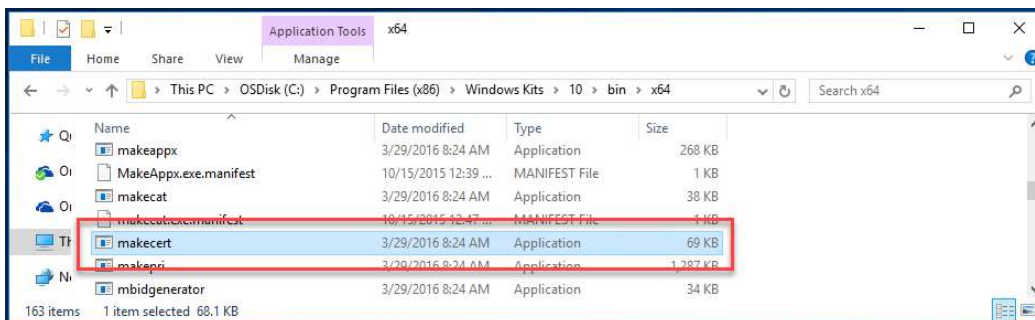
1. Download

2. Install with all default options.

3. Once Installation is complete . you can find the makecert.exe utility under this path: C:\Program Files (x86)\Windows Kits\10\bin<arch>.

4. Now, open a command prompt as administrator and run following commands as administrator, where *RootCertificateName* is the name that you want to use for the certificate.

C:\windows\system32>cd C:\Program Files (x86)\Windows Kits\10\bin\x64

C:\Program Files (x86)\Windows Kits\10\bin\x64>makecert -sky exchange -r -n "CN=RootCertificateName" -pe -a sha1 -len 2048 -ss My "RootCertificateName.cer"
Succeeded
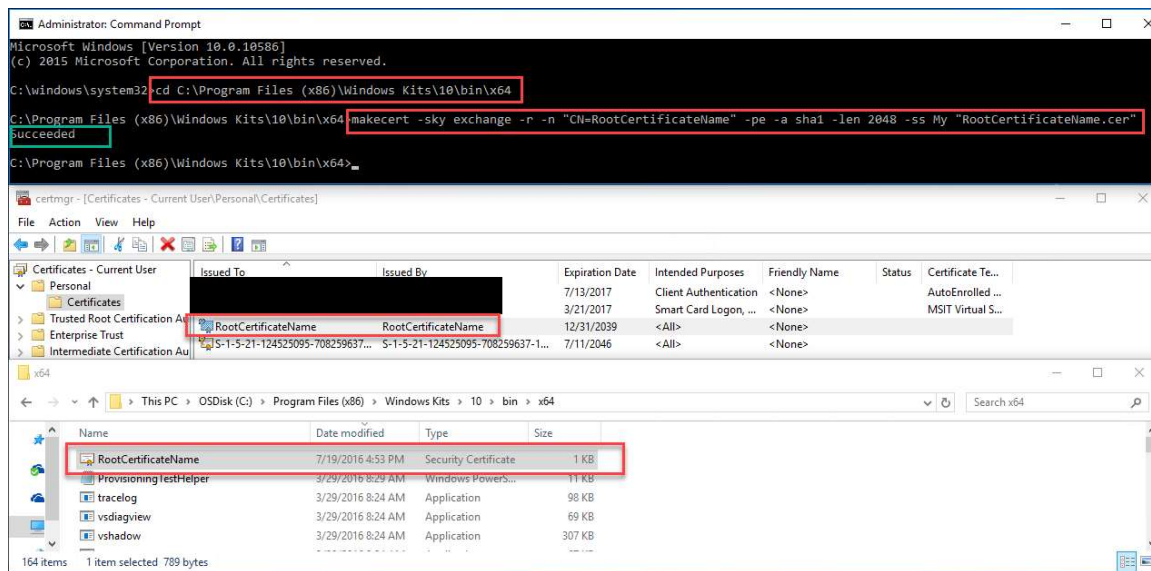
5. The .cer file should not contain the private key of the root certificate.
6. To get the public key export the .cer file as a Base-64 encoded X.509 (.CER) file.

➢ Right Click the certificate choose All Task > Export
➢ Choose Default setting on first two screen.
➢ Choose (Base-64 encoded X.509 (.CER)) on Export File Format > Click Next .

➢

➢ Choose desired location to save the file .

7. Now open that file with notepad. There copy everything in between: -----BEGIN CERTIFICATE----- & -----END CERTIFICATE-----

To generate Client Certificate :

Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\windows\system32>cd C:\Program Files (x86)\Windows Kits\10\bin\x64

C:\Program Files (x86)\Windows Kits\10\bin\x64>makecert.exe -n "CN=ClientCertificateName" -pe -sky exchange -m 96 -ss My -in "RootCertificateName" -is my -a sha1
Succeeded

C:\Program Files (x86)\Windows Kits\10\bin\x64>

makecert.exe -n "CN=ClientCertificateName" -pe -sky exchange -m 96 -ss My -in "RootCertificateName" -is my -a sha1

To export a client certificate

1. To export a client certificate, use *certmgr.msc*. Right-click the client certificate that you want to export, click all tasks, and then click export. This will open the Certificate Export Wizard.

2. In the Wizard, click Next, then select Yes, export the private key, and then click Next.

3.
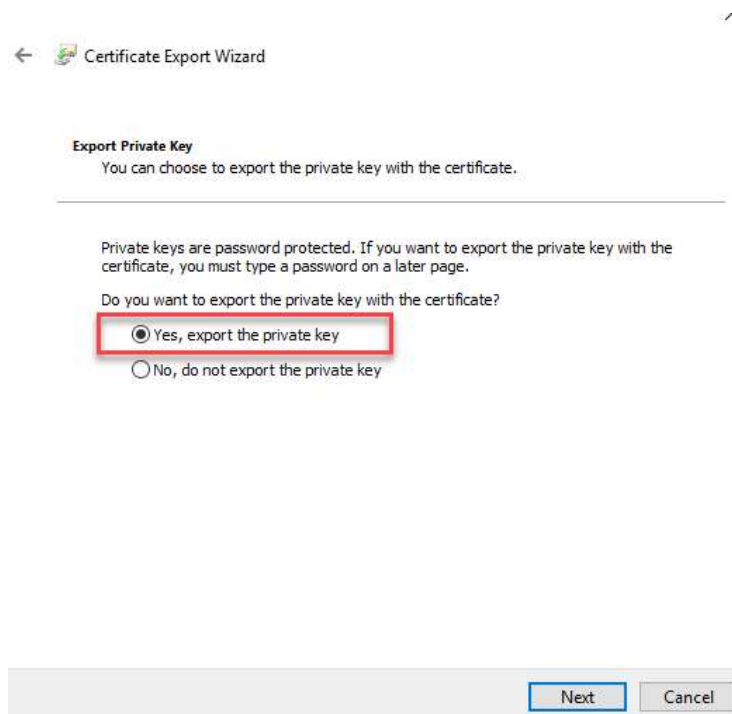
4. On the Export File Format page, you can leave the defaults selected. Then click Next.

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

☐ Include all certificates in the certification path if possible

◉ Personal Information Exchange - PKCS #12 (.PFX)

☑ Include all certificates in the certification path if possible

☐ Delete the private key if the export is successful

☐ Export all extended properties

☐ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

[Next] [Cancel]

5. On the Security page, you must protect the private key. If you select to use a password, make sure to record or remember the password that you set for this certificate.Then clickNext.

Security
To maintain security, you must protect the private key to a security principal or by using a password.

☐ Group or user names (recommended)

[   ] [Add]
                       [Remove]

☑ Password:
[••••••••]

Confirm password:
[••••••••|]

[Next] [Cancel]

6. On the File to Export, Browse to the location to which you want to export the certificate. For File name, name the certificate file. Then click Next.

7. Click Finish to export the certificate.