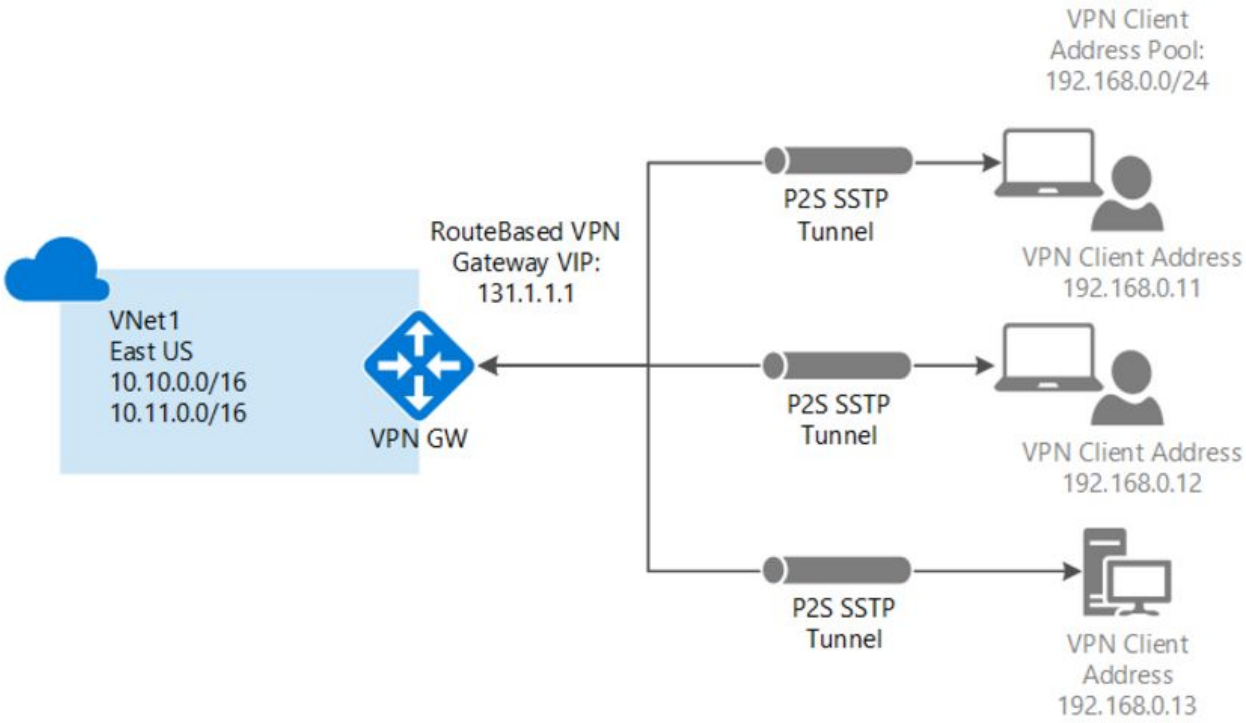
Configure a Point-to-Site VPN connection to a VNet using the classic portal



#Part 1

```
Login-AzureRmAccount
Select-AzureRmSubscription -SubscriptionName "Microsoft Azure
Sponsorship"
$VNetName  = "Aneka-VNET-SITE"
$FESubName = "FrontEnd"
$BESubName = "Backend"
$GWSubName = "GatewaySubnet"
$VNetPrefix1 = "192.168.0.0/16"
$VNetPrefix2 = "10.254.0.0/16"
$FESubPrefix = "192.168.1.0/24"
$BESubPrefix = "10.254.1.0/24"
$GWSubPrefix = "192.168.200.0/26"
$VPNClientAddressPool = "172.16.201.0/24"
```

```
$RG = "Adel_Aneka_Test"
$Location = "Australia Southeast"
$DNS = "8.8.8.8"
$GWName = "GW"
$GWIPName = "GWIP"
$GWIPconfName = "gwipconf"
```
#Create a new resource group.
```
New-AzureRmResourceGroup -Name $RG -Location $Location
```
#Create a front-end, gateway and backend subnet
```
$fesub = New-AzureRmVirtualNetworkSubnetConfig -Name $FESubName
-AddressPrefix $FESubPrefix
$besub = New-AzureRmVirtualNetworkSubnetConfig -Name $BESubName
-AddressPrefix $BESubPrefix
$gwsub = New-AzureRmVirtualNetworkSubnetConfig -Name $GWSubName
-AddressPrefix $GWSubPrefix
```

#Create a virtual network

```
New-AzureRmVirtualNetwork -Name $VNetName -ResourceGroupName $RG
-Location $Location -AddressPrefix $VNetPrefix1,$VNetPrefix2 -Subnet
$fesub, $besub, $gwsub -DnsServer $DNS
```
#Specify the variables for the virtual network you just created.

```
$vnet = Get-AzureRmVirtualNetwork -Name $VNetName -ResourceGroupName
$RG
$subnet = Get-AzureRmVirtualNetworkSubnetConfig -Name "GatewaySubnet"
-VirtualNetwork $vnet
```
#Request a dynamically assigned public IP address. This IP address is necessary for the gateway to work properly. You will later connect the gateway to the gateway IP configuration
```
$pip = New-AzureRmPublicIpAddress -Name $GWIPName -ResourceGroupName
$RG -Location $Location -AllocationMethod Dynamic
$ipconf = New-AzureRmVirtualNetworkGatewayIpConfig -Name
$GWIPconfName -Subnet $subnet -PublicIpAddress $pip
```
 # Generate and upload certificates: for doing this follow the instruction after this code and copy the public key of the generated certificate here
```
$MyP2SRootCertPubKeyBase64 = "MIIDETCCAf2g…….j4/FrCI"
$p2srootcert = New-AzureRmVpnClientRootCertificate -Name
$P2SRootCertName -PublicCertData $MyP2SRootCertPubKeyBase64
New-AzureRmVirtualNetworkGateway -Name $GWName -ResourceGroupName $RG
-Location $Location -IpConfigurations $ipconf -GatewayType Vpn
-VpnType RouteBased -EnableBgp $false -GatewaySku Standard
```

```
-VpnClientAddressPool $VPNClientAddressPool
-VpnClientRootCertificates $p2srootcert
```

Part 2: generate a root certificate

If you are not using an enterprise certificate solution, you'll need to generate a self-signed root certificate. The steps in this section were written for Windows 7 (Should be similar for other Windows with some minor changes).

You can follow either of the following methods:

1. Run command prompt of windows as administrator (right click on command prompt, run as administrator).
2. Change directory to the location of `makecert.exe`.
    a. For my case: `cd C:\Program Files (x86)\Microsoft SDKs\Windows\v7.0A\Bin`
3. Run this command:

```
makecert -sky exchange -r -n "CN=RootCertificateName" -pe
-a sha256 -len 2048 -ss My "RootCertificateName.cer"
```

`RootCertificateName` is the name of root certificate authority (CA), it can be your name. `RootCertificateName.cer` is the name of the file to store this certificate.

`-r` means create a self-signed certificate

`-ss` is the certificate store name that store the output certificate

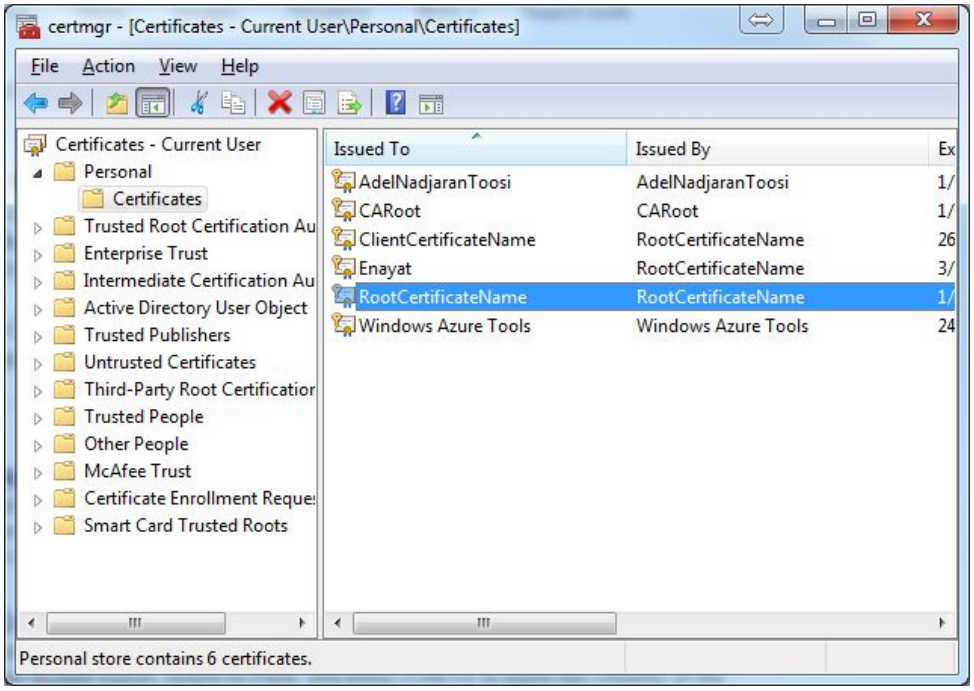
`-a` and `-len` are used for encryption algorithm and length of the key.

By executing this command your self-signed certificate will be added to CurrentUser store location.

Part 2.1: To get the public key

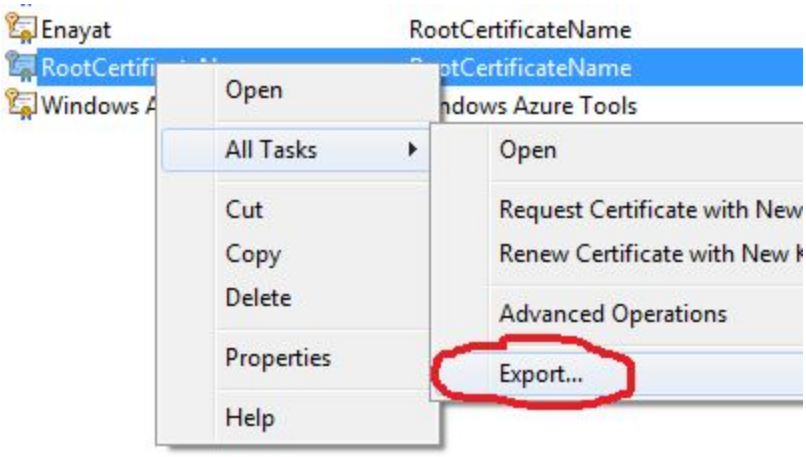
1. First, check that your certificate from previous section is added to your personal certificates.

a. Run `certmgr.msc`, your Certificate should be there in personal certificates.

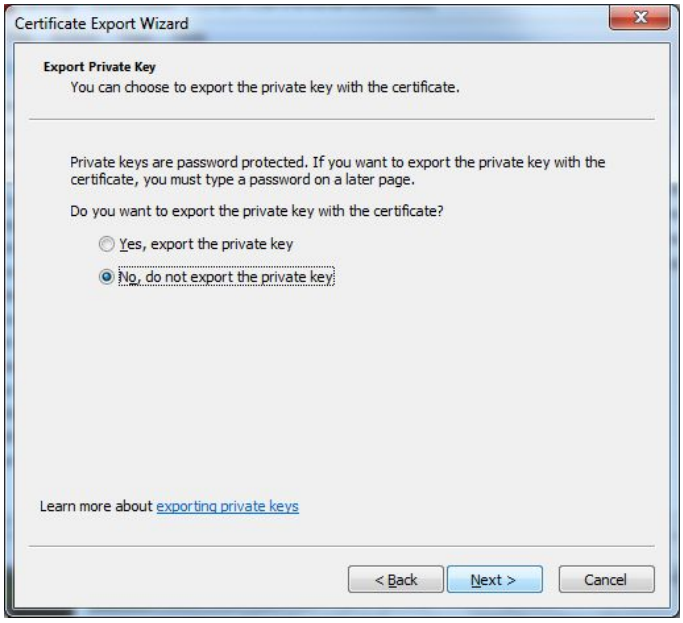


2. To get the public key, export the .cer file as a Base-64 encoded X.509 (.CER) file then open that file with notepad. There copy everything in between: -----BEGIN CERTIFICATE----- & -----END CERTIFICATE-----

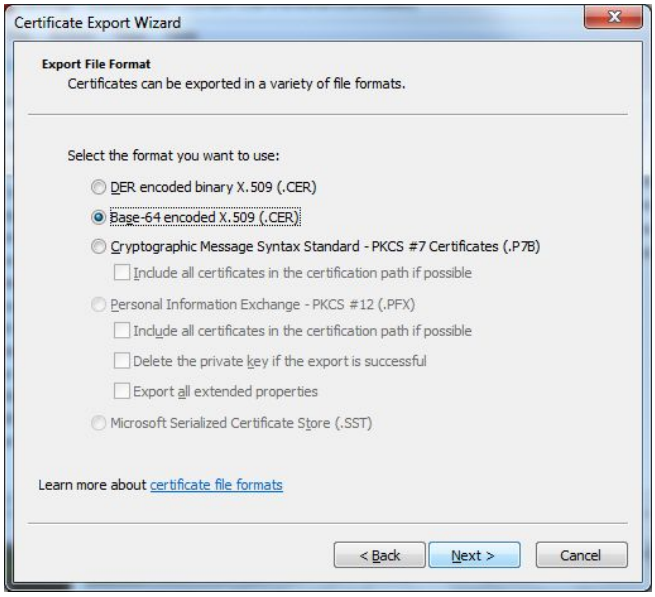
a. Right click on the RootCertificate you created> all Tasks> Export



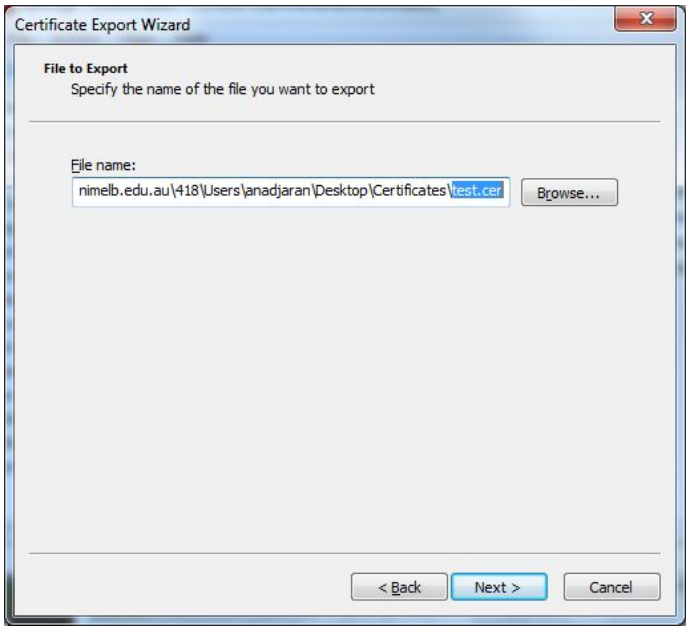
b. Select No, do not export the private key



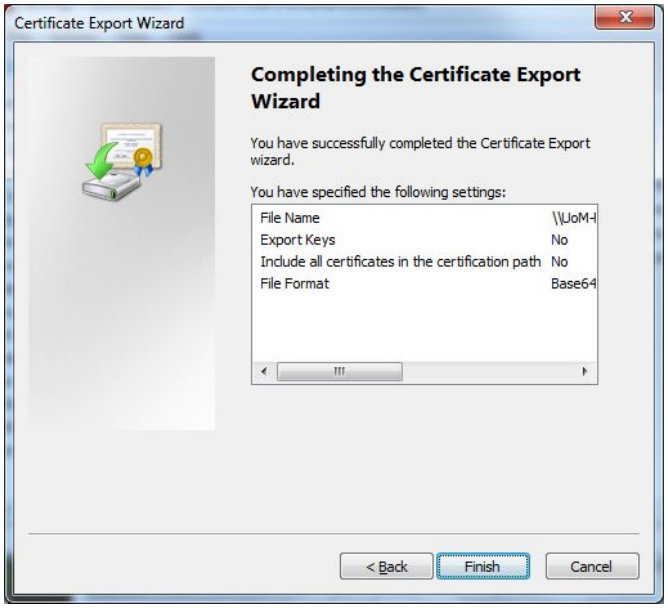
c. Select Base-64 encoded X.509 (.CER)



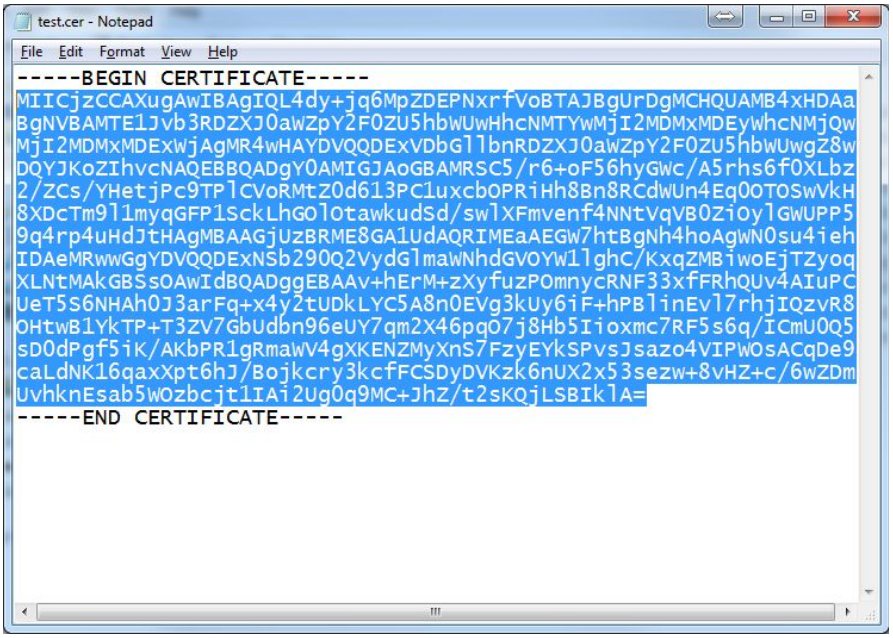
d. Select a path and a name for your certificate file



e. Next and finish.



f. Open the file you saved with notepad and make a single line form of the public key between -----BEGIN CERTIFICATE----- & -----END CERTIFICATE-----



g. This is the public you should be copied to `$MyP2SRootCertPubKeyBase64` variable in # Part 2.1 of the creation of VPN.

Part 3

If your virtual network is created successfully (you can check in Azure portal) now you can connect clients to the virtual network. For doing so you need two things:

1) the VPN client and

2) a client certificate installed.

Part 3.1 Download the VPN client configuration package.

1. To download the client configuration package, run the following commands in powershell. Make sure Azure Resource Manager PowerShell cmdlets is installed (You can use the Microsoft Web Platform

Installer from this address:

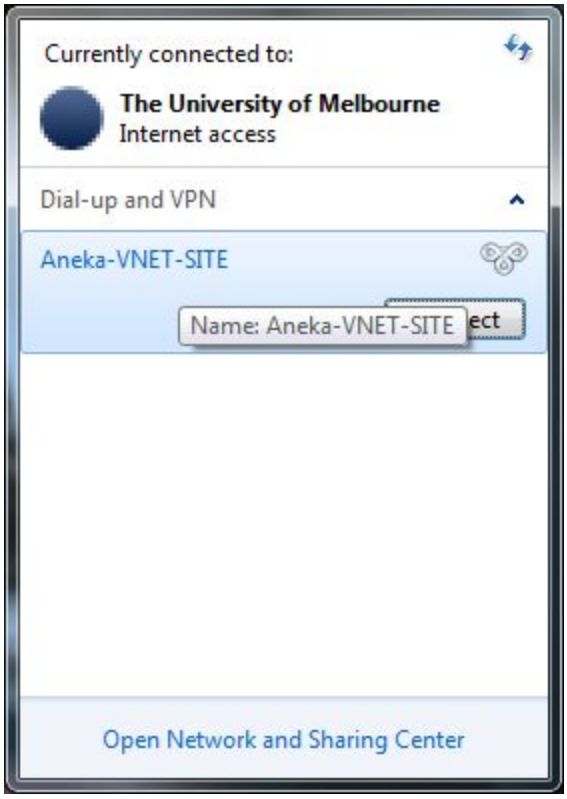
https://www.microsoft.com/web/downloads/platform.aspx)

```
Get-AzureRmVpnClientPackage -ResourceGroupName $RG
-VirtualNetworkGatewayName $GWName
-ProcessorArchitecture Amd64
```

Manual Download:

To download the client VPN manually, visit the microsoft Azure portal and select Resource Groups > [Resource Group Name] > [Gateway Name] , and click on download VPN client.

2. The PowerShell cmdlet will return a URL link. Copy-paste the link that is returned to a web browser to download the package to your computer.
3. Instal the package. You should see the VPN connection on by clicking on your network access icon on tray.



Part 3.2 Generate and install the client certificates.

Follow these steps and generate a certificate for each computer needs to be connected to the virtual network.

Look here if you are not sure what you are doing.
(https://docs.microsoft.com/en-in/azure/vpn-gateway/vpn-gateway-certificates-point-to-site)

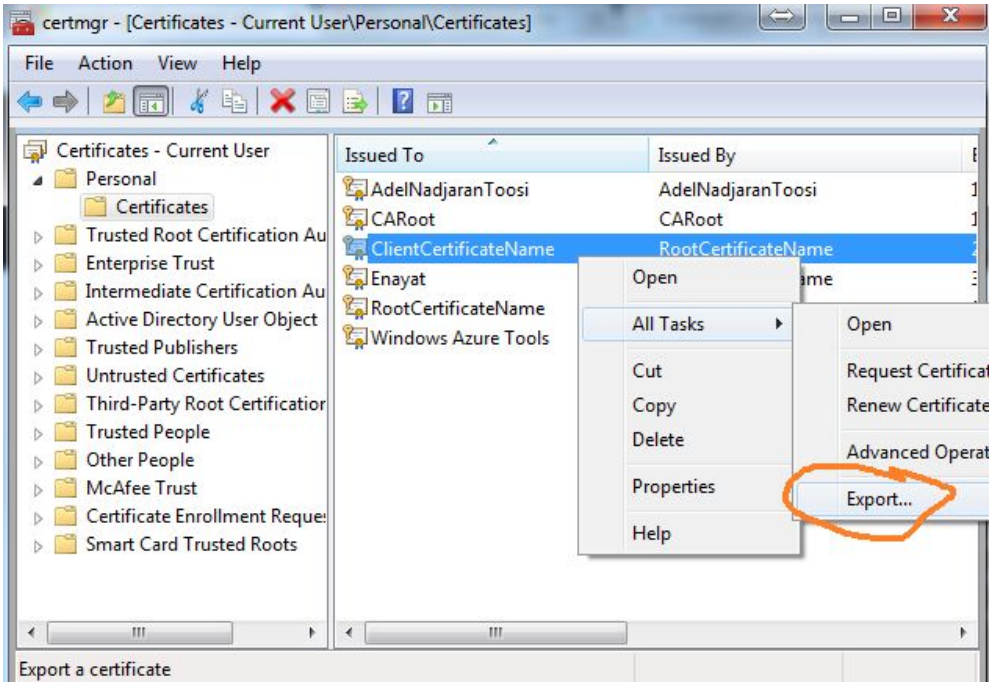
1. First run the following command to generate the Client certificate.

   ```
   makecert.exe -n "CN=ClientCertificateName" -pe -sky exchange -m 96 -ss My -in "RootCertificateName" -is My -a sha256
   ```

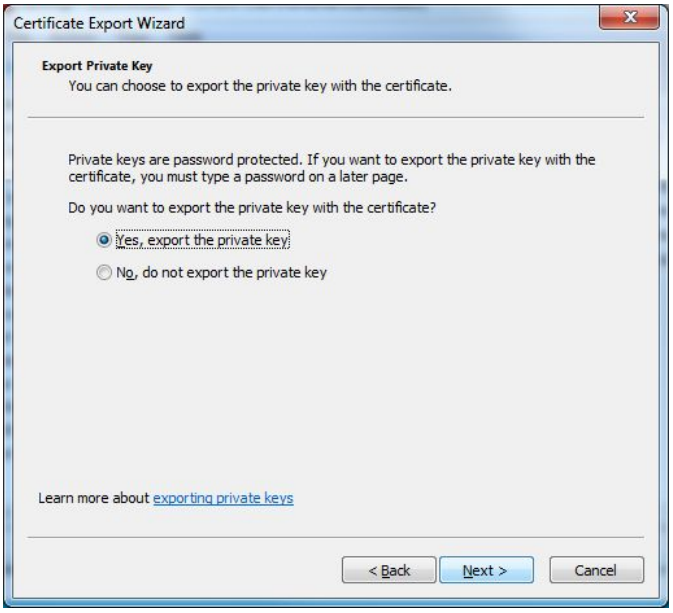
   You can generate as many as client certificate you need this way. If you do not have makecert.exe, you can install it with **Microsoft Windows SDK for Windows 7 and .NET Framework 4.** Find it in C:\

2. Run `certmgr.msc` Make sure the `ClientCertificateName` is added to your personal certificates.

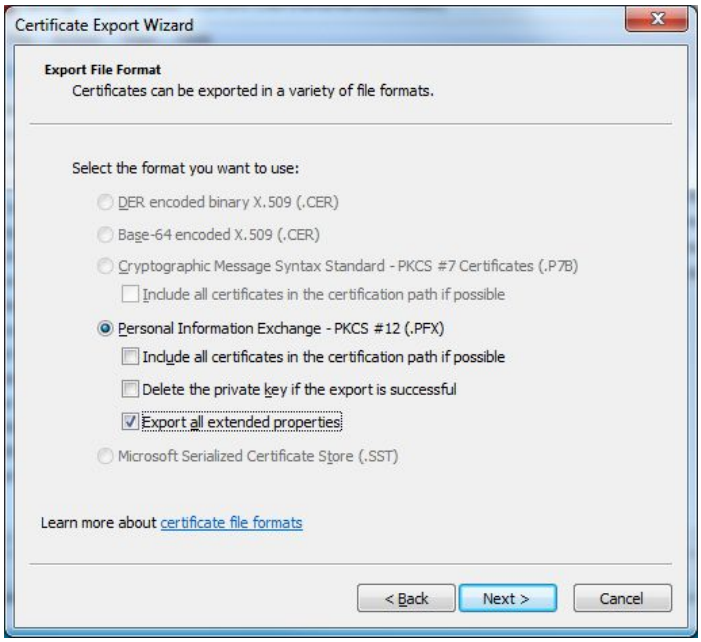
3. Right click on the Client Certificate and export



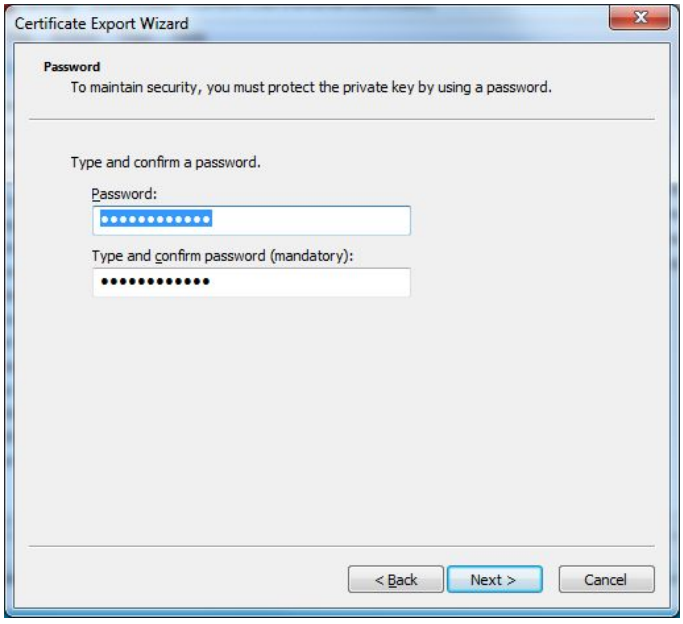
4. Select, Yes export the private key



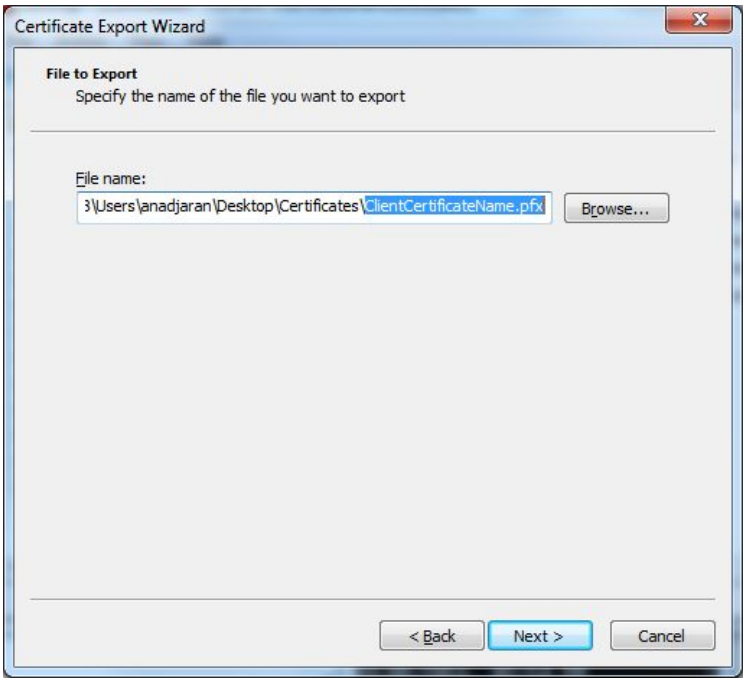
5. Leave the default selection:



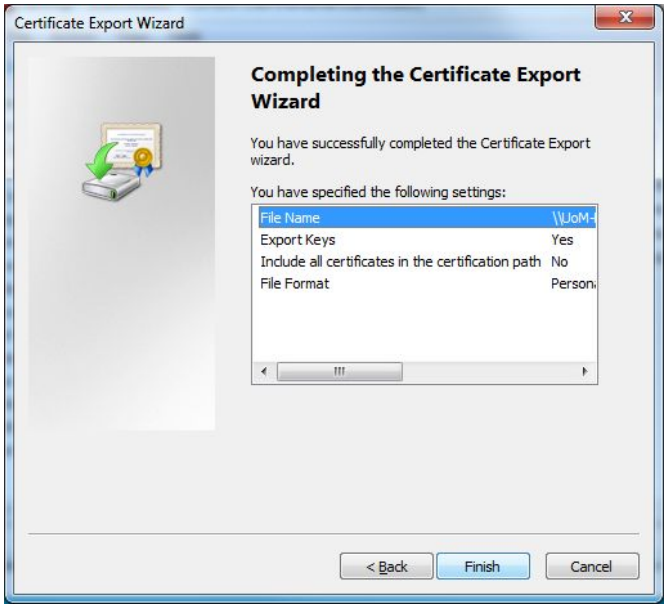
6. Provide a password for the private key



7. Select a path and a name for your certificate file.

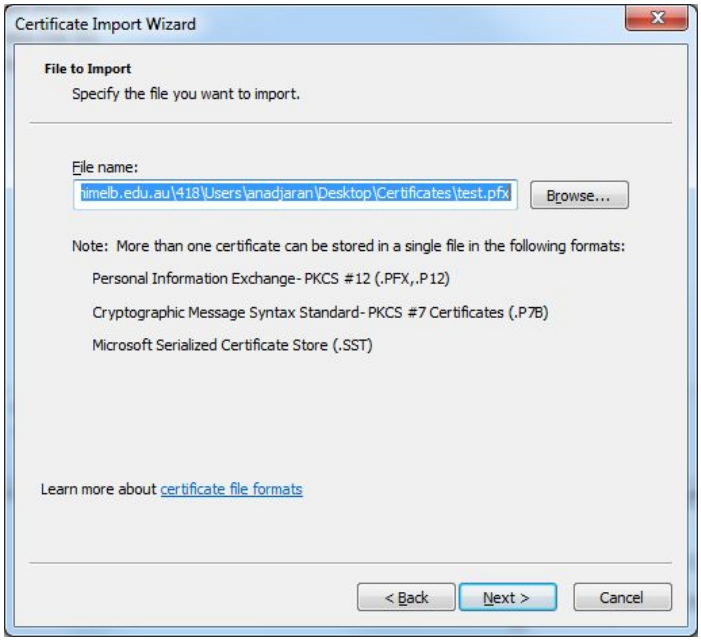


8. Next and finish.

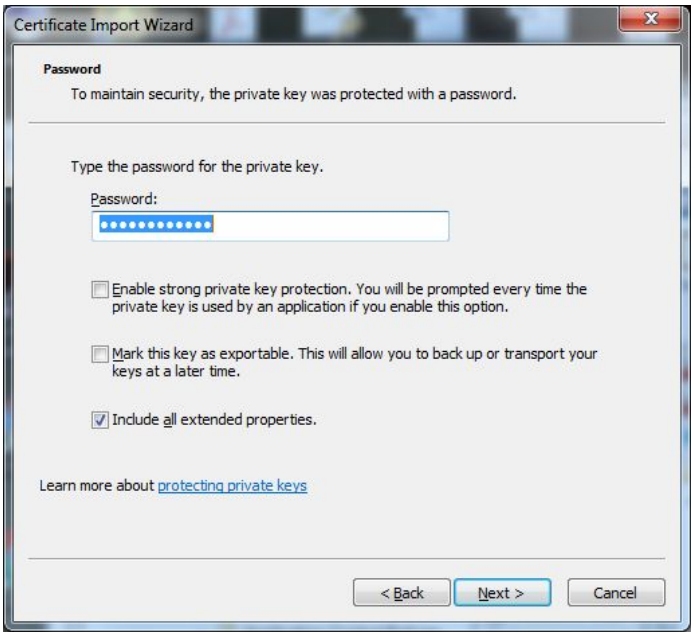


9. Then copy the exported .pfx file to the target machine wants to connect to the virtual network.
10. Double click on the file on the target machine and follow the steps:
    a. Next,

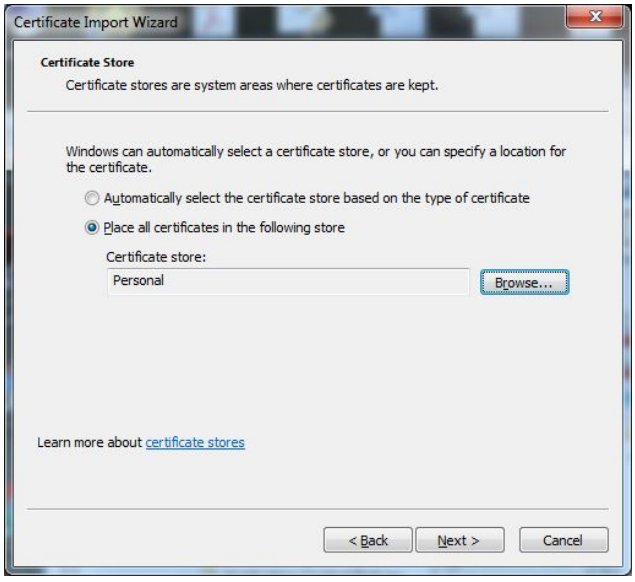
b. Leave the path as it is,



c. Type the password for the private key and make sure Enable strong key protection is not checked. If this option is grayed out you should follow the instruction in part 4to make it selectable.



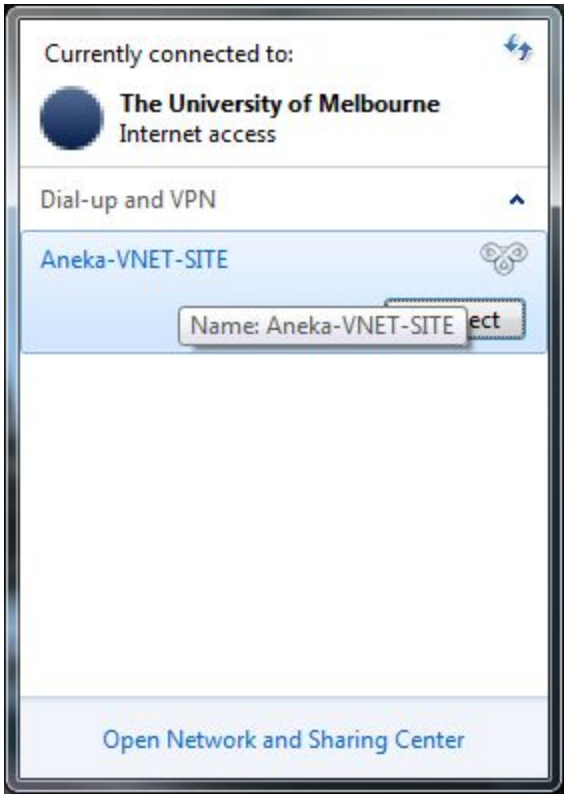
d. Next and select Place all certificates in the following store and browse and find personal.

e. 

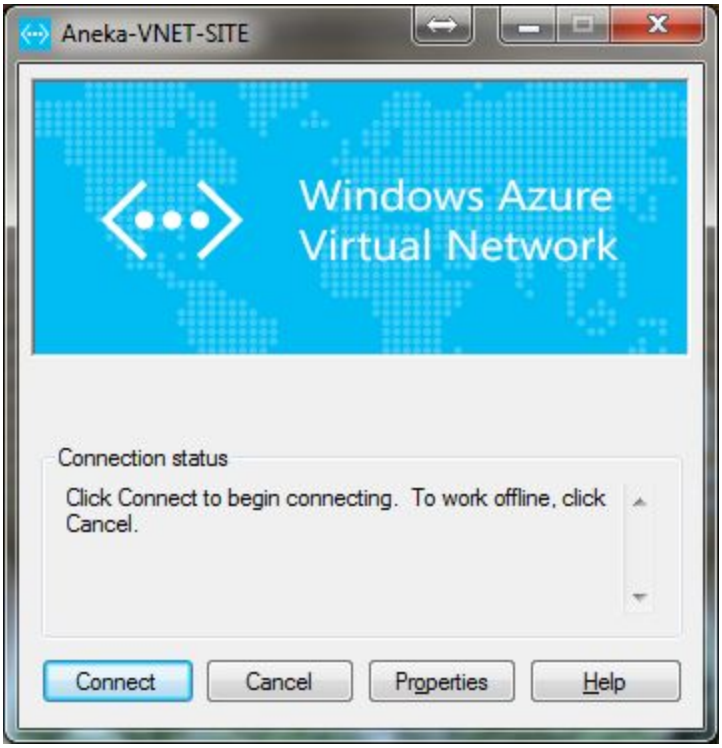
f. Next and finish.

Part 3.3 Connect to the VPN

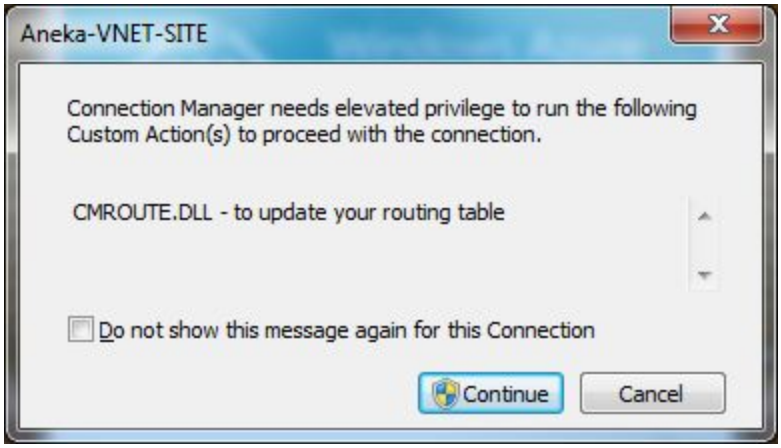
a. Click on connect button on your VPN connection created on part 3.1.3.



b. Click on connect.



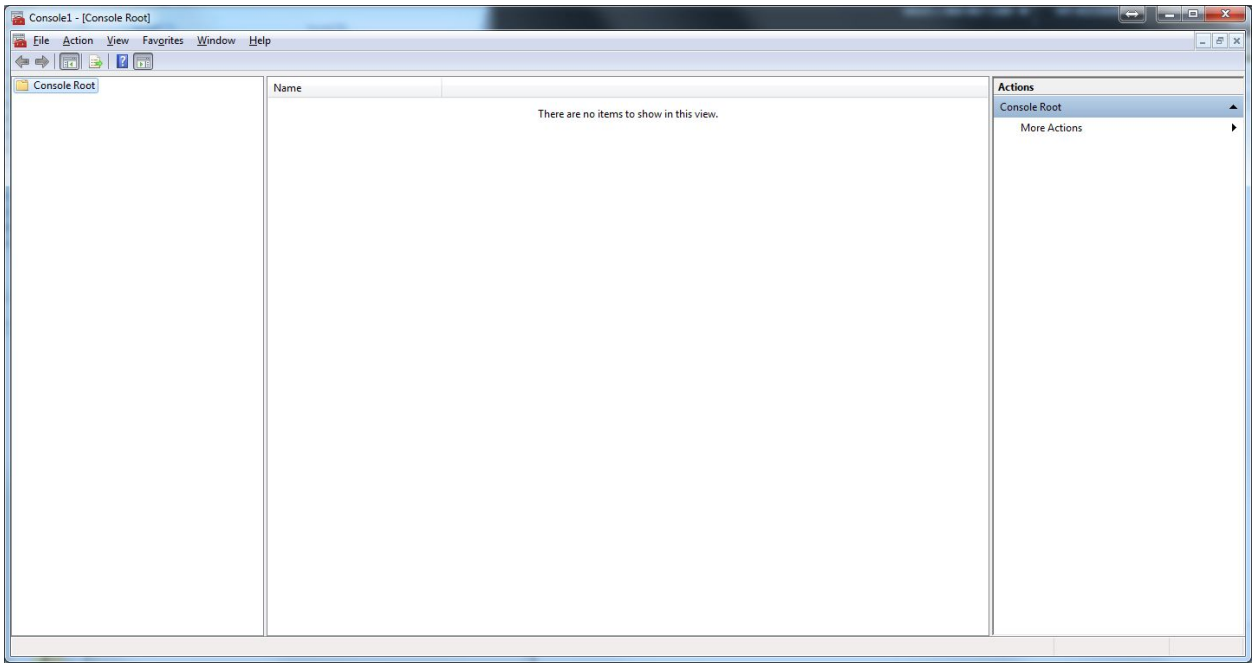
c. Click on continue and accept yes.



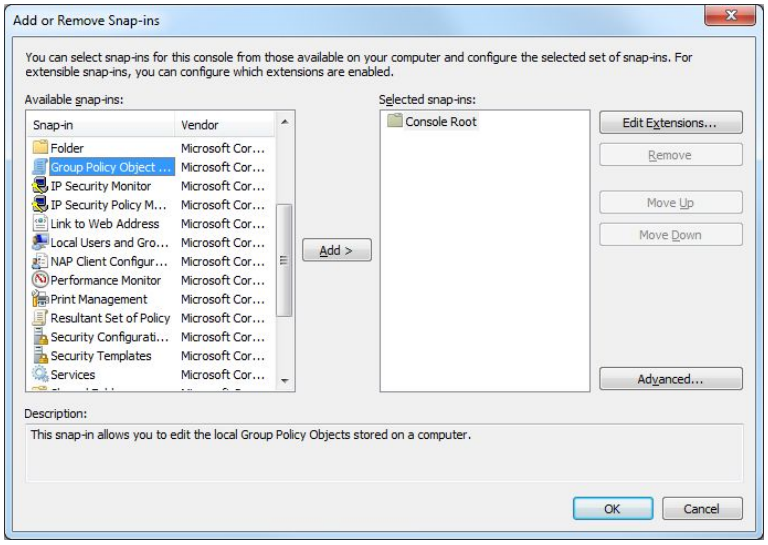
d. Select client certificate you imported and ok, if installed more than one certificate, otherwise it will connects automatically.
e.

Part 4 Enable Strong private key protection.

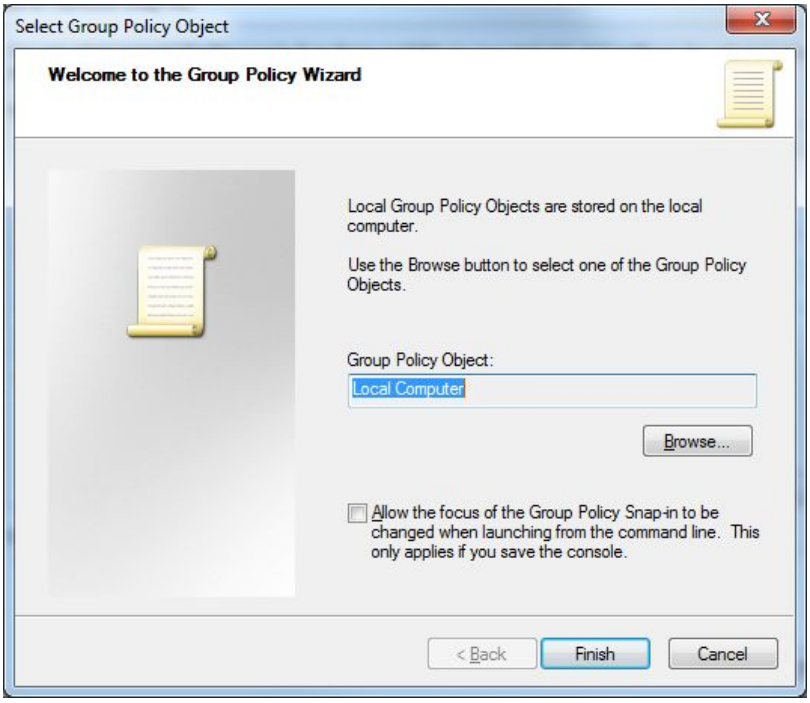
a. Open the mmc.exe on run prompt



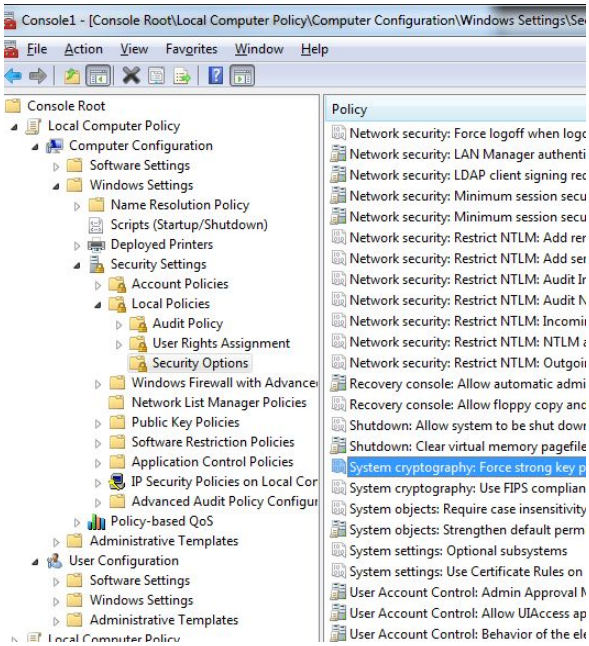
b. File add/Remove Snap-ins, double click on Group policy object:



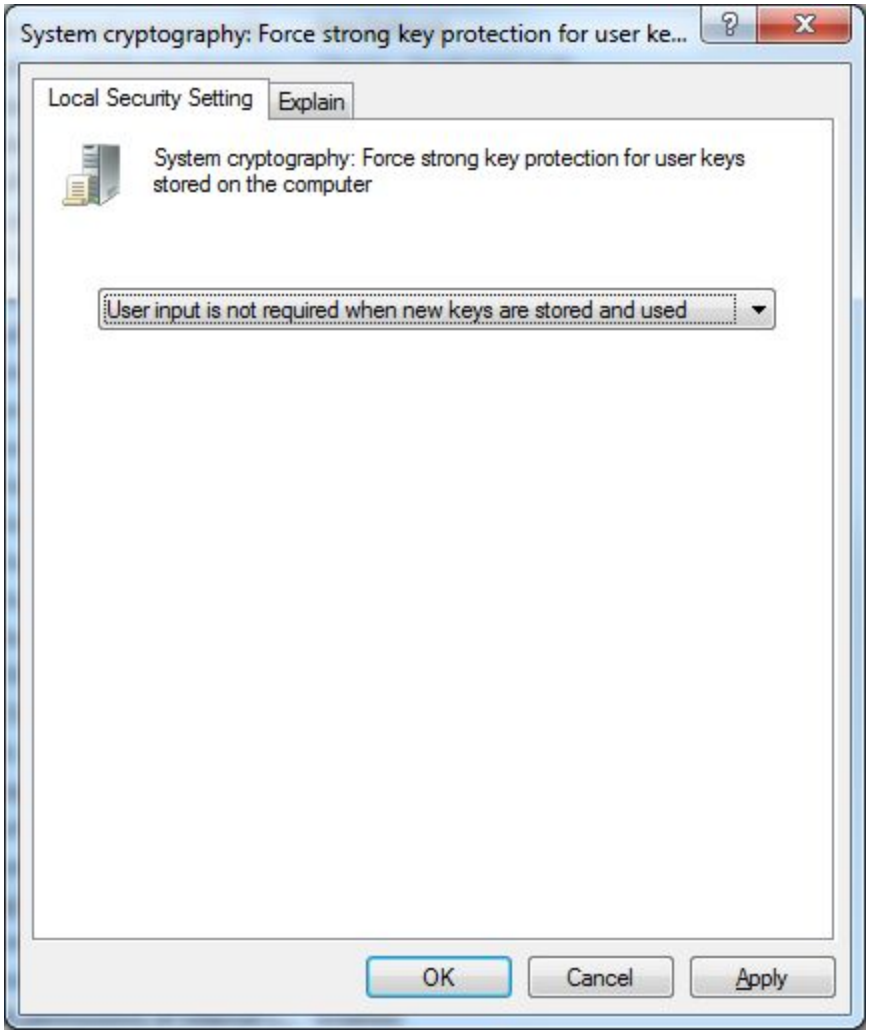
c. Just finish and ok.



d. Open computer configuration> windows Settings> Security Settings> Local Policies>Security Options on the right panel. Then find System Cryptography: Force Strong key protection for user key stored on the computer and open it.



e. Select User is not required when keys are stored and used



f. Apply and ok.

Part 5 To add and remove extra Root Certificates.

You can add up to 20 root certificates to Azure. Follow the steps below to add a root certificate.

1. Create and prepare the new root certificate for upload based on method explained in #part 2, the run following powershell commands:

```
Login-AzureRmAccount
$P2SRootCertName2 = "ARMP2SRootCert2.cer"
$MyP2SCertPubKeyBase64_2 = "MIIC/zC……...m7ju"
```

2. Upload the new root certificate. Note that you can only add one root certificate at a time.

```
Add-AzureRmVpnClientRootCertificate
-VpnClientRootCertificateName $P2SRootCertName2
```

```
-VirtualNetworkGatewayname $GWName -ResourceGroupName $RG
-PublicCertData $MyP2SCertPubKeyBase64_2
```

3. You can verify that the new certificate was added correctly by using the following cmdlet.

```
Get-AzureRmVpnClientRootCertificate -ResourceGroupName $RG
-VirtualNetworkGatewayName $GWName
```

4. You can remove a certificate using the following cmdlet.

```
Remove-AzureRmVpnClientRootCertificate
-VpnClientRootCertificateName $P2SRootCertName2
-VirtualNetworkGatewayName $GWName -ResourceGroupName $RG
-PublicCertData "MIIC/z……qgTWCIcb7ju"
```