Mac OSX Certificate Enrollment Procedure

1. Log on to your Macintosh machine, open a terminal to create a key:
   openssl genrsa -des3 -out dpvpn-cert.key 1024

2. Create a CSR file with the newly created key (make sure that the CN is a simple name, no spaces or special characters):
   openssl req -new -key dpvpn-cert.key -out dpvpn-cert.csr

   NOTE: Correct information must be provided in the below fields so as to allow Datapipe to review and approve your certificate request.

   *Organization = company
   *Organization unit = tunnel-group
   Common Name (your name or whatever, if you have more than one certificate, please make sure the “Comomn Name” in use is unique so that you can easily identify the certificate for the VPN setup)
   Email Address

   *These attributes must match with the firewall configuration, please refer to the Certificate Enrollment Access List for information.

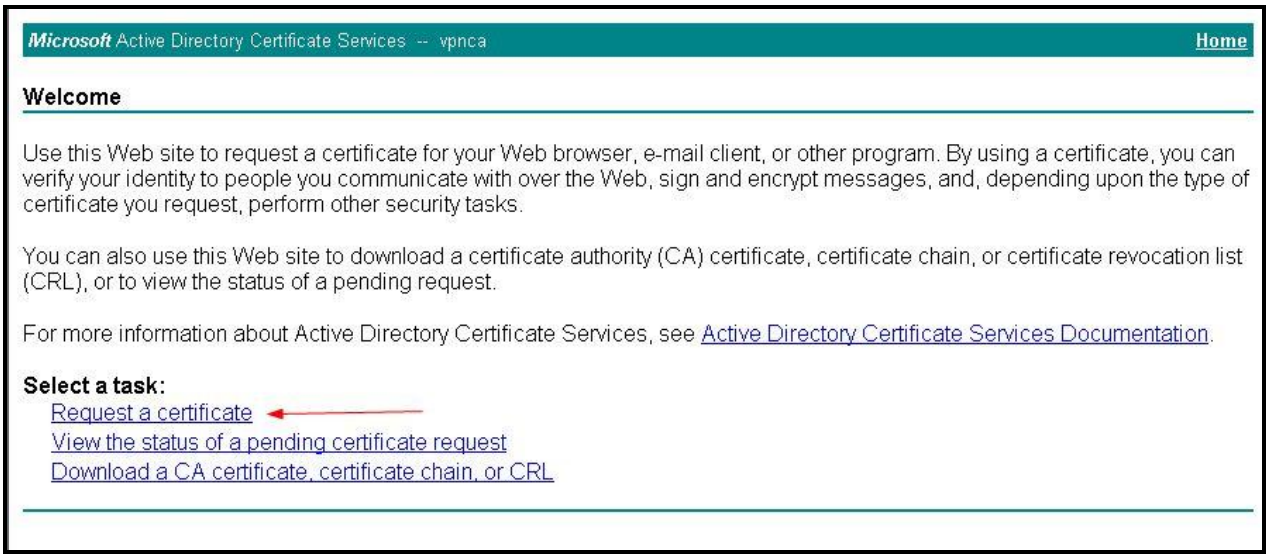
```
$
$ openssl req -new -key dpvpn-cert.key -out dpvpn-cert.csr
Enter pass phrase for dpvpn-cert.key:
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:.
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) [Internet Widgits Pty Ltd]: COMPANY-NAME
Organizational Unit Name (eg, section) []: TUNNEL-GROUP
Common Name (eg, YOUR name) []: YOUR-NAME (if you have more than one certificate, please make sure the “Comomn Name” in use is unique so that you can easily identify the certificate for the VPN setup)
Email Address []: YOUR-EMAIL-ADDRESS

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: ANY-PASSWORD
An optional company name []:.
$
$
$ ls -l
total 8
-rw-r----- 1 klo klo 651 2012-10-12 15:50 dpvpn-cert.csr
-rw-r----- 1 klo klo 958 2012-10-12 15:44 dpvpn-cert.key
$
$
klo@ltsp03:~/tmp/cer$ more dpvpn-cert.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIBpzCCARACAQAwTjENMAsGA1UEChMEZXdheTEMMAoGA1UECxMDYWxsMQ4wDAYD
VQQDEwVrZW5ueTEfMB0GCSqGSIb3DQEJARYQa2xvQGRhdGFwaXBlLmNvbTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAtwJRdFuuVSvQfEsHdExnwYNd1XIXmY8N
LOVlRdQxNYJ5BOCL+W9eq7pxY3S8fwHa2D0+GMA+Vm/Gy7gmdGiJN9rh2asEjO3B
jT3XbKB3D+HrSLRQyMQbmpCmRqOnowFKc8OdVBnWVGhRGSEVU1548kqOWW5daTIn
Cj4/JG1qbl8CAwEAAaAZMBcGCSqGSIb3DQEJBzEKEwhjZXJ0MTIzNDANBgkqhkiG
9w0BAQUFAAOBgQCDU+AGbjz+LxRaTVFLuSP4gs6SfTfNfbNt8tg0BDjE8q2ozcsm
+GgtDo1YubjWuKVhe69vt6kpzC0cQaTw35NerUixi7Ndc12srNxBhJK9xyWkiveu
0+7UHzy7Yx0BOmydzQj1IuCnwbgtKxYxuq+T+uR0VhqTc1IO+s3HyWbhAA==
-----END CERTIFICATE REQUEST-----
$
```

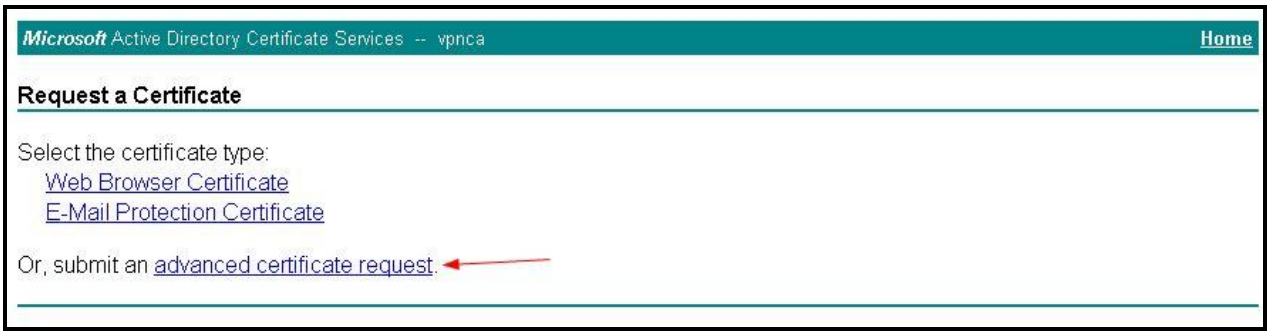
3. Follow the below steps to enroll for a certificate.

3.1 Browse to http://vpnca.datapipe.net/certsrv using your browser from your Macintosh Machine.

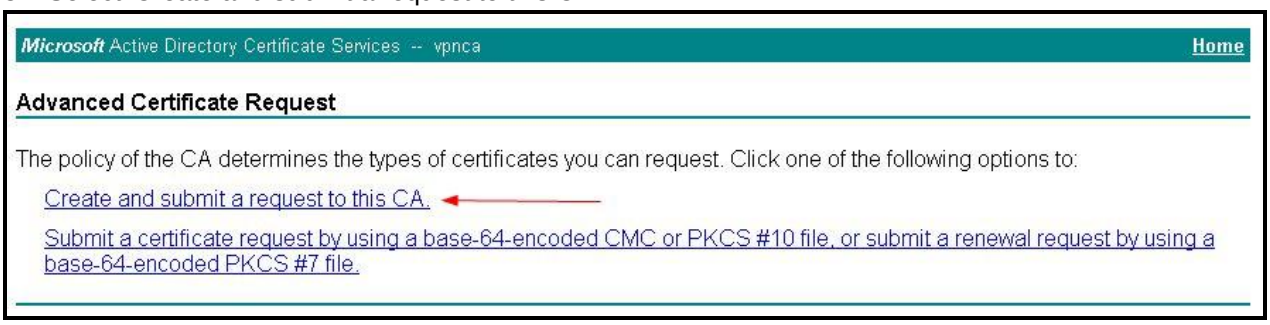
3.2 On the home page under Select a Task, choose 'Request a certificate'.



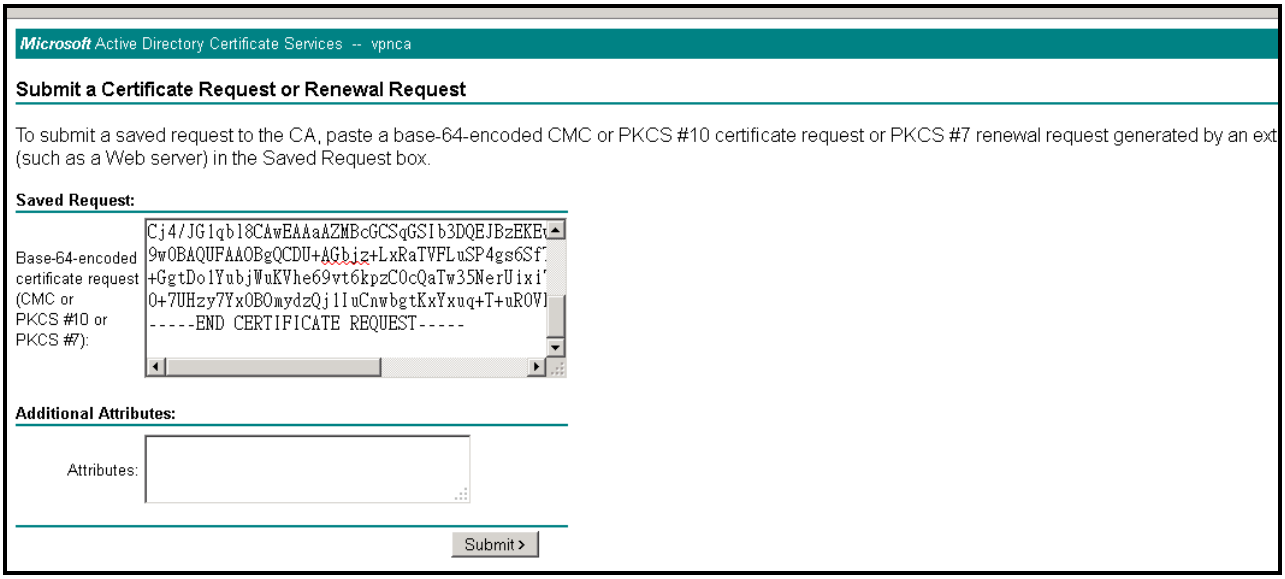
3.3 Select 'advanced certificate request'.



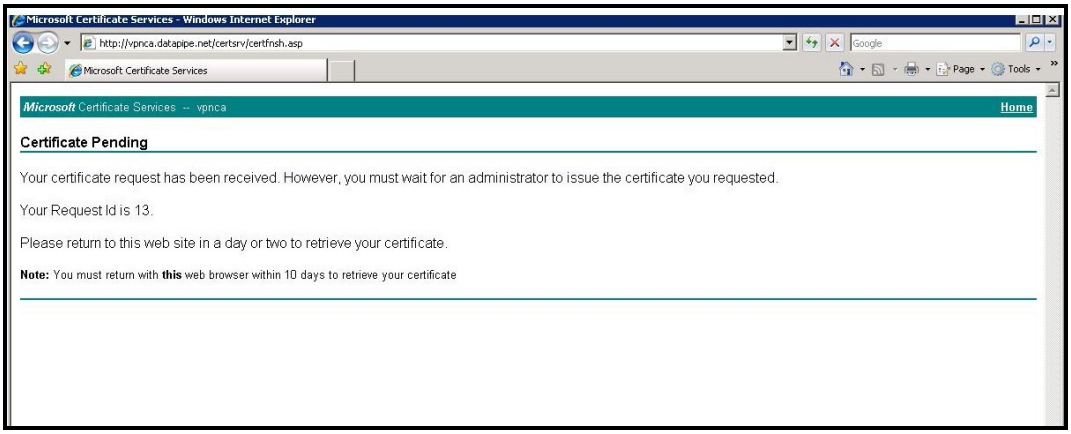
3.4 Select 'Create and submit a request to this CA'.



3.5 Copy and paste the dpvpn-cert.csr content to the “Saved Request box” and click “submit” to request for a certificate.

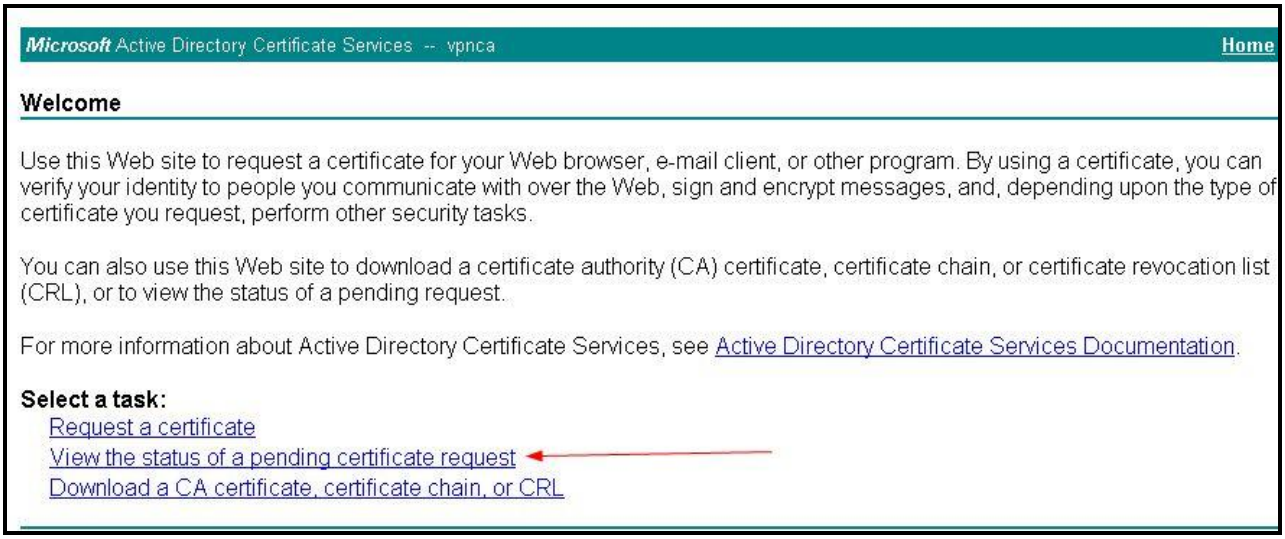


3.6 Your certificate request is now pending. You will get redirected to a confirmation page like the screenshot below. You will also receive an email from a member of the security department once your certificate has been approved. This may take up to one business day.

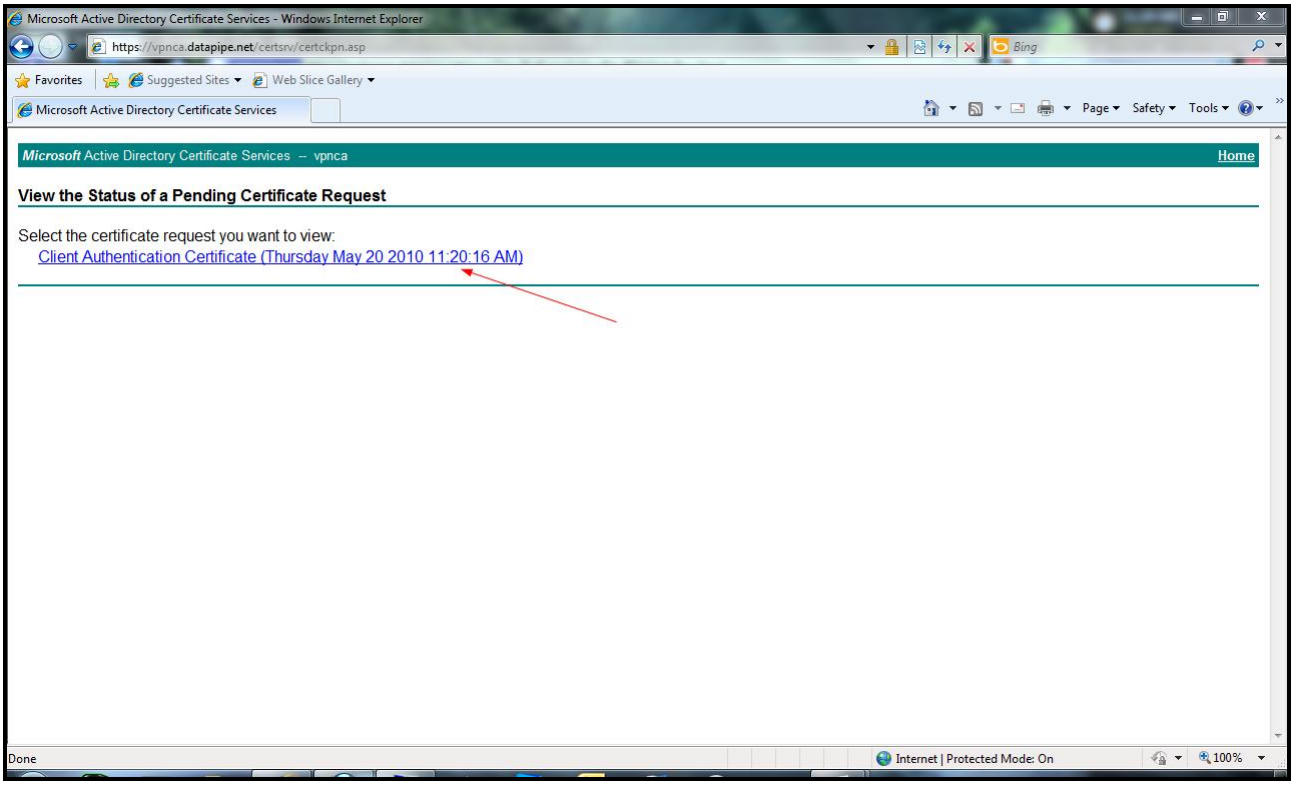


Important: Please be reminded not to clear your browser cache until you have successfully installed your certificate.

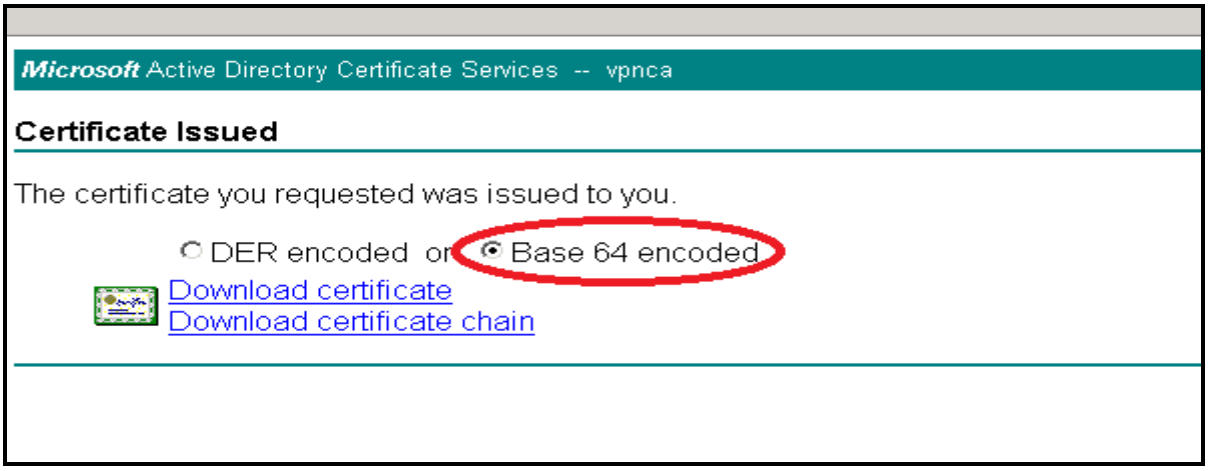
3.7 When you are notified via ticket or email that your certificate has been approved, click the 'Home' link on the top right of the Certificate Pending page or browse to http://vpnca.datapipe.net/certsrv the **same computer** used to enroll for a certificate. On the home page, select the task: '**View the status of a pending certificate request**'.



3.8 You will see something similar to the screenshot below. Click on the certificate request you want to install.



3.9 Check **"Base 64 encoded"** and click "Download certificate" to download and save your certificate.

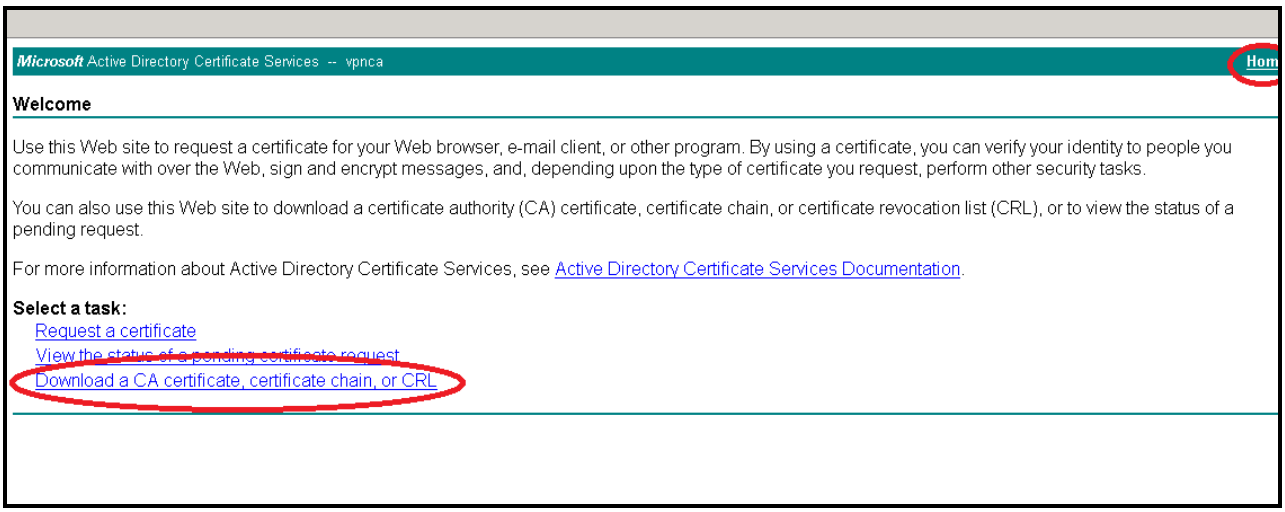


4. Create a p12 file from the key and the certificate:
   openssl pkcs12 -export -inkey dpvpn-cert.key -in certnew.cer -out dpvpn.p12

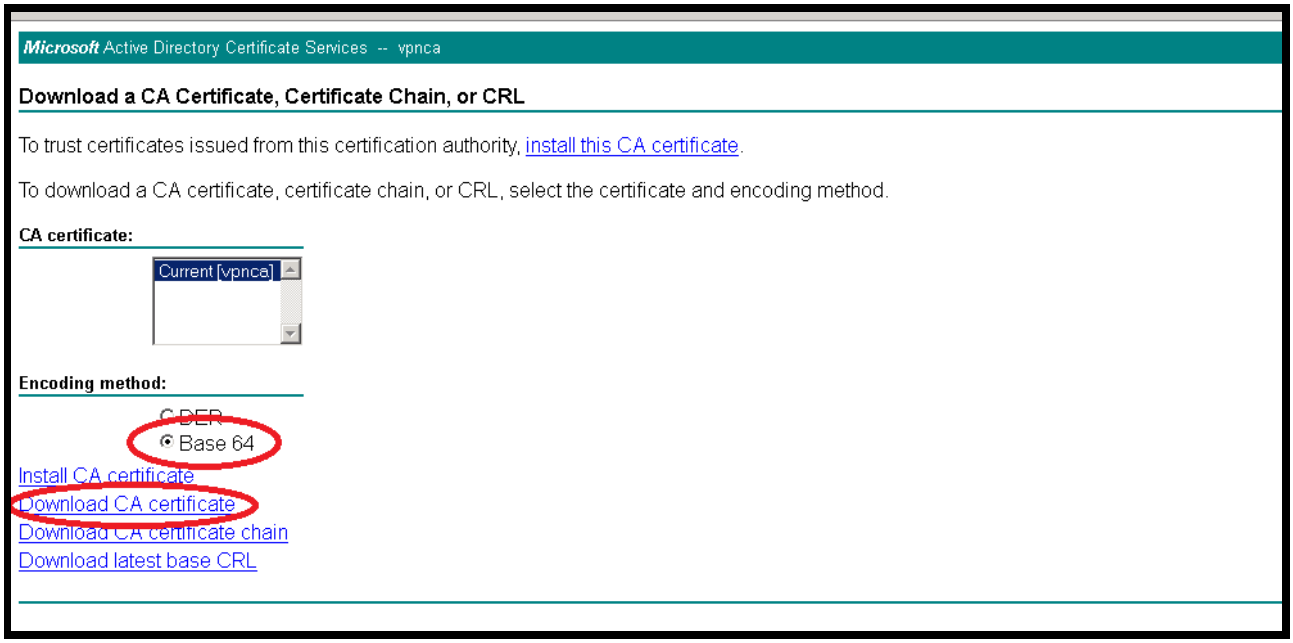
   NOTE: certnew.cer is the certificate you just downloaded from the Datapipe CA, replace it with the correct file name if it is saved with another name.

5. Import the p12 file (containing the key and certificate) in the system keychain (not the login keychain, that doesn't work):
   sudo security import dpvpn.p12 -k /Library/Keychains/System.keychain

6. Download and install Datapipe CA Certificate



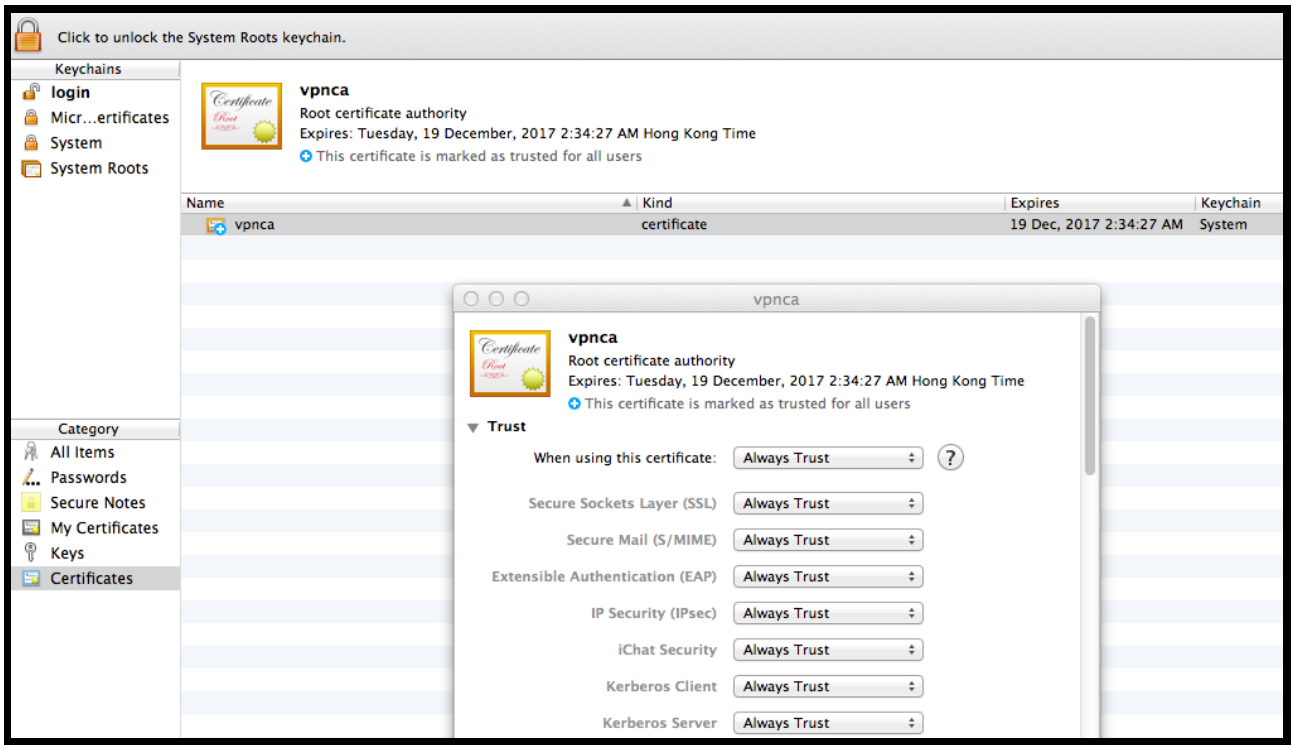
7. Check "**Base 64**" and click "Download CA certificate" to download and save the CA certificate.



8. Import the Datapipe CA certificate and trust it.

8.1 import the Datapipe CA Certificate to your keychain:
sudo security add-trusted-cert -k /Library/Keychains/System.keychain dp-ca.cer
Note: please replace dp-ca.cer with the correct file name. Make sure that you imported CA certificate to your Keychains, otherwise the VPN server certificate will not be verified correctly.

8.2 Go to Finder -> Applications -> Utilities -> KeyChain Access, search the 'vpnca' (it is the Datapipe CA certificate), double click on the vpnca certificate to open it, then expand the “Trust” folder, select "Always Trust" at "When using this certificate"



9. If you are using Mountain Lion (10.8.x), you need follow to the below steps: 9.1-9.8 to grant the VPN certificate (the private key part) to allow for all applications to access.

   9.1 Open Keychain Access (use spotlight), search for the certificate you use in your VPN configuration using the search box which is located in top right of the winddow, you may have to select the appropriate keychain from the list in the left hand navigation column titled 'Keychains'.
   9.2 You should see your certificate listed in the main window, it should have a small arrow to the left of the certificate name.
   9.3 Click on the arrow and this should reveal the private key below, it has a key icon associated with it.
   9.4 Double click on the private key and a window should pop up showing the private key.
   9.5 At the top of this window there are two buttons that can be toggled, 'Attributes' and 'Access Control', by default the Attributes button is selected (greyed out). Click on the 'Acces Control' button.
   9.6 The window changes to display a couple of buttons, the top one 'Allow all applications to access this item' and 'Confirm before allowing access'. Click the top button 'Allow all applications to access this item'.
   9.7 Click on the button 'Save Changes', you may need to enter your admin password.
   9.8 Close all the windows and quit Keychain Access.

10. To use the certificate for your VPN, please do the following:

   10.1 Open System Preferences

   10.2 Go to Network

   10.3 Click “+” to add a new network interface

   10.4 Select Interface: VPN

   10.5 VPN Type: Cisco IPSec

   10.6 Click Create

   10.7 In the “Server Address” field, key in the hostname of the firewall,
   - please check with Datapipe for the firewall hostname
   - it should be in the format of FWhostname.asa.datapipe.net
   - the hostname is **case sensitive**, please make sure your put the exact hostname provided by Datapipe in the “Server Address” field. Otherwise your VPN connection will be failed.

   10.8 add an entry to /etc/hosts as shown below
   IP.IP.IP.IP FWhostname.asa.datapipe.net

   10.9 please check with Datapipe for the firewall hostname and IP address

   10.10 Select Certificate and Click Select

   10.11 Select the correct certificate that you just imported

   10.12 Click OK

10.13 Click Apply

10.14 Click Connect to establish the VPN connection.

Note:
If you have problem connecting the VPN, please do the following:
a. Open a terminal, cd to /var/log
b. Run command “tail -f system.log”
c. Connect the VPN
d. Copy the output message from step# b above and send it to Datapipe for investigation.

:: End ::