



# DEPLOYMENT OF NOKIA E SERIES WITH ISR'S

## Introduction:

This document explains the configuration of Cisco ISR for use with Nokia Mobile VPN Client. It is assumed that the Cisco ISRs basic configuration is in place. These configurations are any network related configurations, such as inside and outside interface assignments, IP address configuration, hostname, domain, default routes and so on. For this document, Cisco 3845 ISR has been used with E71/E66 phones. The configuration is shown using Cisco command line interface (CLIs).

This deployment guide has two main parts:

-Part I: Discusses the configuration required on ISR's.

-Part II: Discusses step by step installation and management of VPN settings on Phone including: .vpn policy creation, VPN Settings, VPN Connectivity etc.

## Part I: ISR Configurations

Following are the steps to configure the Easy VPN to work with Nokia E series phone. This configuration shows deployment with and without x-auth and performs authentication based on PKCS 12 certificates from Microsoft CA. Also this assumes no split-tunnel and assumes that the "OU" or department field in the certificate has the keyword "phonepki", and it is matched in the isakmp profile "phonepki" defined on step 6 with the certificate map "phonepki-map". This is optional, and is needed when you want multiple profiles in the same server and want to match based on "OU"/Department name. Otherwise it is possible to remove it.

**Note: Replace the highlighted parenthesis (shown as <description>) with the values suggested within the parenthesis.**

### Step1) Defining AAA settings:

This step is used to define the Authentication, Authorization and Accounting settings.

```
aaa new-model
```

```
aaa group server radius EzVPN
 server-private <ip address of aaa server> auth-port <port no.> acct-port <port no.> key
 7 <password> ip radius source-interface Loopback1
aaa authentication login easyVPN local group EzVPN
aaa authorization network easyVPN local group EzVPN
```

### **Step2) Define the PKI trustpoint:**

This section defines certificate related configurations including the certificate server to be used.

```
crypto pki trustpoint <any name e.g. ca>
 enrollment mode ra
 enrollment url http://<url for CA server, tested with Microsoft CA server for e.g.
 http://ca.cisco.com:80/certsrv/mscep/mscep.dll>
 serial-number
 ip-address none
 revocation-check none
```

### **Step 3) To get a root certificate and device certificate from the CA**

Since this makes sure router uses SCEP enrollment process, we need Microsoft Ca with SCEP Client.

```
crypto pki authenticate <CA server name>
crypto pki enroll <CA server name>
```

### **Step 4) Defining a map (Optional)**

This steps defines pki maps which is required only if multiple profiles are being used. This is optional, and is needed when you want multiple profiles in the same server and want to match based on “OU”/Department name. Otherwise it is possible to remove it. However for scalability it is recommended to use the below cli’s.

```
crypto pki certificate map phonepki-map 10
 subject-name co phonepki
```

### **Step 5) ISAKMP policy:**

These steps define the ISAKMP policy and settings.

```
crypto isakmp policy 2
 encr 3des
 group 2
 crypto isakmp keepalive 50
 crypto isakmp nat keepalive 50
 crypto isakmp xauth timeout 90
```

### **Step 6) Pool from which ipaddress to client is assigned.**

```
ip local pool easyvpn-pool <10.xx.xxx.3 10.xx.xxx.xxx>
```

### **Step 7) Defining the mode-config parameters:**

These steps define the parameters that an easy vpn client receives from the server.

```
crypto isakmp client configuration group phonepki
dns <dns server name>
domain <domain name>
pool easyvpn-pool
```

### **Step 8) Defining isakmp profile:**

This steps defines an isakmp profile which links the CA server, Maps, AAA settings, mode config parameters defined above together in a single profile.

```
crypto isakmp profile phonepki
ca trust-point <any name defined in step 2 above e.g. ca>
match identity group phonepki
match certificate phonepki-map (if defined on step 3)
client authentication list easyVPN (optional required only for xauth)
isakmp authorization list easyVPN
client configuration address respond
virtual-template 6
```

### **Step 9) Defining Transform set.**

This defines the ipsec settings.

```
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
```

### **Step 10) Defining ipsec profile**

This profiled links all possible transform sets under a single profile.

```
crypto ipsec profile stealth
set transform-set t1
```

### **Step 11) Defining virtual template**

This associates the physical interface with the virtual interface and also applies ipsec profile to this virtual interface.

```
Interface Virtual-Template6 type tunnel
```

```
ip unnumbered <WAN interface e.g. Loopback1 or Fa4 etc>
ip mtu 1400
ip tcp adjust-mss 1200
tunnel mode ipsec ipv4
tunnel path-mtu-discovery
tunnel protection ipsec profile stealth
```

Note if we use loopback 1 as our WAN interface above  
interface Loopback1  
ip address <Routable wan IP> <Mask>  
end

## Part II: Nokia E71 manual step by step process of VPN Certificate setup

The E71 phone has to be activated and associated with a phone number. The Internet access is operational.

1. Install “Nokia PC Suite on your PC” – from CD.
2. Upgrade your Nokia E71 software if needed. Use “Nokia PC suite” to upgrade the SW, connecting USB or Bluetooth or Infrared.



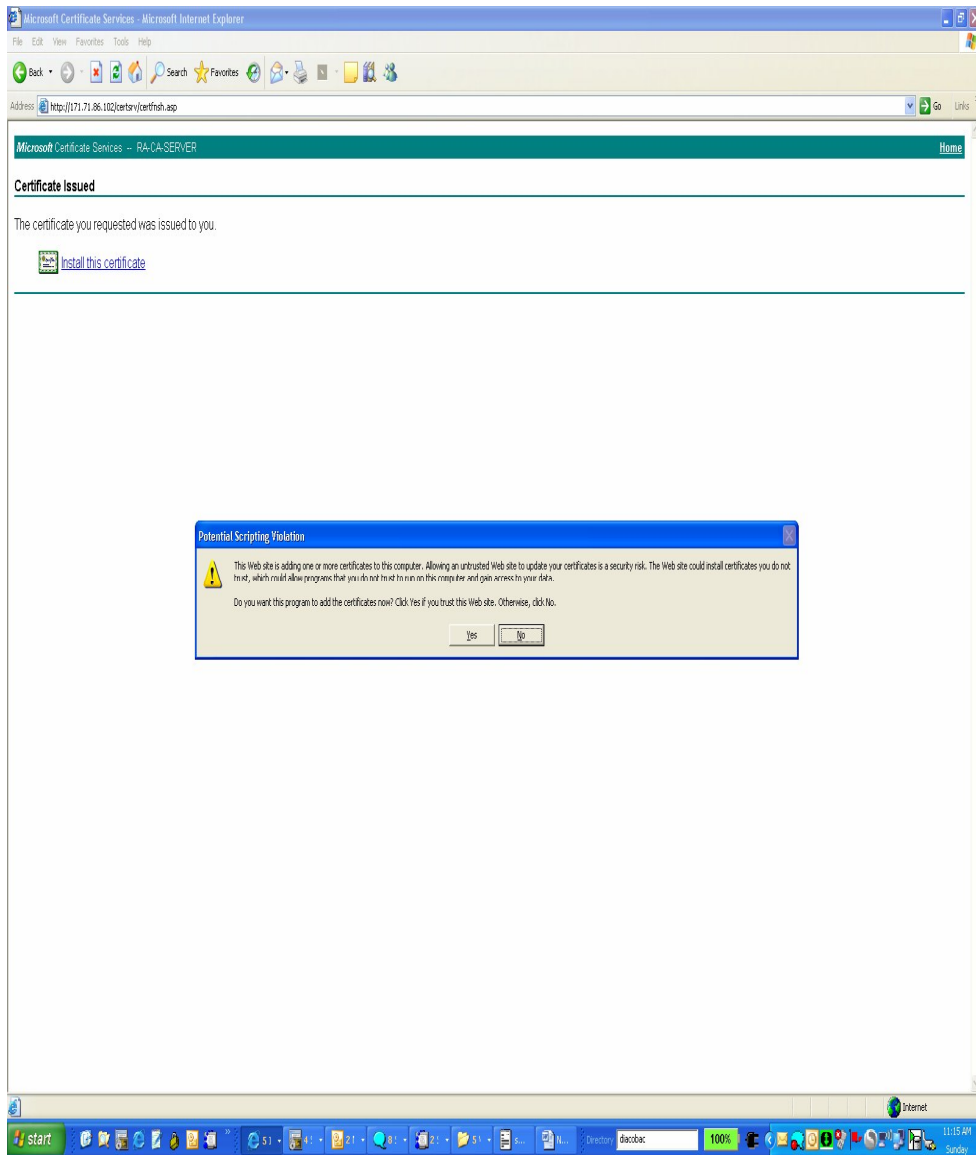
3. Request a certificate for the phone from RA-CA-SERVER - http://<ip of CA server>/certsrv

The screenshot shows a Microsoft Internet Explorer browser window displaying the 'Advanced Certificate Request' page. The address bar shows 'http://beta-ca/certsrv/certqma.asp'. The form is divided into several sections:

- Identifying Information:** Fields for Name (Mobile E71 Certificate), E-Mail (pthakore@cisco.com), Company (Cisco Systems Inc.), Department (phonepki), City (San Jose), State (Ca), and Country/Region (US).
- Type of Certificate Needed:** A dropdown menu set to 'Client Authentication Certificate'.
- Key Options:** Radio buttons for 'Create new key set' (selected) and 'Use existing key set'. A CSP dropdown is set to 'Microsoft Enhanced Cryptographic Provider v1.0'. Key Usage has radio buttons for 'Exchange', 'Signature', and 'Both' (selected). Key Size is set to 1024. Other options include 'Automatic key container name' (selected), 'Mark keys as exportable' (checked), 'Export keys to file', 'Enable strong private key protection', and 'Store certificate in the local computer certificate store' (unchecked).
- Additional Options:** Radio buttons for 'CMC' (selected) and 'PKCS10'. Hash Algorithm is set to 'SHA-1'. There is a checkbox for 'Save request to a file' and an 'Attributes' field.

Note the department field above is the same as defined in the configuration of the ISR i.e. phonepki.

## 4. Install the Certificate



## 5. Export the certificate:

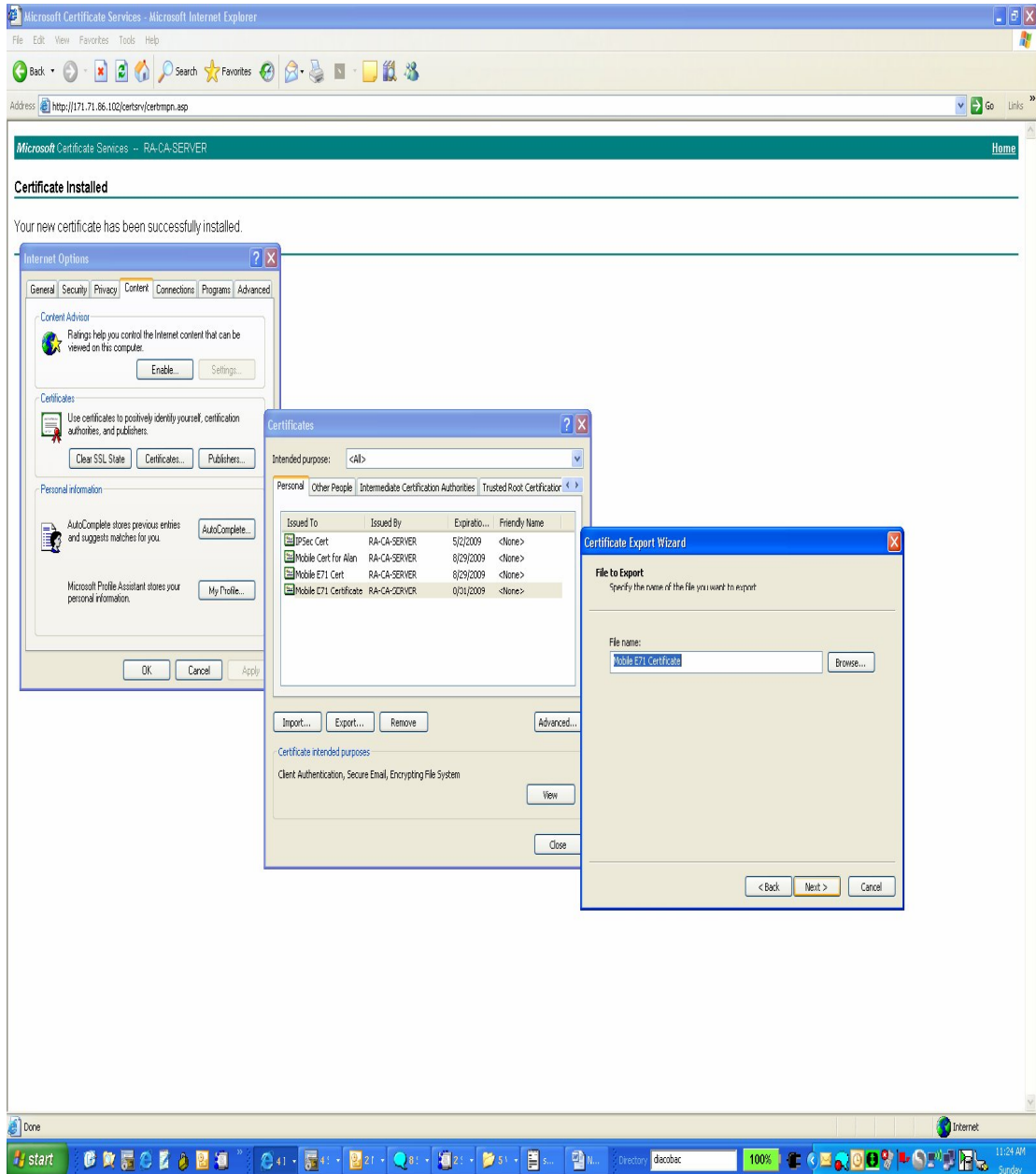
Click Yes on “Export the private keys”

Check the box “Include all the certificates in the certification path if possible”

Type a password - “password”

Provide a name for the certificate – “Mobile E71 Certificate.p12”

Complete the export. The certificate is being exported to the desktop.



6. Create a VPN policy using “Nokia Mobile VPN Client Policy Tool”

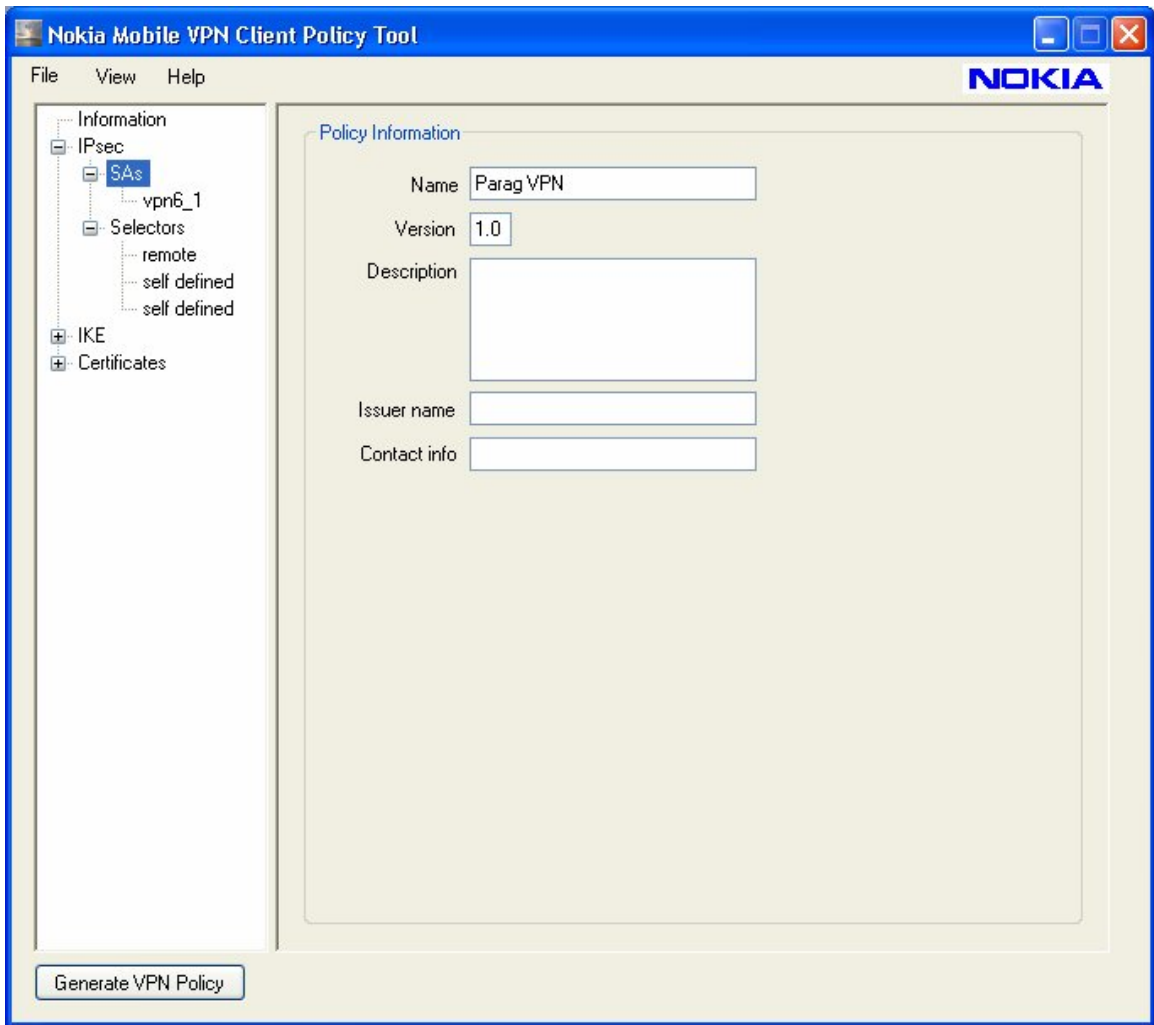
The screenshot shows the Nokia Mobile VPN Client Policy Tool interface. The window title is "Nokia Mobile VPN Client Policy Tool". The menu bar includes "File", "View", and "Help". The interface is divided into several sections:

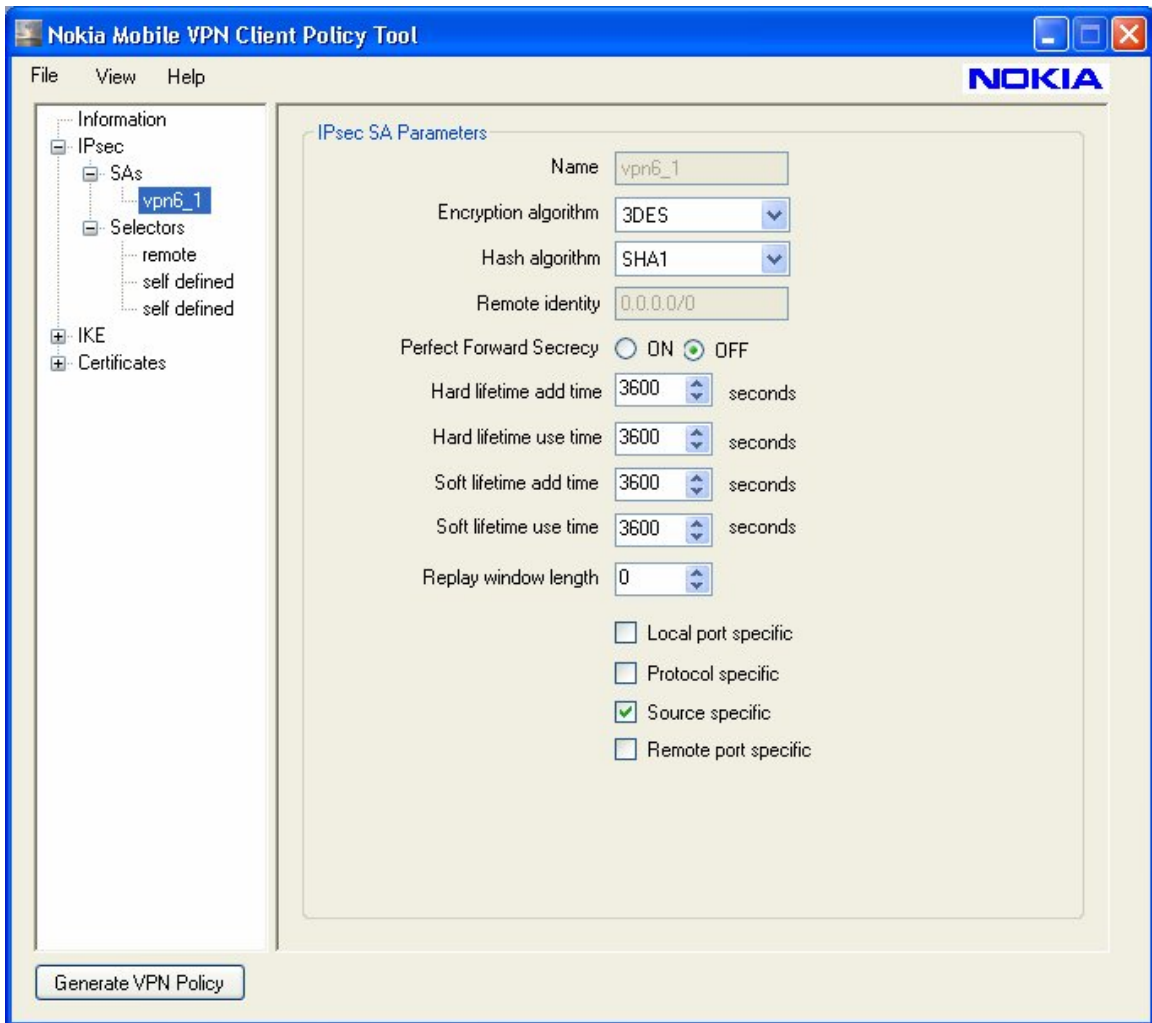
- General Information:** Policy name: Parag\VPN; VPN gateway address: <vpn-gatewayipaddress>
- Certificate Authority:** Format: BIN; Data: C:\Program Files\Nokia\Nokia Mobile V
- IKE:** IKE mode: IKEv1 main; Authentication method: RSA\_SIGNATURES; Identity type: RFC822\_NAME; Identity value: pthakore@cisco.com; Remote ID type: ; Remote ID: ; EAP realm prefix:
- User Certificate:** Certificate: user-1.cer; Private key: user-1.key; Subject DN suffix: ; RFC822NAME (FQDN): ; Key length: 1024
- PKCS#12:** PKCS file: C:\Program Files\Nokia\Nokia Mobile V; VPC file:
- Silent CRACK:** Username: ; Password:
- Preshared Key:** Format: STRING\_FORMAT; Key:

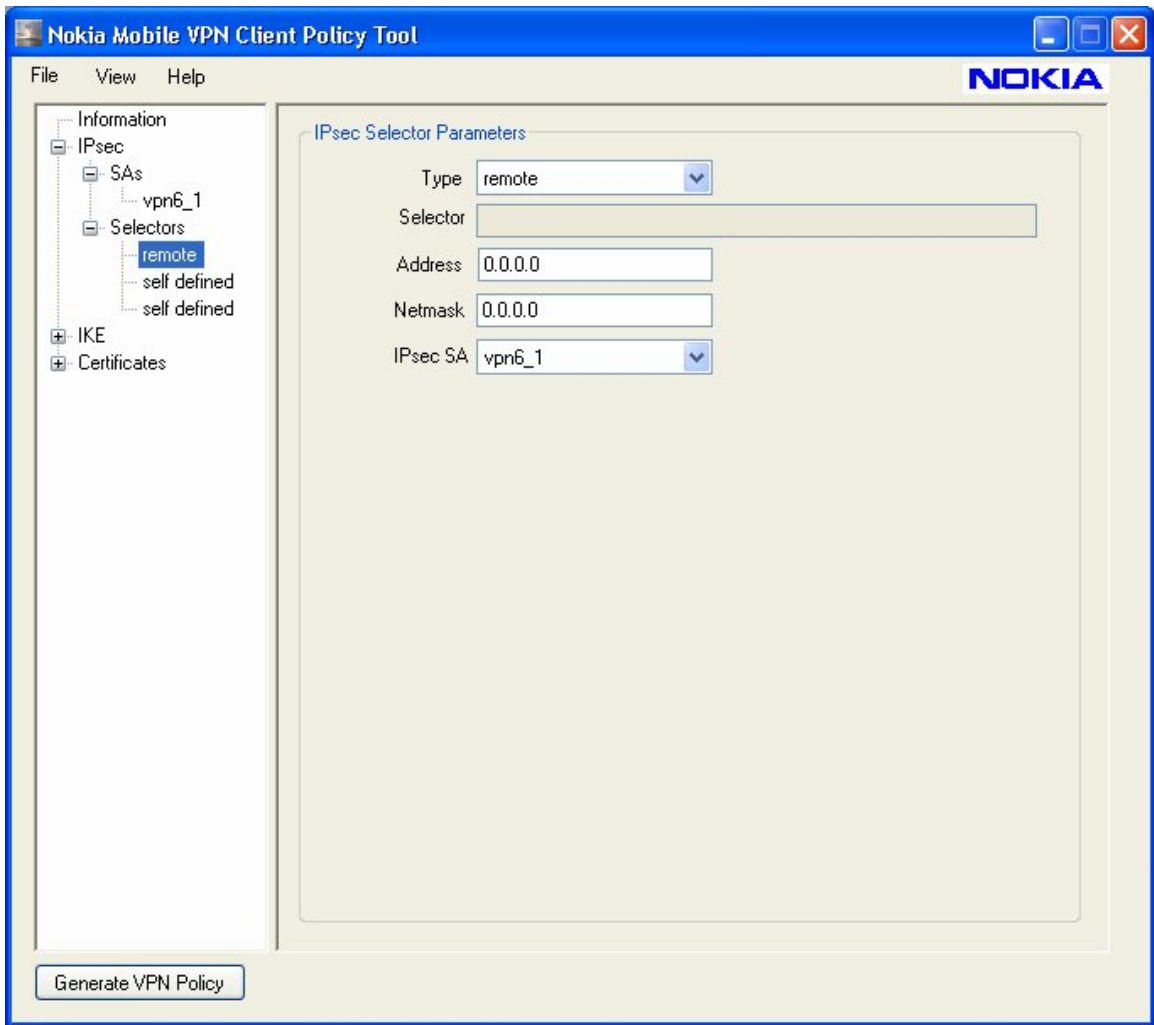
A "Generate VPN Policy" button is located at the bottom left of the window.

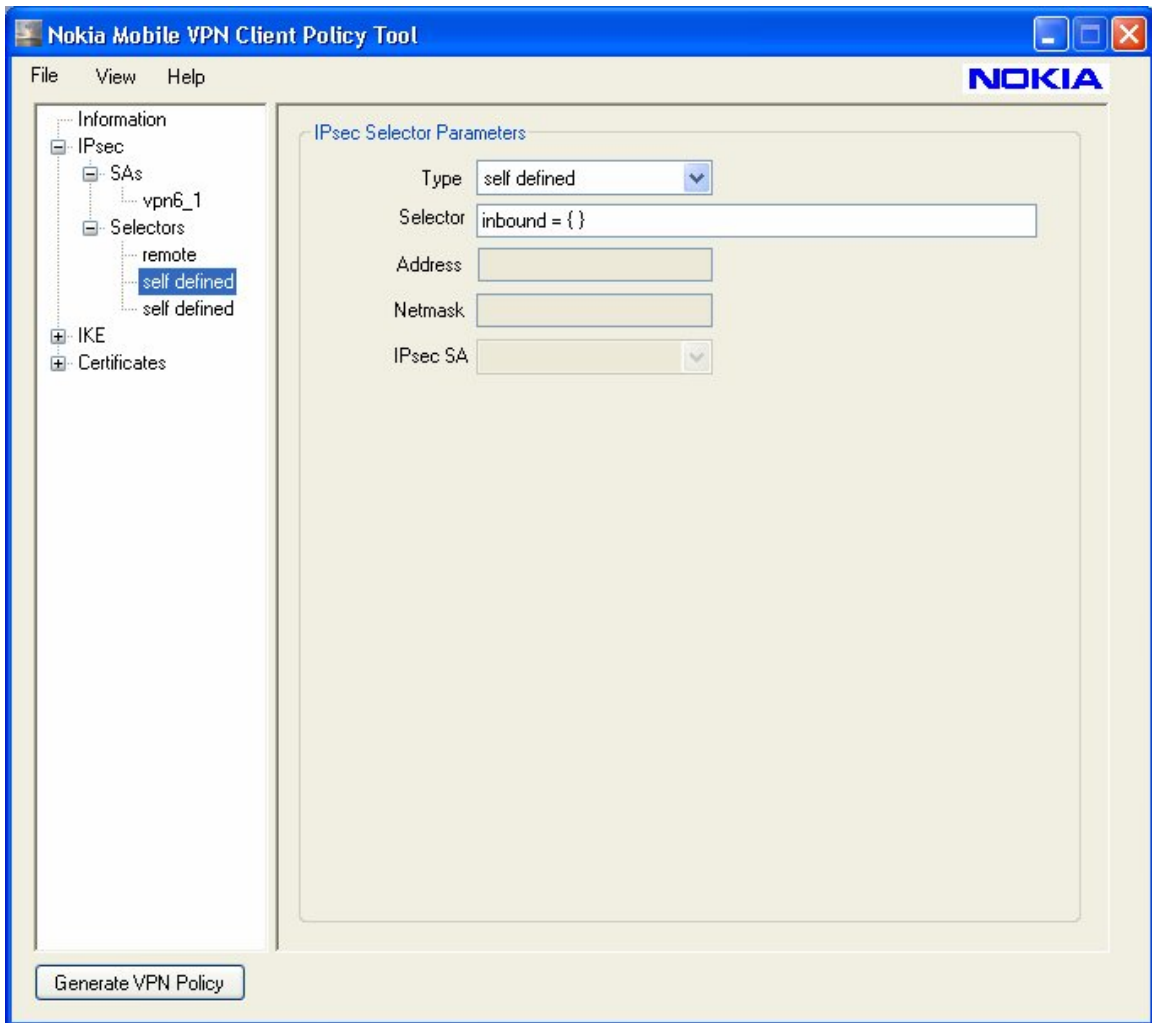
Step 7) Configuring advanced wizard.

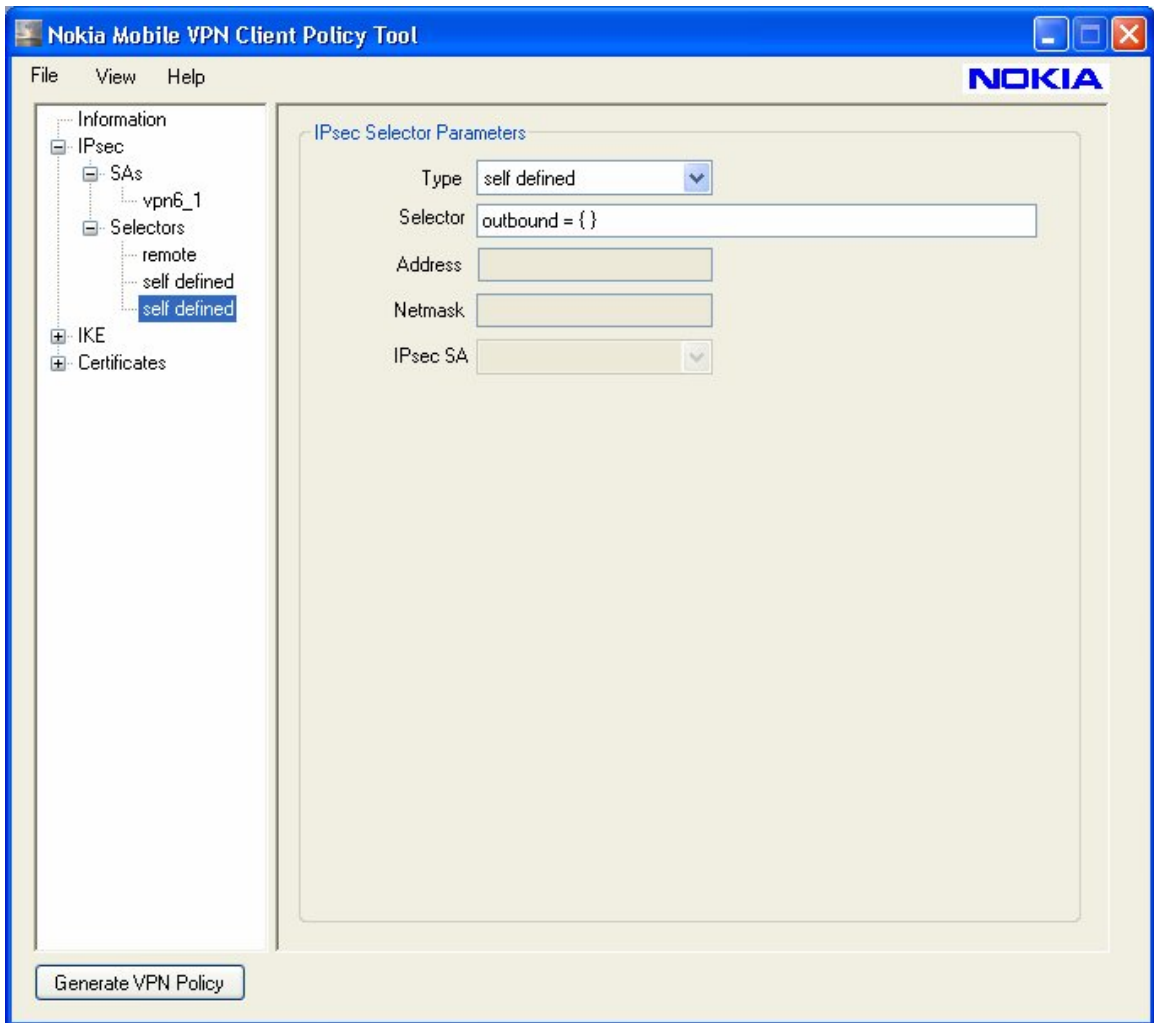
Note you may also go to view->advanced wizard and generate an isakmp and ipsec policies as configured on the ISR's. Below are the settings made in advanced wizard view for both ISAKMP and IPSEC.

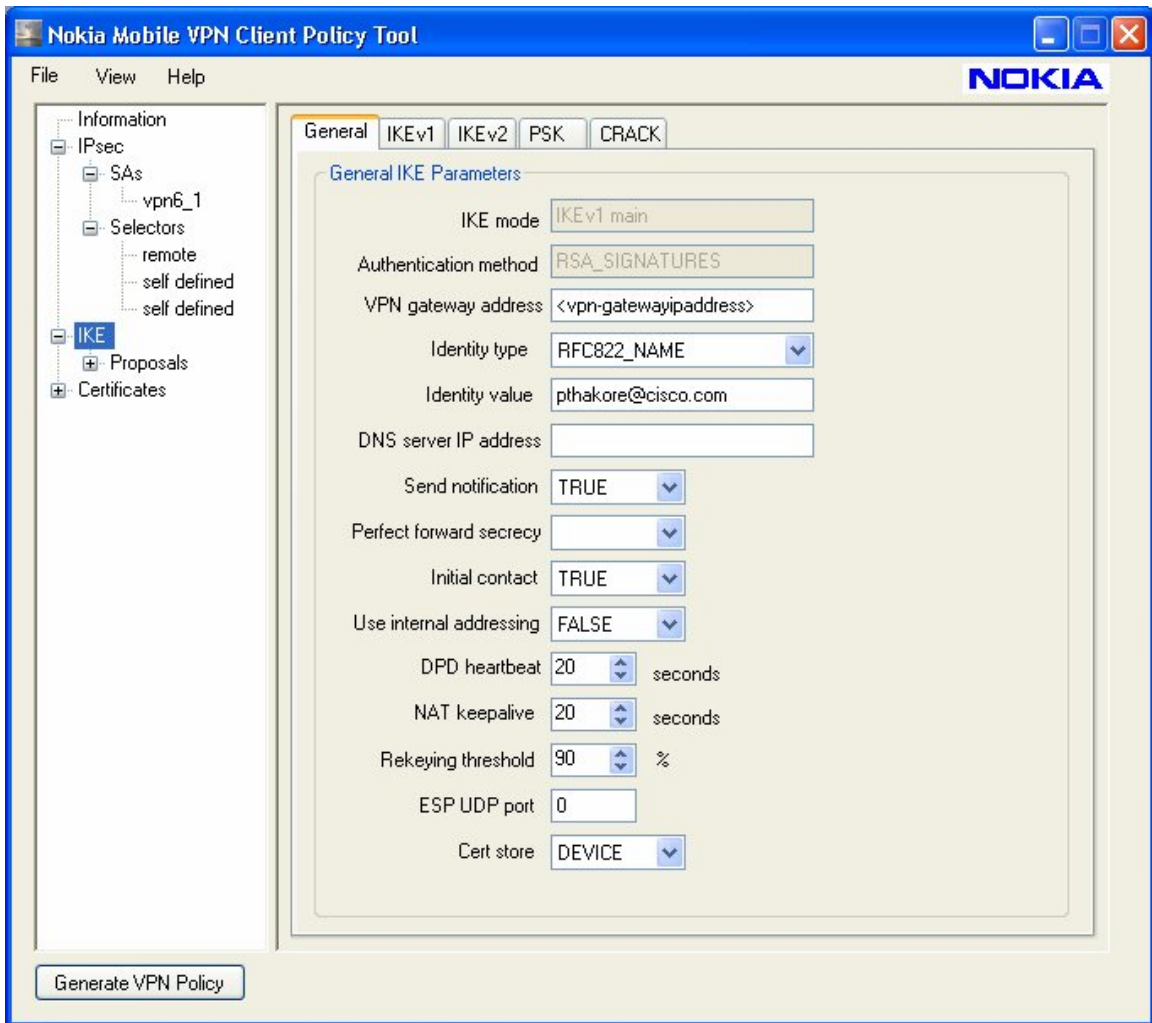


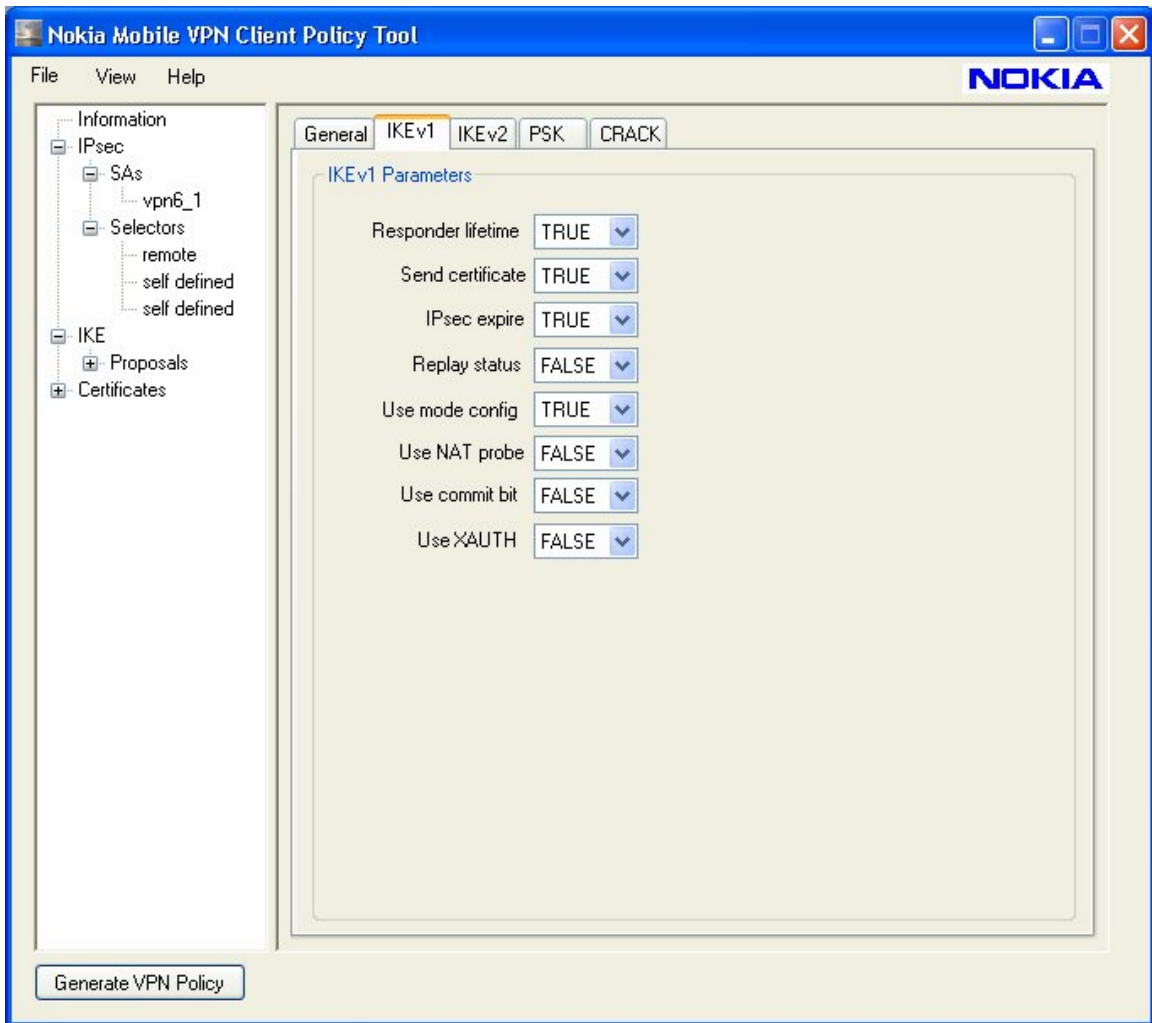


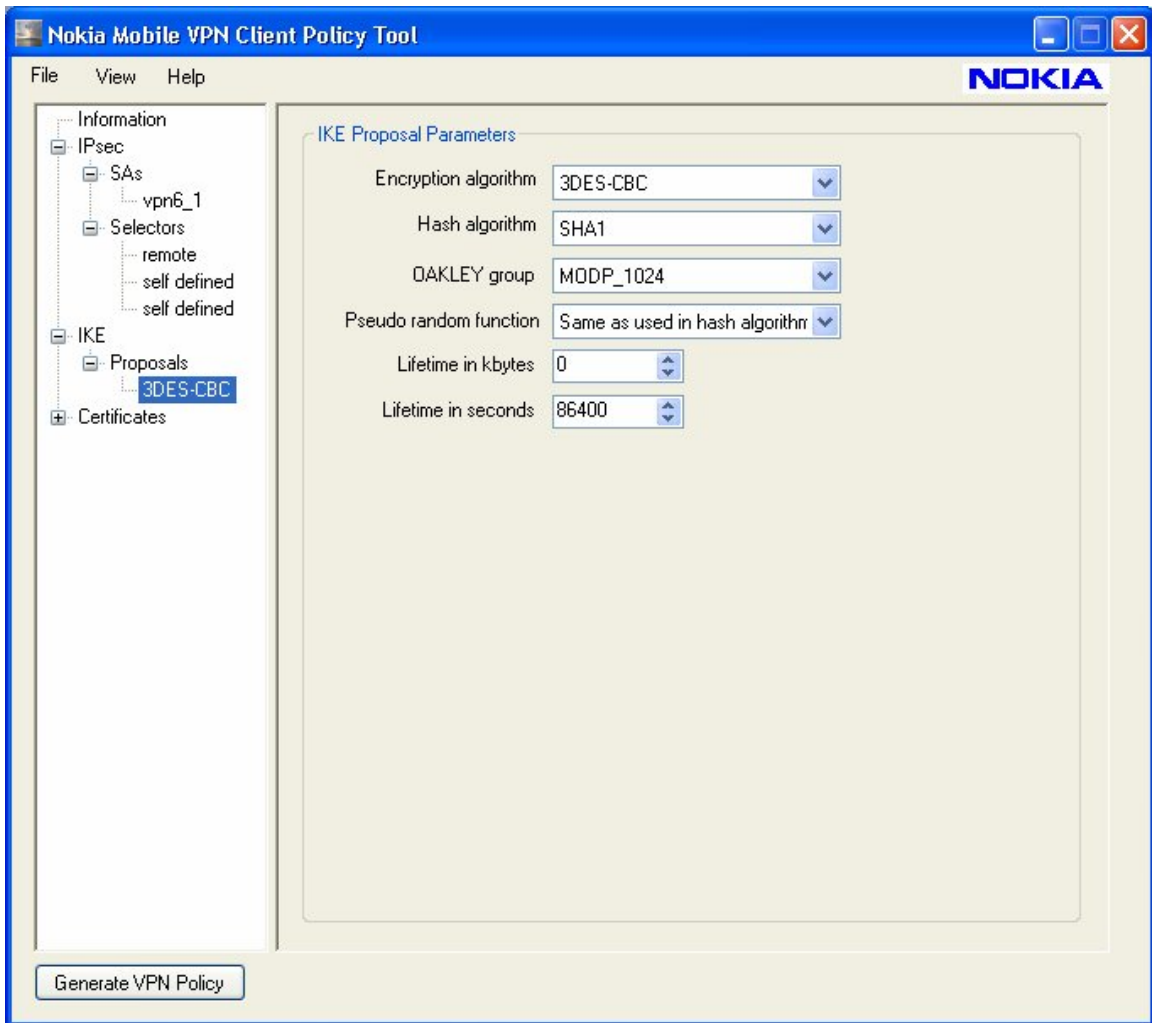




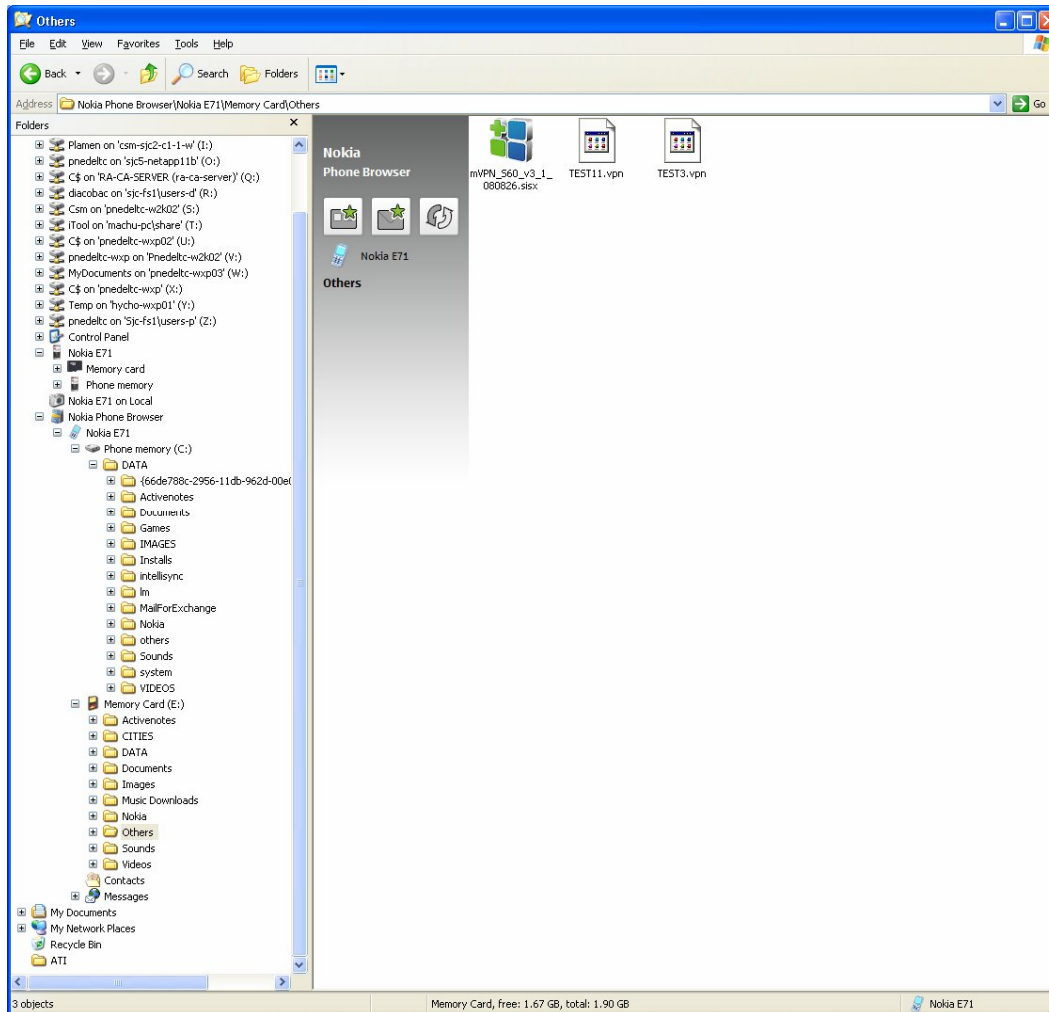








8. Use “Nokia PC suite” to connect the phone to PC with USB or Bluetooth.
  - Copy the “TEST11.vpn” policy to any of the folders of the E71.
  - Copy the new VPN client mVPN\_S60\_v3\_1\_080826.sisx to the same directory.



9. Disconnect the phone from USB.

10. Go to E71 - Menu->Office->File Manager and find the new VPN client. Click & Install it.

11. Go to Menu->Office->File Manager and find the new VPN policy. Click & Install it. Provide the P12 password (step 5) and then a phone store password (new password - no less than 6 chars).

12. Go to Menu->Settings->General->Security->Certificate Management->Authority Certificates and make sure RA-CA-SERVER certificate is installed.

13. Go to Menu->Settings->General->Security->Certificate Management->Phone Certificate and make sure Mobile E71 Certificate.p12 is installed.

14. If the idea is to use Access point for data instead of the Service provider network go to Menu-Tools-Settings-Conncection-AP-> Add a new AP and its corresponding security settings.

15. Go to Menu->Settings->Connection->VPN->VPN Management->VPN Policies-TEST11-Make sure "Certificate Status" is OK.

16. Go to Menu->Settings->Connection->VPN->VPN Access Points->Define a policy "Cisco VPN"->VPN Policy (associate with TEST11).  
The new (VPN) access point policy should look like:

Connection name – "Cisco VPN"

VPN Policy – "TEST11"

Internet Access point – (Service Provider Data Network/ (Access point defined in Step 14)

Proxy Server address – no

Proxy port number – 80

17. Launch a browser and use the the vpn access point configured above and make sure you can access corporate resources.