



# Application Note 22

---

## **IPSEC VPN tunnel between two Digi Transport Routers using Certificates and SCEP**

UK Support

November 2015

## Contents

|     |                                                                       |    |
|-----|-----------------------------------------------------------------------|----|
| 1   | Introduction.....                                                     | 4  |
| 1.1 | Outline.....                                                          | 4  |
| 1.2 | Corrections.....                                                      | 5  |
| 1.3 | Version.....                                                          | 5  |
| 2   | The Certificate Infrastructure.....                                   | 6  |
| 2.2 | IKE – Authentication .....                                            | 6  |
| 2.3 | IPSEC – Secure Data Transfer.....                                     | 7  |
| 3   | Microsoft® 2003 Server Configuration.....                             | 7  |
| 3.1 | Requirements.....                                                     | 7  |
| 3.2 | Configure the Microsoft® 2003 Server as a Certificate Authority ..... | 7  |
| 3.3 | Automatic Enrolment .....                                             | 14 |
| 4   | VPN Responder Certificates .....                                      | 17 |
| 4.1 | Ethernet 0 LAN Configuration .....                                    | 17 |
| 4.2 | Time and Date.....                                                    | 17 |
| 4.3 | ADSL Interface Configuration.....                                     | 18 |
| 4.4 | Creating the Private Key and Certificate Request .....                | 19 |
| 5   | VPN client Certificates .....                                         | 34 |
| 5.1 | Ethernet 0 LAN Configuration .....                                    | 34 |
| 5.2 | Time and Date.....                                                    | 34 |
| 5.3 | Wireless WAN Interface Configuration.....                             | 35 |
| 5.4 | Creating the Private Key and Certificate Request .....                | 38 |
| 5.5 | Using SCEP to retrieve the CA certificates .....                      | 41 |
| 5.6 | Using SCEP to Enroll the Certificate Request .....                    | 44 |
| 6   | Configure IKE and IPSEC – VPN Responder .....                         | 47 |
| 6.1 | Configure IKE (Internet Key Exchange).....                            | 47 |
| 6.2 | Configure IPSEC .....                                                 | 48 |
| 7   | Configure IKE and IPSEC – VPN client.....                             | 51 |
| 7.1 | Configure IKE (Internet Key Exchange).....                            | 51 |
| 7.2 | Configure IPSEC .....                                                 | 54 |

|     |                                                                                                            |           |
|-----|------------------------------------------------------------------------------------------------------------|-----------|
| 8   | Testing.....                                                                                               | 56        |
| 8.1 | Check the WAN Link is Active.....                                                                          | 56        |
|     | <i>NB: The default PPP instance for the WAN interface may differ depending on the type of router. ....</i> | <i>56</i> |
| 8.2 | Check the IPSEC Tunnel is Active .....                                                                     | 56        |
| 8.3 | Test the IPSEC Routing.....                                                                                | 58        |
| 9   | Configuration Files.....                                                                                   | 65        |
| 9.1 | Digi Transport Configuration Files .....                                                                   | 65        |

# 1 INTRODUCTION

## 1.1 Outline

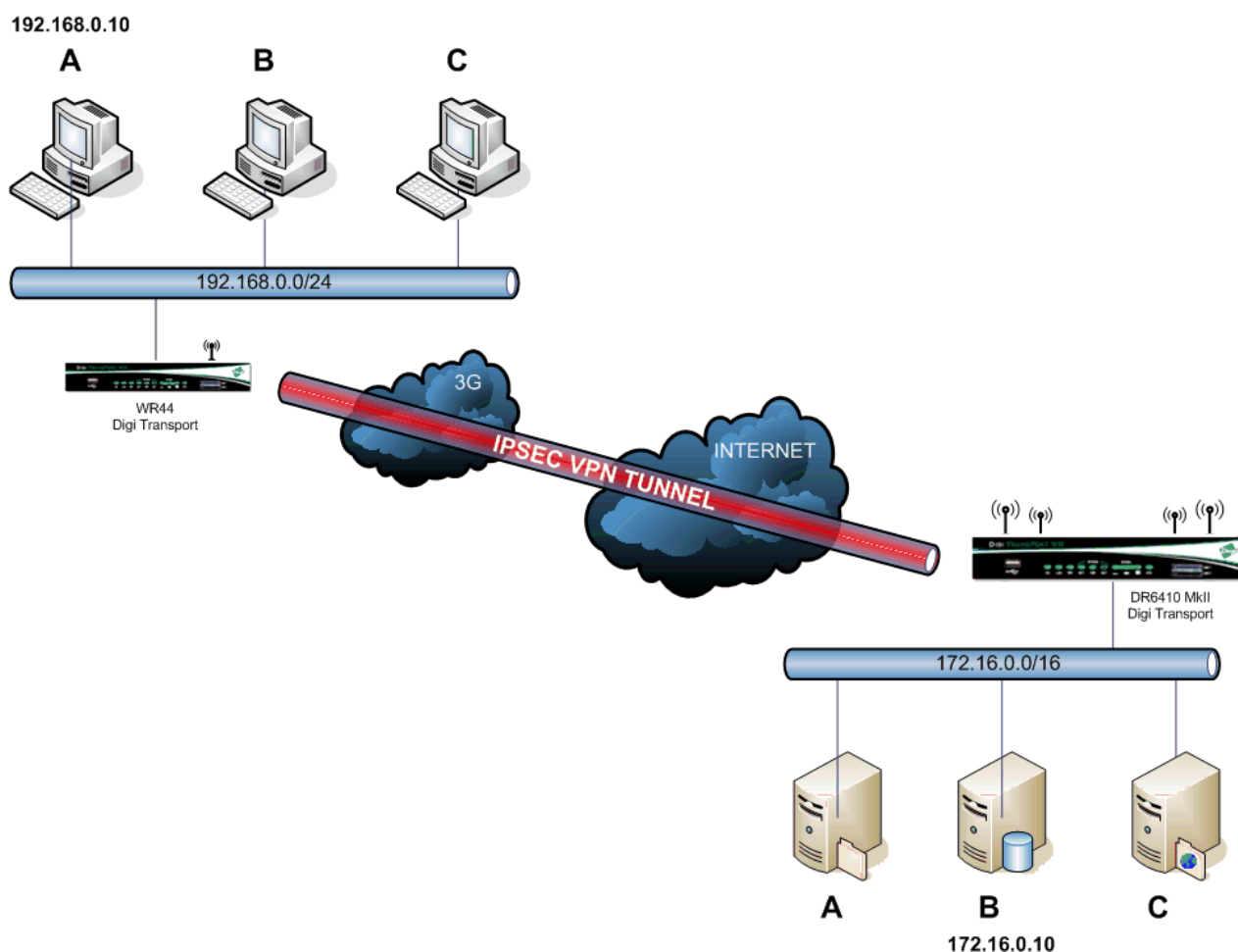
This application note is intended to explain how to create RSA key files, certificate requests, and how to use SCEP to retrieve a signed certificate from a Microsoft® 2003 server for use with IPSEC.

This document is a worked example of how to configure two TransPort routers to establish an IPSEC tunnel between each other using signed certificates, RSA key files and CA (Certificate Authority) certificates. This will allow full secure connectivity between two private networks connected together via the Internet.

The advantages of using RSA certificates over pre-shared keys are;

Scalable - pre-shared keys become unmanageable on large schemes

Provides increased security over pre-shared keys



## Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

This application note applies only to;

**TransPort Model:** Any 2000 series TransPort router or later

Firmware versions: 4.804 or later.

**Configuration:** This Application Note assumes that the TransPort product is set to its factory default. Most configuration commands are only shown if they differ from the factory default.

**Microsoft® Operating System:** Microsoft® 2003 Server with IIS (Internet Information Services) and Certificate Services installed

## 1.2 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: [applicationnotes@digicom.com](mailto:applicationnotes@digicom.com)

Requests for new application notes can be sent to the same address.

## 1.3 Version

| Version Number | Status                |
|----------------|-----------------------|
| 1.0            | Published             |
| 1.1            | Minor classification  |
| 1.2            | Change to section 3.2 |
| 1.3            | Update & rebranding   |
| 2.0            | Firmware Change       |

## 2 THE CERTIFICATE INFRASTRUCTURE

### 2.1.1 Private Key

Each device creates its own private key. The private key is the basis for all the security for this method of IKE authentication and as such it is important that it is kept safe. If it becomes available to anyone other than the owner of the certificate, the certificate can no longer be used to confirm the owner's identity.

Private Key files installed on a TransPort router should be in the format of "priv\*.pem" (e.g. **privxxxx.pem**). Private Key files of this format cannot be copied, renamed or have their contents read.

### 2.1.2 Certificate Request

In order to receive a signed public key certificate from a CA (Certificate Authority), a certificate request is generated from the private key and sent to the CA for signing.

### 2.1.3 Public Key Certificate

The Certificate request is sent to a trusted CA (Certificate Authority). The CA digitally signs the certificate request thus creating a public key certificate.

The public key certificate is used to identify Router 'A' with the opposite router 'B' and vice versa.

Public key certificate files installed on a TransPort router should be in the format of "cert\*.pem" (e.g. **certxxxx.pem**).

### 2.1.4 CA (Certificate Authority) Certificate

The CA Certificate contains the public portion of the CA's public/private key pair which signed the certificate request.

## 2.2 IKE – Authentication

Before you begin to send and receive confidential data you need to be sure that you are connecting to your trusted host and not some impostor.

When making the trusted connection between two routers, each router will send its signed **Public Key Certificate** to the other if it is available on the FLASH filing system. If it is not available, the remote unit must be able to access the file by some other means. These Certificates will then have their digital signatures compared with the signature of the trusted **CA Certificate**. If the signatures match, this proves that the Certificate Authority did sign the certificates.

**Router 'A'** then uses its **Private Key** to sign (encrypt) a HASH which is created from other data unique to the negotiation. The signature is sent to **Router 'B'** which uses **Router 'A's** public key to verify the signature.

The certificates are used for authentication purposes only. A unique set of keys, applicable only to that IKE session are created for the secure transfer of data.

## 2.3 IPSEC – Secure Data Transfer

Once the Identities of each router have been proved the transfer of secure data can begin. Dynamically generated Public and Private Keys are used to secure data, only this time the Private Key is used to de-encrypt data and the Public Key is used to encrypt data.

Example (see diagram on page 3)

**Router ‘A’** receives a confidential text document from **computer ‘A’**. The text document should be sent in a secure manner over the Internet to **Router ‘B’** then forwarded to **Server ‘B’**.

Using the **Public Key** received from **Router ‘B’**, **Router ‘A’** encrypts the IP packets containing the text file and sends them to **Router ‘B’** over the Internet connection via the VPN tunnel. **Router ‘B’** uses its secure **Private Key** to decrypt the IP packets containing the text document and forwards them to **Server ‘B’**.

This is highly secure because only the owner of the **Private Key** can de-encrypt the data. So if the data is intercepted by a third party it is rendered useless without possession of the correct Private Key.

## 3 MICROSOFT® 2003 SERVER CONFIGURATION

**If you have already have access to a working Certificate Authority server then you can skip to section 5**

### 3.1 Requirements

For a Microsoft® 2003 server to act as a Certificate Authority the following services must be installed;

**IIS** (Internet Information Services)

Certificate Services, including Certificate Services CA and Certificate Services Web Enrolment Support.

The Simple Certificate Enrolment Protocol (SCEP) Add-on for Certificate Services will also require downloading to the server for installation.

At the time of publication the SCEP add-on could be obtained from the following link.

<http://www.microsoft.com/downloads/details.aspx?FamilyID=9f306763-d036-41d8-8860-1636411b2d01&DisplayLang=en>

### 3.2 Configure the Microsoft® 2003 Server as a Certificate Authority

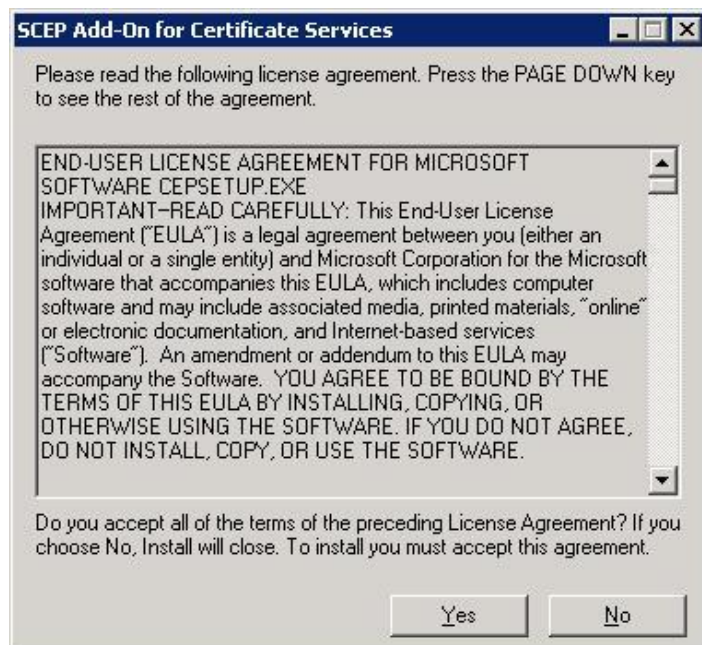
#### 3.2.1 Install SCEP Add-on for certificates

Login to the Microsoft® 2003 Server with an appropriate System Administrator account. With your mouse double-click the **cepsetup.exe** icon to begin installation.

The following dialogue box will appear. Click **Yes** to proceed.



Next the end user licence agreement will appear. If you agree, click **YES**.



The SCEP Add-on for Certificate Services Setup Wizard will start. To proceed click **Next**.





A dialogue box will appear asking for the identity that IIS (Internet Information Services) should use for running the SCEP Add-on for Certificate Services.

Choose Use the local system account and click Next.



A dialogue box will appear asking if you wish to select the challenge phrase if you wish the CA to automatically issue certificates to SCEP requests.

Select the Require SCEP Challenge Phrase to Enroll tick box. Click Next.



A form will appear in which you are asked for information to enrol for the RA\* (Registration Authority) certificates. Enter appropriate details and click **Next**.

\*RA. A computer that is configured for an administrator to request and retrieve issued certificates on behalf of other users

**SCEP Add-On for Certificate Services Setup Wizard**

**SCEP RA Certificate Enrollment**  
Enter the below information to enroll for the RA certificates

Name:

Email:

Company:

Department:

City:

State:  Country/Region:

☐ Advanced Enrollment Options

The SCEP Add-On needs a special certificate (RA Certificate) that allows it to make request to the CA on behalf of the router.

< Back   Next >   Cancel

A dialogue box will appear completing the SCEP Add-on for Certificate Services Setup Wizard. Confirm the details shown are correct. If so click **Finish**.

**SCEP Add-On for Certificate Services Setup Wizard**

**Completing the SCEP Add-On for Certificate Services Setup Wizard**

You have successfully completed the SCEP Add-On for Certificate Services Setup Wizard.

You have specified the following settings:

|                          |                      |
|--------------------------|----------------------|
| Application Identity     | Local System         |
| Require Challenge Phrase | Yes                  |
| RA Credentials           | sarianca_demo        |
|                          | support@sarian.co.uk |
|                          | Sarian Systems Ltd   |
|                          | Demo                 |
|                          | Ilkley               |
|                          | Yorkshire            |
|                          | UK                   |

< Back   Finish   Cancel

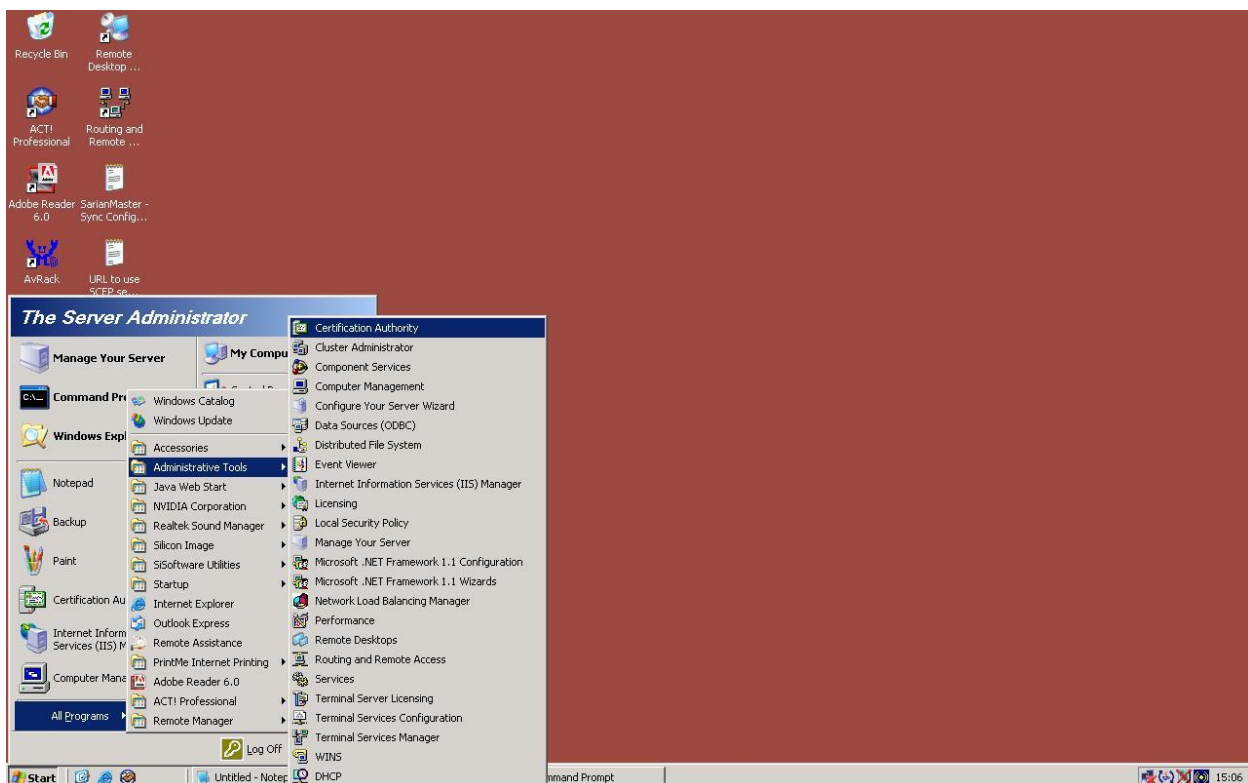
Finally a dialogue box will appear containing a URL to use for SCEP enrolment.

**IMPORTANT:** Make a permanent note of this URL. You will need it every time you create certificates with this CA.

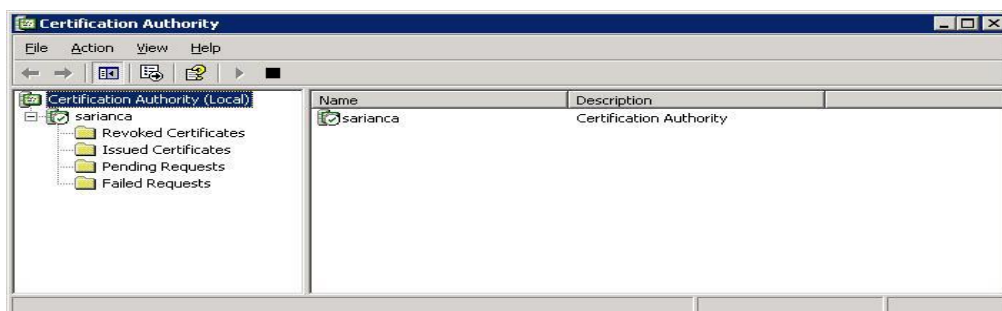


### 3.2.2 Check the CA Certificate service is running

To check the CA Certificate service is running, click **Start → All Programs → Administrative Tools → Certificate Authority**.



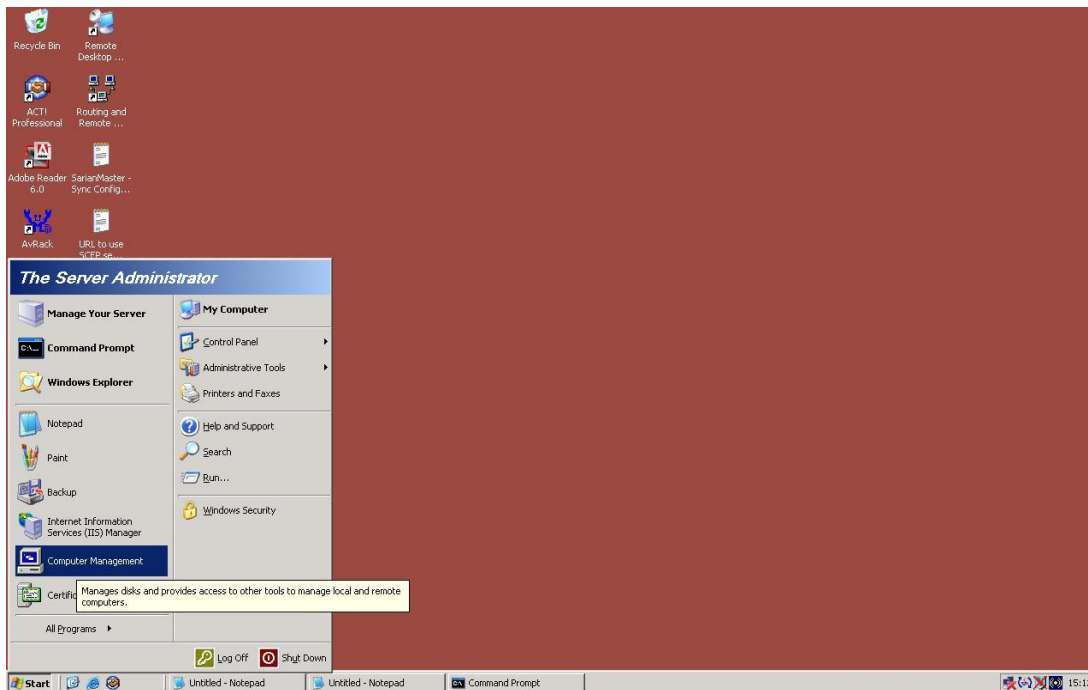
The Certificate Authority console window will open. If the service is running there will be a green tick on your Certificate Authority. If not the service will need to be started by right clicking on the Certificate Authority, select **All Tasks → Start Service**.



### 3.2.3 Configure IIS

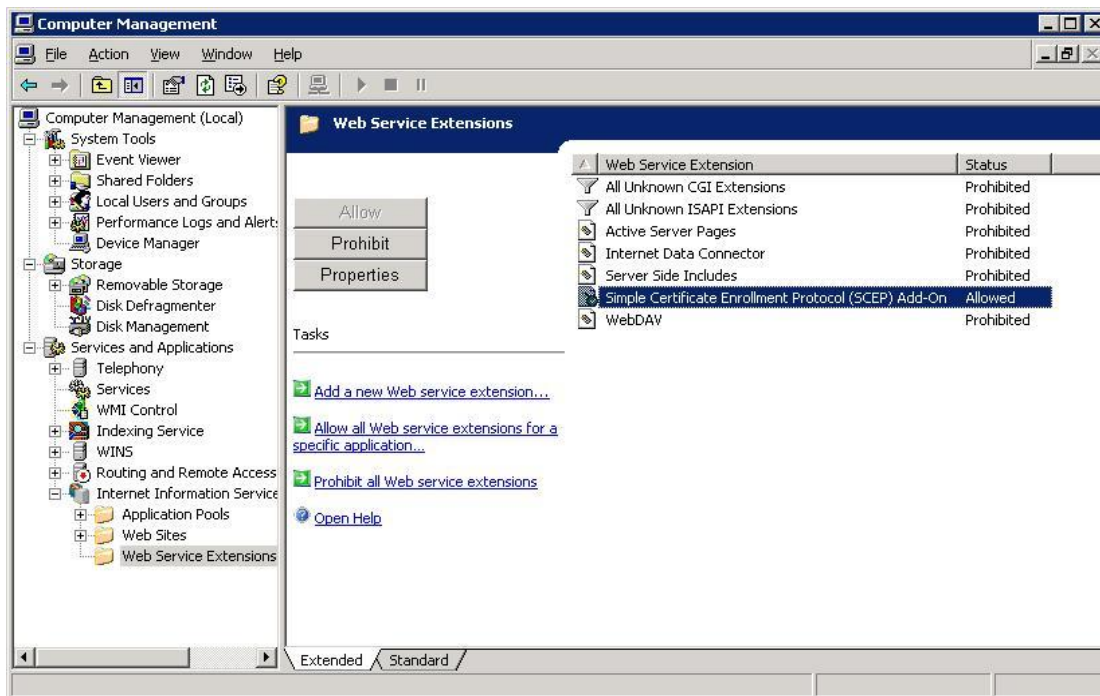
When IIS is installed, the service is installed in a highly secure and locked mode. Therefore you may have to configure IIS to allow the SCEP Add-on service to run in IIS.

Open the Computer Management console.



Expand the Services and Applications icon and Internet Information Services and Web Service Extensions.

In the **Web Service Extensions** window, highlight **Simple Certificate Enrolment Protocol (SCEP) Add-on**. Click the **Allow** button. A green tick should appear on that item.



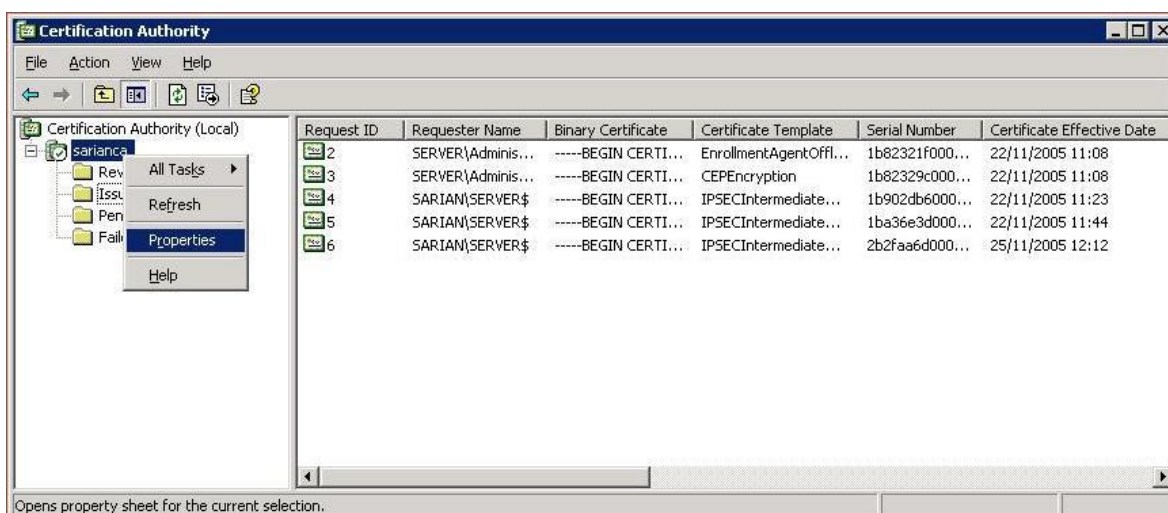
### 3.3 Automatic Enrolment

As with this application note, the default action for the Microsoft 2003 Certificate Authority is for all certificate requests to be issued manually by the CA administrator. This ensures that the administrator is responsible for verifying the identity of the certificate requestor.

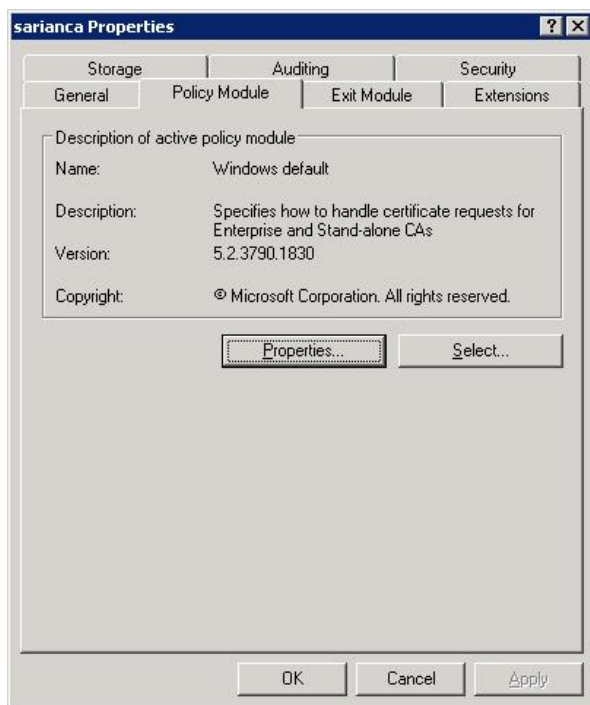
However, Microsoft have included a facility for automatic enrolment where certificates are signed and issued by the CA server automatically on receipt of the certificate request.

To enable this feature open the Certificate Authority console as previous. click **Start → All Programs → Administrative Tools → Certificate Authority**.

Right click on your certificate authority and select **Properties**.



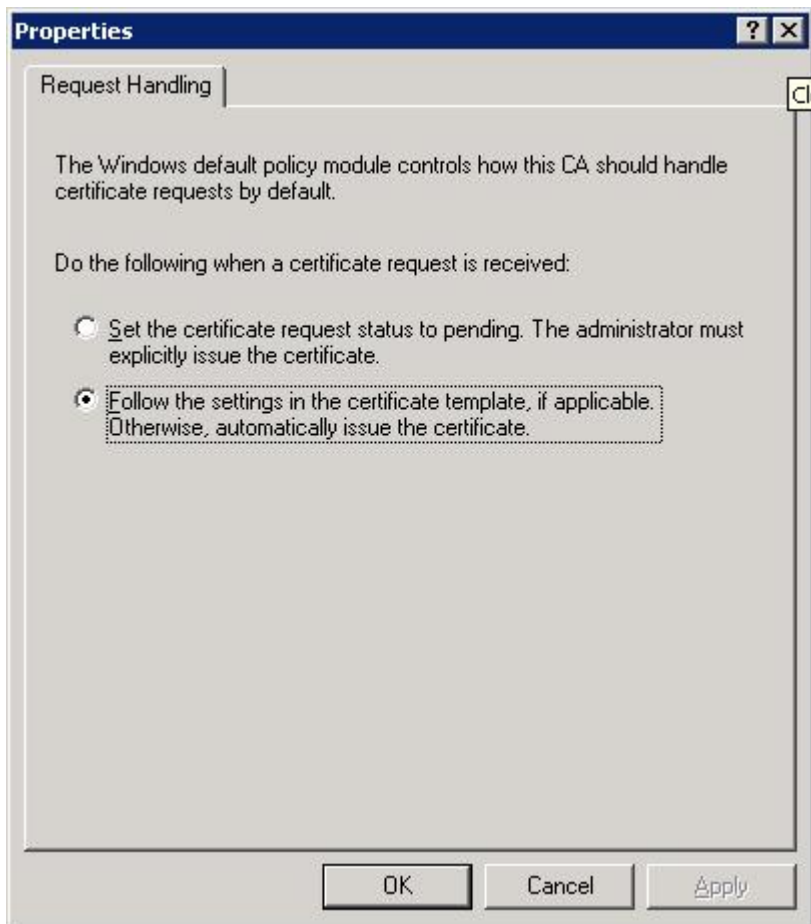
In the **Properties** window select the **Policy Module** tab.



Whilst in the **Policy Module** tab click the **Properties** button.

Select Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate.





Click **OK** and again **OK** on the **Policy Module** tab.

**Note:** For the change to take effect, certificate services must be stopped and started again.



## 4 VPN RESPONDER CERTIFICATES

### 4.1 Ethernet 0 LAN Configuration

The following configures the Ethernet local area network IP address for the VPN responder.

Browse to **CONFIGURATION - NETWORK → INTERFACES → ETHERNET → ETH 0**.

Configuration - Network > Interfaces > Ethernet > ETH 0

▼ ETH 0

Description: Inside Inrterface

☐ Get an IP address automatically using DHCP

☒ Use the following settings

IP Address: 172.16.0.254

Mask: 255.255.0.0

Gateway:

DNS Server:

Secondary DNS Server:

Changes to these parameters may affect your browser connection

| Parameter   | Setting      | Description                            |
|-------------|--------------|----------------------------------------|
| IP Address: | 172.16.0.254 | Configures the IP address for the LAN  |
| Mask:       | 255.255.0.0  | Configures the subnet mask for the LAN |

### 4.2 Time and Date

Any certificates stored on the TransPort's flash will have a validity period. Therefore it is important that the TransPort is configured with the correct time and date.

Browse to **CONFIGURATION → SYSTEM → Date and Time**

Amend the time and date as appropriate and click **Set Time** button.

**Configuration - System > Date and Time**

► **Device Identity**

▼ **Date and Time**

Current system time: 16 Aug 2012 12:28:23

Manually set the time

Hours: 12 Minutes: 28 Seconds: 23

Month: August Day: 16 Year: 2012

### 4.3 ADSL Interface Configuration

By default on the DR6410 MKII VPN Concentrator, PPP 1 is configured for use with ADSL. Here you enter the details of your ADSL account and enable IPSEC on this interface

Browse to

**Configuration - Network > Interfaces > Advanced > PPP 0 - 9 > PPP 1**

▼ **PPP 1 - ADSL**

Description:

This PPP interface will use

Dial out using numbers:

Prefix:  to the dial out number

Username:

Password:

Confirm password:

☒ Allow the remote device to assign a local IP address to this router

☐ Try to negotiate to use  as the local IP address for this router

☐ Use  as the local IP address for this router (i.e. not negotiable)

Use mask  for this interface

Use the following DNS servers if not negotiated

Primary DNS server:

Secondary DNS server:

DNS Port:

← Missing Lines →

☒ Enable NAT on this interface  
☒ IP address ☐ IP address and Port  
 NAT Source IP address:

☒ Enable IPsec on this interface  
☒ Keep Security Associations (SAs) when this PPP interface is disconnected  
 Use interface   for the source IP address of IPsec packets

☐ Enable the firewall on this interface

| Parameter         | Setting       | Description                                                 |
|-------------------|---------------|-------------------------------------------------------------|
| Username:         | Adsl_username | Enter the username for your ADSL account                    |
| Password:         | password      | Enter the password for your ADSL account                    |
| Confirm Password: | password      | Confirm the password for your ADSL account                  |
| IPSEC:            | ON            | Enables IPSEC on PPP 1 (ADSL) Interface                     |
| Keep SA           | ON            | Keeps Security Associations after Interface is disconnected |

**NB:** When configuring a router as an IPSEC “responder” such as this example where the outside interface is “always on” and has a fixed IP address, it is recommended that you choose the IPSEC option “**On – Keep SA’s when link down**”. This prevents the IPSEC Security Associations from being deleted should the link be dropped and thus enables the VPN tunnel to continue to work immediately as soon as the link becomes available again.

If this IPSEC value is set to “**On – Remove SA’s when link down**”, then the VPN tunnel will not continue to work should the link be dropped and raised until the IPSEC Security Associations on the IPSEC “Initiator” have timed out and new IPSEC Security Associations have been re-negotiated.

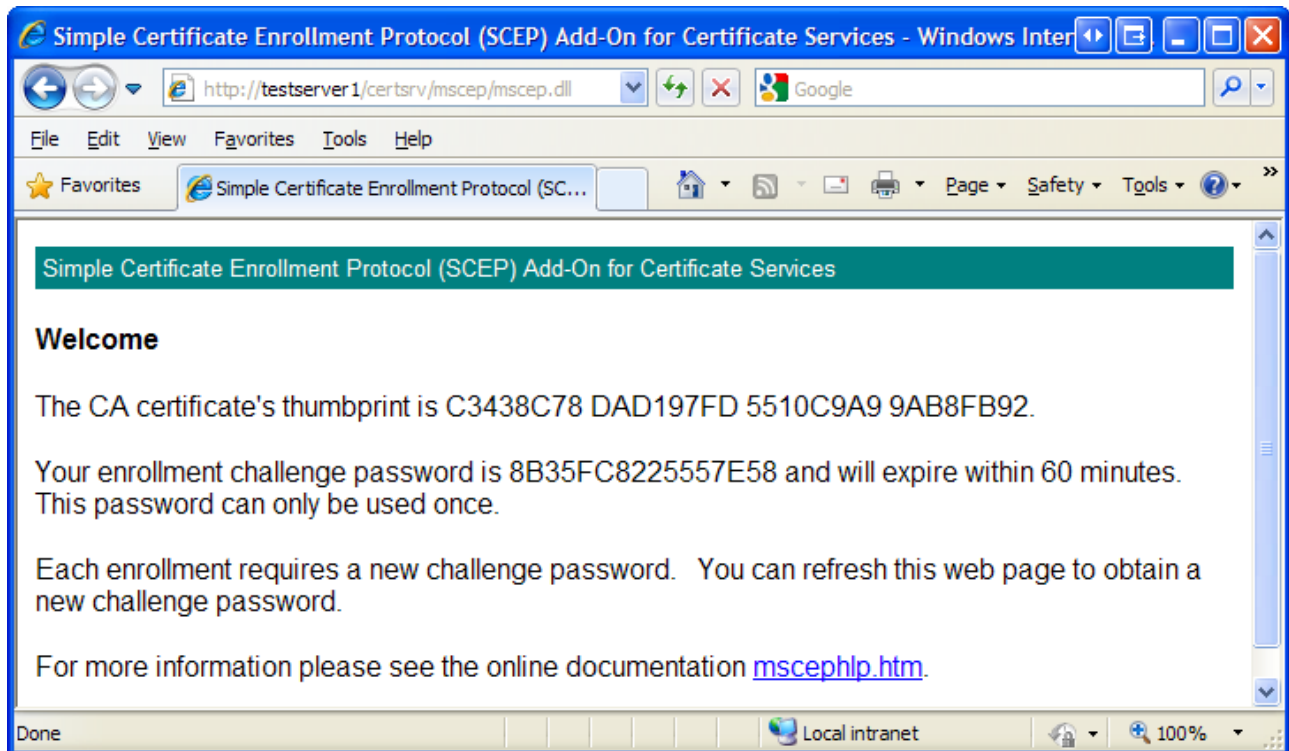
## 4.4 Creating the Private Key and Certificate Request

### 4.4.1 Obtain a Challenge Password for the Certificate Request.

Before you can create a certificate request you must first obtain a challenge password from the Certificate Authority Server. This password is generally obtained from the SCEP CA server by way of WEB server, or a phone call to the CA Server Administrator. For the Microsoft® SCEP server, you browse to a web interface. If the server requires a challenge password, it will be displayed on the page along with the CA certificate fingerprint.

This challenge password is usually only valid once and for a short period of time, in this case 60 minutes, meaning that a certificate request must be created after retrieving the challenge password.

From a PC browse to the following Microsoft® CA server web page using URL <http://<hostname>/certsrv/mscep/mscep.dll> (as detailed in “Microsoft® 2003 server Configuration) and make a note of the challenge password.

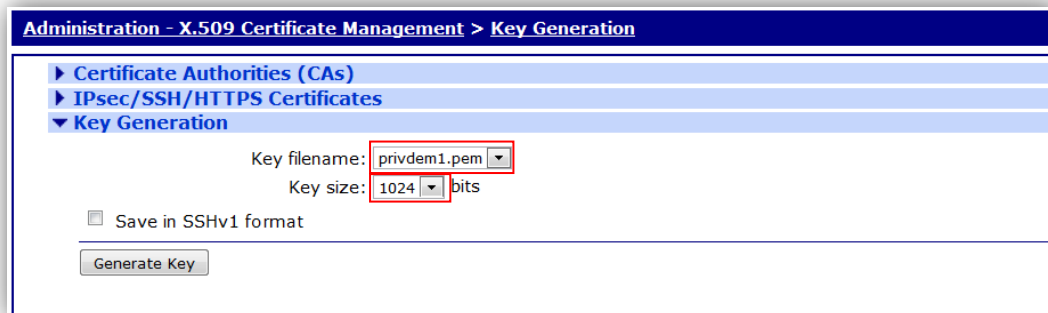


#### 4.4.2 Create the Private Key and Certificate

Now the details for the certificate request have been entered, the TransPort must create a Private Key and from this the certificate request will be created.

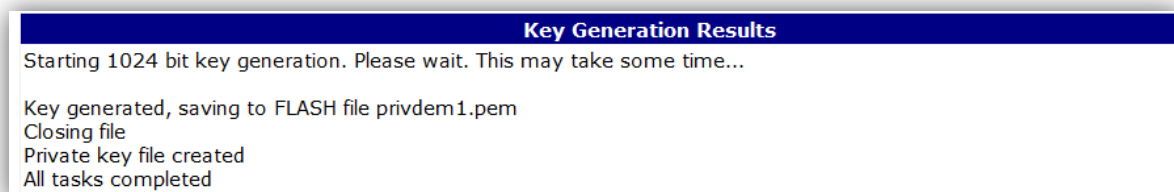
**NOTE:** This method assumes that a private key does NOT already exist. Both the private key and certificate request will be created simultaneously.

Browse to **Administrator – X.509 Certificate Management > Key Generation**.



| Parameter             | Setting      | Description                                                                                |
|-----------------------|--------------|--------------------------------------------------------------------------------------------|
| New Key Size:         | 1024         | Size of the private key in bits                                                            |
| Private Key filename: | privdem1.pem | Enter a name for the private key (must be prefixed with “priv” and have a .pem extension). |

Click the **Generate Certificate Request** button. You will see some indication of the progress as the TransPort generates the Private Key file and certificate request as follows;



### 4.4.3 Using SCEP to retrieve the CA certificates

Before delivering the request to the server, the unit must first have access to the server CA certificate(s). Some servers require the use of more than one CA certificate. In this case the Microsoft® 2003 server requires 3 CA certificates before SCEP can work. For other servers, just one certificate may be used for all three tasks. Check your server vendor for details.

The tasks these certificates are used for are:

**CA certificate.** This is the certificate that will contain the public key portion of the key used to sign the certificate request.

**CA encryption certificate.** This certificate is used to encrypt the data the client will send to the server.

**CA signature certificate.** This is attached to the reply from the CA which is validated by the client. The public key from this certificate is used to verify the signature.

Browse to **Administration – X.509 Certificate Management > Certificate Authorities (CAs)**

**Administration - X.509 Certificate Management > Certificate Authorities (CAs)**

**Upload CA Certificates**

Upload certificate authority (CA) certificates. Files may be in ASN.1 DER or PEM Base64 encoded formats.

Upload File:

**Obtain CA certificates from a SCEP Server**

SCEP Server IP address:  Port:

Path:

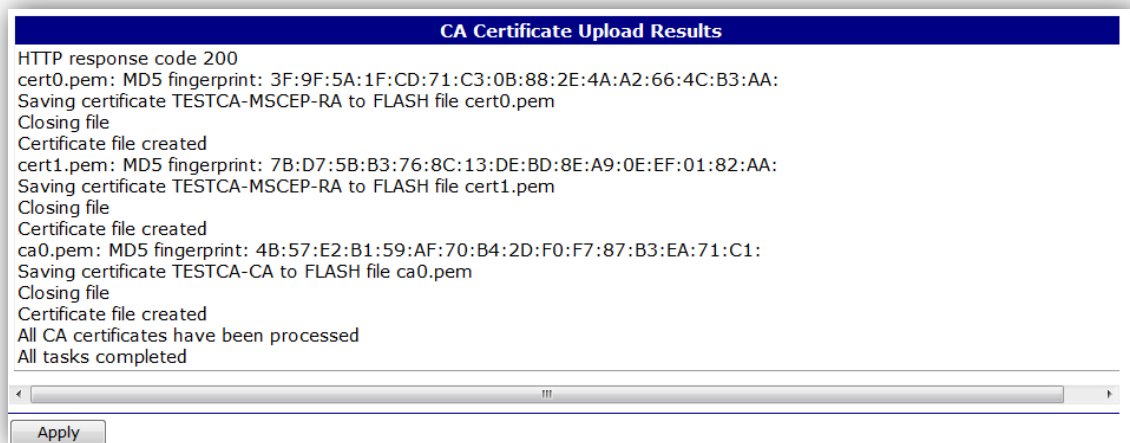
Application:

CA identifier:

| Parameter    | Setting                 | Description                                                                          |
|--------------|-------------------------|--------------------------------------------------------------------------------------|
| Host:        | CA server ip address    | The IP address/hostname of your CA server                                            |
| Remote port: | 0                       | MS SCEP uses HTTP port 80 to carry the requests unless you specify otherwise here.   |
| Path:        | certsrv/mscep/mscep.dll | Select Microsoft SCEP from drop down list and the path will be entered automatically |
| Application: | pkiclient.exe           | This represents the SCEP application on the server                                   |

|                |        |               |
|----------------|--------|---------------|
| CA Identifier: | testca | CA identifier |
|----------------|--------|---------------|

Click the **Get Ca certificate/s** button to retrieve the CA certificates from the Microsoft® 2003 Server. An indication of progress will be shown as follows;



The fingerprint of each certificate is displayed. This fingerprint of the CA certificate should be checked (using some out of band mechanism) against the fingerprint of the CA certificates as advertised by the server. For the Microsoft® server the CA certificate fingerprint is displayed when the page <http://<hostname>/certsrv/mscep/mscep.dll> is accessed.

If the fingerprints do not match, it possibly means that you have some attacker sitting between the unit and the server.

With a telnet session to the router issue the **dir** command, you will see the CA certificates prefixed with ca and cert.

|              |         |    |           |    |     |      |     |      |
|--------------|---------|----|-----------|----|-----|------|-----|------|
| direct       | 60720   | ro | 11:14:48, | 06 | Aug | 2012 | CRC | ???  |
| sbios        | 524288  | ro | 11:14:50, | 06 | Aug | 2012 | CRC | d340 |
| mirror       | 60720   | ro | 11:14:48, | 06 | Aug | 2012 | CRC | ???  |
| image        | 4496614 | rw | 11:14:48, | 06 | Aug | 2012 | CRC | 6f12 |
| sregs.dat    | 4096    | rw | 11:14:48, | 06 | Aug | 2012 | CRC | 08b2 |
| x3prof       | 4096    | rw | 11:14:48, | 06 | Aug | 2012 | CRC | bb5f |
| cert0.pem    | 1752    | rw | 14:34:29, | 16 | Aug | 2012 | CRC | d2b5 |
| cert1.pem    | 1728    | rw | 14:34:34, | 16 | Aug | 2012 | CRC | 4a3e |
| ca0.pem      | 1126    | rw | 14:34:39, | 16 | Aug | 2012 | CRC | fba0 |
| templog.cl   | 262144  | ro | 11:14:48, | 06 | Aug | 2012 | CRC | fbe9 |
| config.fac   | 9078    | ro | 11:14:48, | 06 | Aug | 2012 | CRC | 66c8 |
| image4.cl    | 224476  | rw | 11:14:48, | 06 | Aug | 2012 | CRC | 27c3 |
| LOGCODES.TXT | 19723   | rw | 11:14:48, | 06 | Aug | 2012 | CRC | d324 |
| 95159w#D.web | 1052005 | rw | 11:14:48, | 06 | Aug | 2012 | CRC | 34e0 |
| manual.sb    | 26826   | rw | 11:14:48, | 06 | Aug | 2012 | CRC | 0b0a |
| activate.sb  | 33685   | rw | 11:14:48, | 06 | Aug | 2012 | CRC | a314 |
| prlupdate.sb | 31523   | rw | 11:14:48, | 06 | Aug | 2012 | CRC | 11be |
| python.zip   | 1631597 | rw | 11:14:48, | 06 | Aug | 2012 | CRC | a6b3 |
| sregs.fac    | 4096    | ro | 11:14:48, | 06 | Aug | 2012 | CRC | 08b2 |
| wizards.zip  | 250087  | rw | 11:14:48, | 06 | Aug | 2012 | CRC | c8ab |
| fw.txt       | 762     | rw | 11:14:48, | 06 | Aug | 2012 | CRC | e5b3 |
| dspfw.bin    | 44340   | rw | 11:14:48, | 06 | Aug | 2012 | CRC | d16f |
| pwd.da0      | 154     | rw | 11:15:36, | 06 | Aug | 2012 | CRC | ???  |
| config.da0   | 1977    | rw | 09:44:38, | 15 | Aug | 2012 | CRC | 8020 |
| fwstat.txt   | 1800    | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| fwstat.htm   | 10500   | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| fwrules.htm  | 10500   | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| fwlog.txt    | 2100    | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| evstat.txt   | 10200   | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| evstat.htm   | 52500   | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| evstat.js    | 52500   | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| eventlog.txt | 35501   | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| eventlog.xml | 35501   | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| statbin.enc  | 60000   | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| ana.txt      | 1000000 | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| anaeth.cap   | 1000000 | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| anapp.cap    | 1000000 | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| anaip.cap    | 1000000 | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| anawifi.cap  | 1000000 | ro | 14:47:24, | 16 | Aug | 2012 |     |      |
| debug.txt    | 1000000 | ro | 14:47:24, | 16 | Aug | 2012 |     |      |



#### 4.4.4 Configure the Certificate Request Postion of page

Browse to **Administration - X.509 Certificate Management > IPsec/SSH/HTTPS Certificates**

Enter the above challenge password and configure all other fields as appropriate. These details will form part of the certificate request and thus form part of the signed public key certificate

**NOTE:** The **Common Name** (case sensitive) field is important as this will be used as the ID for the device for the IKE negotiations.

Administration - X.509 Certificate Management > IPsec/SSH/HTTPS Certificates

Enrollment

SCEP Server IP address: 10.1.10.249 Port: 0

Path: certsrv/mscep/mscep.dll (Microsoft SCEP)

Application: pkiclient.exe

CA identifier: testca

CA certificate: TESTCA-CA (ca0.pem)

CA encryption certificate: TESTCA-MSCEP-RA (cert1.pem)

CA signature certificate: TESTCA-MSCEP-RA (cert0.pem)

RSA Private Key: ☒ Use Existing Key  
☐ Generate new key with size 1024 bits

Private key filename: privdem1.pem

Enrollment Password: F88714641FE0666A

Common Name (CN): DR6400

Country Code (C): UK

State or Province (ST): Yorkshire

Locality (L): Leeds

Organisation (O): Digi International

Organisational unit (OU): Tech Support

E-mail: uksupport@digicom

Unstructured name: (Optional)

Digest Algorithm: MD5

☐ Ignore NONCE in SCEP response

Enroll

| Parameter           | Setting               | Description                                            |
|---------------------|-----------------------|--------------------------------------------------------|
| Challenge Password: | Password from website | Enter the Challenge Password issued by the SCEP server |
| Country:            | UK                    | Enter a two character representation of the country    |
| Common Name:        | DR6000                | Enter a Common Name for the router's ID                |

|                      |                      |                                                                              |
|----------------------|----------------------|------------------------------------------------------------------------------|
| Locality:            | Ilkley               | The Location of the unit                                                     |
| Organisation:        | Digi International   | An appropriate Company name                                                  |
| Organisational Unit: | Tech Support         | An appropriate organisational unit                                           |
| State:               | Yorkshire            | State or County or Province                                                  |
| Email Address:       | support@sarian.co.uk | An appropriate email Address                                                 |
| Unstructured Name:   |                      | Optional descriptive text                                                    |
| Digest Algorithm:    | MD5                  | Choose either MD5 or SHA1. This is used when signing the certificate request |

#### 4.4.5 Using SCEP to Enroll the Certificate Request

The next process is to send the certificate request to the CA server for signing. This will be the router's 'public key'. Complete the SCEP configuration as follows in order to enroll the certificate request.

**NB:** See section 5.6.1 for identifying the CA certificates

Browse to **Administration - X.509 Certificate Management > IPsec/SSH/HTTPS Certificates**.

**Administration - X.509 Certificate Management > IPsec/SSH/HTTPS Certificates**

**Enrollment**

SCEP Server IP address: 10.1.10.249 Port: 0

Path: certsrv/mscep/mscep.dll (Microsoft SCEP)

Application: pkiclient.exe

CA identifier: testca

CA certificate: TESTCA-CA (ca0.pem)

CA encryption certificate: TESTCA-MSCEP-RA (cert1.pem)

CA signature certificate: TESTCA-MSCEP-RA (cert0.pem)

RSA Private Key: ☒ Use Existing Key ☐ Generate new key with size 1024 bits

Private key filename: privdem1.pem

Enrollment Password: F88714641FE0666A

Common Name (CN): DR6400

Country Code (C): UK

State or Province (ST): Yorkshire

Locality (L): Leeds

Organisation (O): Digi International

Organisational unit (OU): Tech Support

E-mail: uksupport@digicom

Unstructured name: (Optional)

Digest Algorithm: MD5

☐ Ignore NONCE in SCEP response

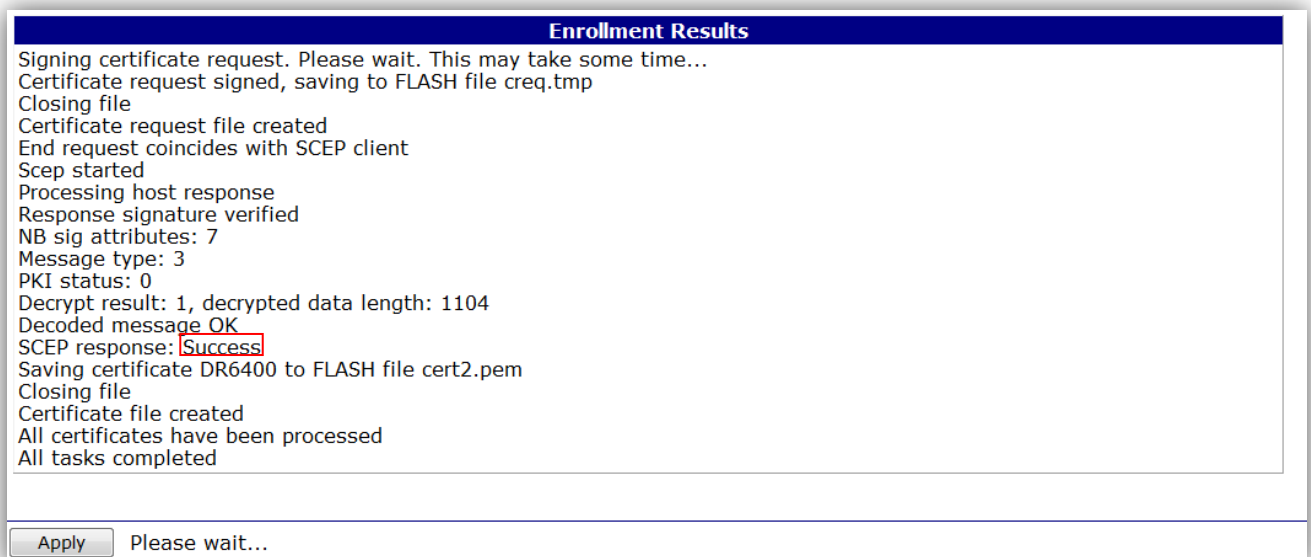
**Enroll**

| Parameter                     | Setting                 | Description                                                                          |
|-------------------------------|-------------------------|--------------------------------------------------------------------------------------|
| Host:                         | 10.1.10.249             | The IP address/hostname of your CA server                                            |
| Remote port:                  | 0                       | MS SCEP uses HTTP port 80 to carry the requests unless you specify otherwise here.   |
| Path:                         | certsrv/mscep/mscep.dll | Select Microsoft SCEP from drop down list and the path will be entered automatically |
| Application:                  | pkiclient.exe           | This represents the SCEP application on the server                                   |
| CA Identifier:                | testca                  | CA identifier                                                                        |
| Private Key filename :        | privdem1.pem            | The name of the private key created earlier                                          |
| Certificate request filename: | creq.pem                | The name of the certificate request                                                  |

|                                     |              |                                                                            |
|-------------------------------------|--------------|----------------------------------------------------------------------------|
|                                     |              | created earlier                                                            |
| Certificate filename:               | certdem1.pem | Enter a name for the public key certificate (must be prefixed with 'cert') |
| CA certificate filename:            | ca2.pem      | Enter the name of the CA certificate.                                      |
| CA encryption certificate filename: | ca1.pem      | Enter the name of the CA encryption certificate.                           |
| CA signature certificate filename:  | ca0.pem      | Enter The name of the CA signature certificate                             |

#### 4.4.6 Signing the certificate request

Once the SCEP configuration page has been completed click the **Enroll Certificate Request** button.

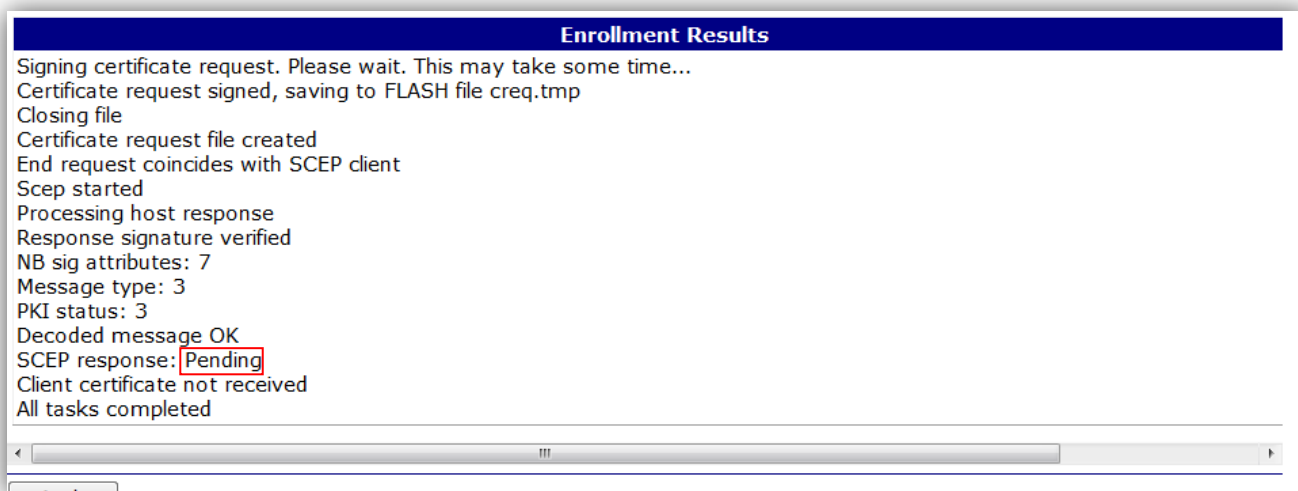


You should receive one of three responses.

**Failure** - The request failed. Check that the correct CA certificates have been used. Check that the challenge password is correct. Check that the correct certificate request has been specified, and that the correct private key has been used. Check the server logs to see what the problem is.

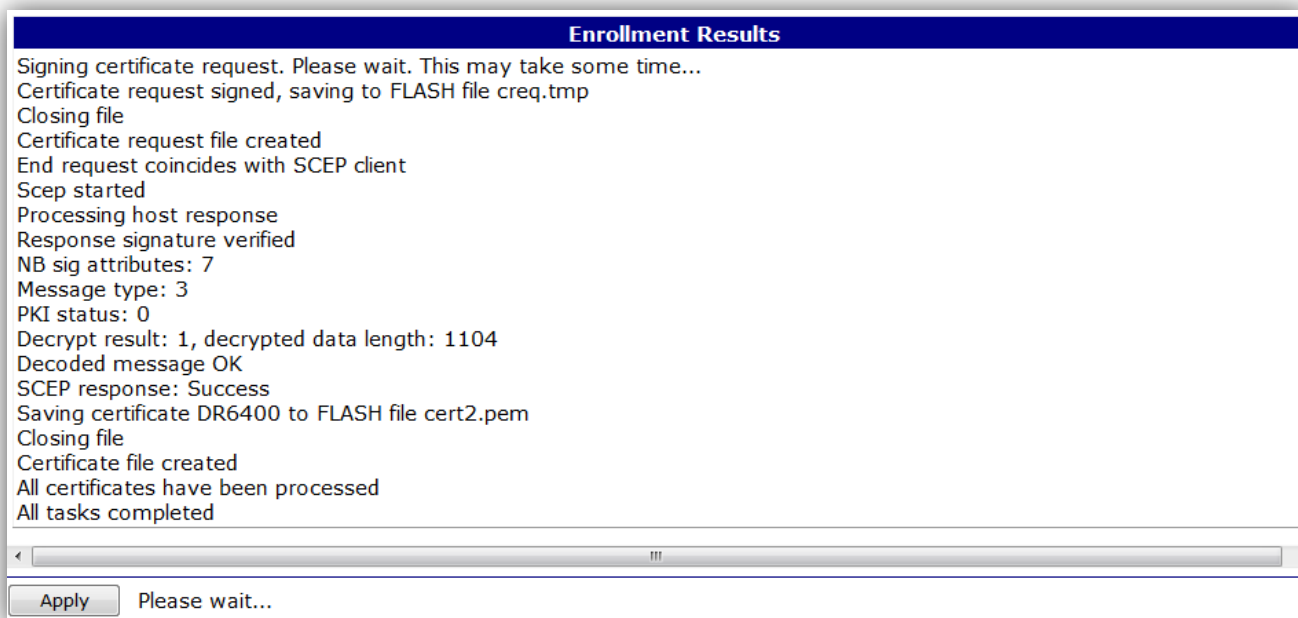
**Success** - The response should contain the signed certificate.

**Pending** - The server has our request, but hasn't signed it yet. It may require some input by the System Administrator.



The unit should poll the server occasionally until the certificate is returned. However, if you know that the certificate request has been allowed having contacted the System Administrator you can simply press the **Enroll Certificate Request** button again rather than wait for the TransPort to re-poll.

**NB:** If you are the CA Server Administrator and you have received the **Pending** enrollment result, see **section 5.4.9** to see how you would issue and approve or deny a certificate request. Otherwise skip to paragraph 6.



#### 4.4.7 Identifying the CA certificates

To complete the previous task you would normally need to determine which certificate is used for what task. For the purpose of this application note these have already been determined but for future reference the following information will be useful

If only one CA certificate is returned, it is a trivial task. When three are returned, you need to display the certificates using the 'view' button having selected a CA certificate from the drop down list and investigate the attributes of the certificate.

##### Identifying the CA certificate:

This certificate will have matching Issuer and Subject fields. It may have a V3 extension which shows something like...

```
X509v3 Basic Constraints: critical
```

```
CA: TRUE
```

##### Identifying the encryption certificate:

This certificate will have an Issuer which matches the CA certificate. It will probably have a V3 extension something like...

```
X509v3 Key Usage: critical
```

```
Key Encipherment, Data Encipherment
```

##### Identifying the signature certificate:

This certificate will have an Issuer which matches the CA certificate. It will probably have a V3 extension something like...

```
X509v3 Key Usage: critical
```

```
Digital Signature, Non Repudiation
```

For example the following screen shot of the same page after clicking a 'view' button to determine which of the CA certificates is the encryption certificate.

## Configuration - Security > Certificates > SCEP

Certificate file: cal.pem

MD5 fingerprint: E0:50:4A:66:F5:01:5A:61:E3:6E:4A:87:A5:66:EE:21:

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

56:42:1a:f8:00:00:00:00:00:03

Signature Algorithm: sha1WithRSAEncryption

Issuer: CN=testCA

Validity

Not Before: Jul 3 14:43:02 2009 GMT

Not After : Jul 3 14:53:02 2010 GMT

Subject: C=UK,

ST=Yorkshire,

L=Ilkley,

O=Digi International,

OU=Tech Support,

CN=sarianca\_demo/emailAddress=support@digi.co.uk

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:b3:29:9f:ae:79:fc:4c:43:70:3c:72:f9:34:47:f2:  
35:65:6c:0d:73:4f:52:b2:21:7b:74:02:37:19:c9:f5:  
7e:2e:18:82:71:7b:64:16:03:4f:f8:75:b5:5c:a5:8a:  
81:a8:96:79:3a:ec:e6:89:ac:ea:cc:89:56:77:1f:16:  
82:a6:8e:79:4e:9c:e5:8c:5c:e7:44:12:2e:0b:8e:9f:  
8e:86:b2:33:06:47:85:c1:f8:67:22:38:1f:7b:ac:c0:  
46:0e:42:cb:f1:3c:5c:09:f6:e8:65:a4:bf:1a:a9:d6:  
e4:ef:5b:1d:91:d1:52:a9:dc:33:35:d4:e1:f2:23:18:  
63

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage: critical

Key Encipherment, Data Encipherment

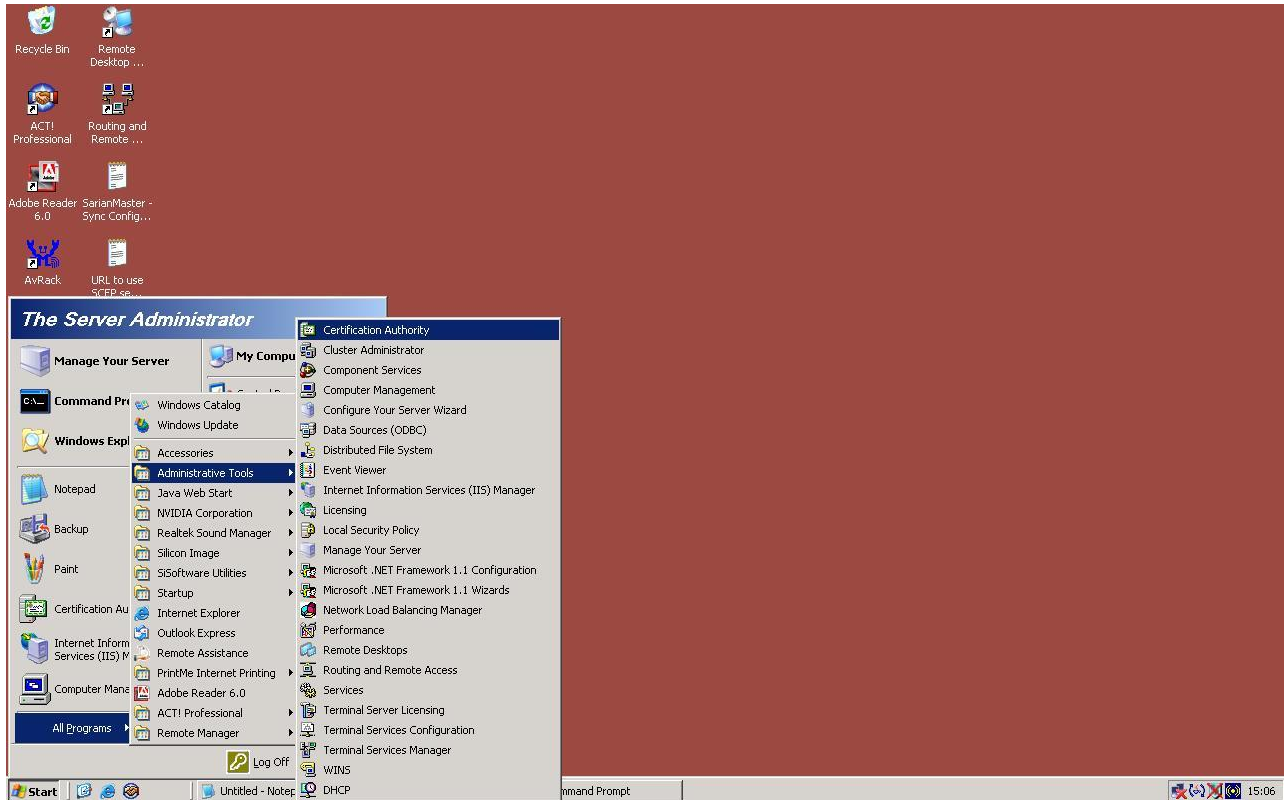
S/MIME Capabilities:

0'0...\*.H.....80...\*.H.....80...+....

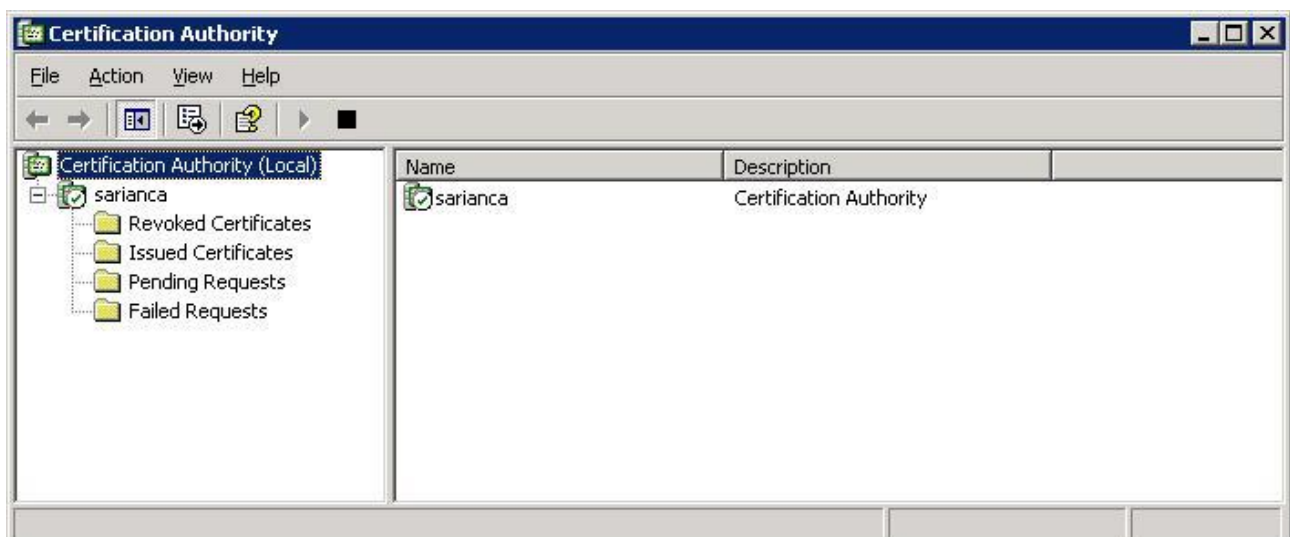
#### 4.4.8 Issuing a Signed Certificate on the Microsoft® 2003 Server

Login to the Microsoft® 2003 Server with an appropriate System Administrator account

With your mouse click START → ALL PROGRAMS → ADMINISTRATIVE TOOLS → CERTIFICATION AUTHORITY



The **Certification Authority** console will open.

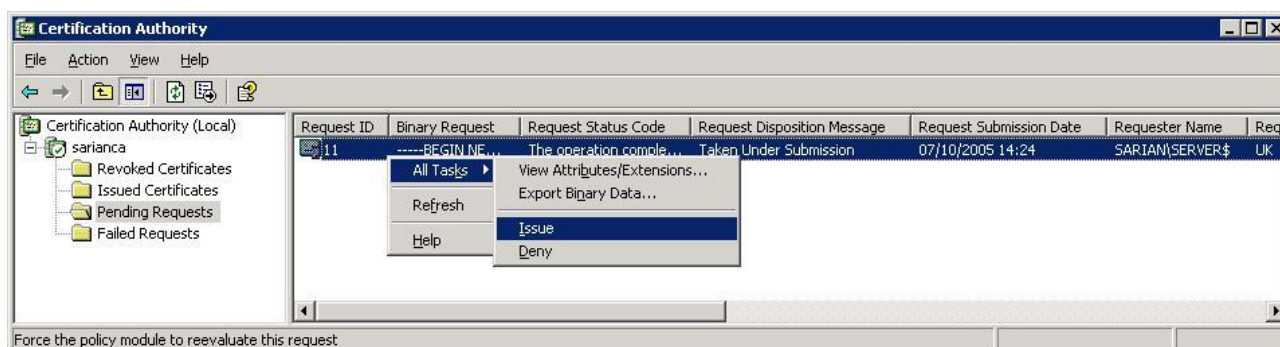




To sign and issue a pending certificate request click on the **Pending Requests** directory.

Right-click the pending certificate and highlight the '**All Tasks**' option which will reveal another menu.

From the new menu select the '**Issue**' option to sign the certificate request.



Once the certificate request has been signed you can wait for the router to automatically re-poll the CA server over time or re-poll manually by again clicking on the **Enroll Certificate Request** button as before.

You should now see a success message indicating that the certificate request has been signed and returned by the CA. This is the routers public key.

**If you wish to view your public key certificate, browse to CONFIGURATION → SECURITY → CERTIFICATES → SCEP. In the Certificate filename: parameter drop down list select the name of the public key certificate (certdem2.pem in this case) and click the view button.**

## 5 VPN CLIENT CERTIFICATES

### 5.1 Ethernet 0 LAN Configuration

The following configures the Ethernet local area network IP address for the VPN responder.

Browse to **CONFIGURATION → INTERFACES → ETHERNET → ETH 0 → CONFIGURE**

The screenshot shows the 'Configuration - Network > Interfaces > Ethernet > ETH 0' page. Under the 'ETH 0' tab, the 'Description' is 'Inside Interface'. The 'Get an IP address automatically using DHCP' option is unselected, and 'Use the following settings' is selected. The 'IP Address' field is set to '192.168.0.254' and the 'Mask' field is set to '255.255.255.0'. Below these are fields for 'Gateway', 'DNS Server', and 'Secondary DNS Server'. A message states 'Changes to these parameters may affect your browser connection'. At the bottom, there are tabs for 'Advanced', 'QoS', and 'VRRP'. An 'Apply' button is present, and a message says 'Configuration successfully applied. Click [here](#) to save configuration.'

| Parameter   | Setting       | Description                            |
|-------------|---------------|----------------------------------------|
| IP Address: | 192.168.0.254 | Configures the IP address for the LAN  |
| Mask:       | 255.255.255.0 | Configures the subnet mask for the LAN |

### 5.2 Time and Date

Any certificates stored on the TransPort's flash will have a validity period. Therefore it is important that the TransPort is configured with the correct time and date.

Browse to **CONFIGURATION → SYSTEM → TIME**

Amend the time and date as appropriate and click **Set Time** button.

**Configuration - System > Date and Time**

► **Device Identity**

▼ **Date and Time**

Current system time: 16 Aug 2012 12:28:23

Manually set the time

Hours: 12 Minutes: 28 Seconds: 23

Month: August Day: 16 Year: 2012

### 5.3 Wireless WAN Interface Configuration

By default on the WR44 W-WAN router, PPP 1 is configured for use with 3G.

Here you enter the details of your 3G/GPRS account and enable IPSEC on this interface

Browse to **Configuration - Network > Interfaces > Advanced > PPP 1**.

**Configuration - Network > Interfaces > Advanced > PPP 1**

▼ **PPP 1 - W-WAN**

Description: W-WAN

This PPP interface will use W-WAN

Dial out using numbers: \*98\*1#

Prefix: to the dial out number

Username:

Password:

Confirm password:

☒ Allow the remote device to assign a local IP address to this router

☐ Try to negotiate to use 0.0.0.0 as the local IP address for this router

☐ Use 0.0.0.0 as the local IP address for this router (i.e. not negotiable)

Use mask 255.255.255.255 for this interface

Use the following DNS servers if not negotiated

**Configuration - System > Date and Time**

► **Device Identity**

▼ **Date and Time**

Current system time: 16 Aug 2012 12:28:23

Manually set the time

Hours: 12 Minutes: 28 Seconds: 23

Month: August Day: 16 Year: 2012

☒ Enable NAT on this interface  
☒ IP address ☐ IP address and Port  
 NAT Source IP address:

☒ Enable IPsec on this interface

☐ Keep Security Associations (SAs) when this PPP interface is disconnected  
 Use interface   for the source IP address of IPsec packets

☐ Enable the firewall on this interface

| Parameter         | Setting  | Description                                   |
|-------------------|----------|-----------------------------------------------|
| Username:         | username | Enter the username for your 3G/GPRS account   |
| Password:         | password | Enter the password for your 3G/GPRS account   |
| Confirm Password: | password | Confirm the password for your 3G/GPRS account |
| IPSEC:            | ON       | Enables IPSEC on PPP 1 (ADSL) Interface       |

**NB:** When configuring a router with a dynamic WAN IP address as an IPSEC “initiator” such as this example, it is recommended that you choose the IPSEC option “**On** –

Browse to **Configuration - Network > Interfaces > Mobile**

The screenshot shows the 'Configuration - Network > Interfaces > Mobile' page. It includes a 'Mobile' section with instructions to select a SIM and apply settings. A dropdown menu shows 'SIM: 1 (PPP)' and 'IMSI: Unknown'. Below is the 'Mobile Settings' section with instructions to select service plan and connection settings. The 'Mobile Service Provider Settings' section contains fields for 'Service Plan / APN' (with a placeholder 'Your.APN.goes.here'), 'Use backup APN' (checkbox), 'Retry the main APN after' (0 minutes), 'SIM PIN' (Optional), 'Confirm SIM PIN', 'Username' (Optional), 'Password' (Optional), and 'Confirm Password'.

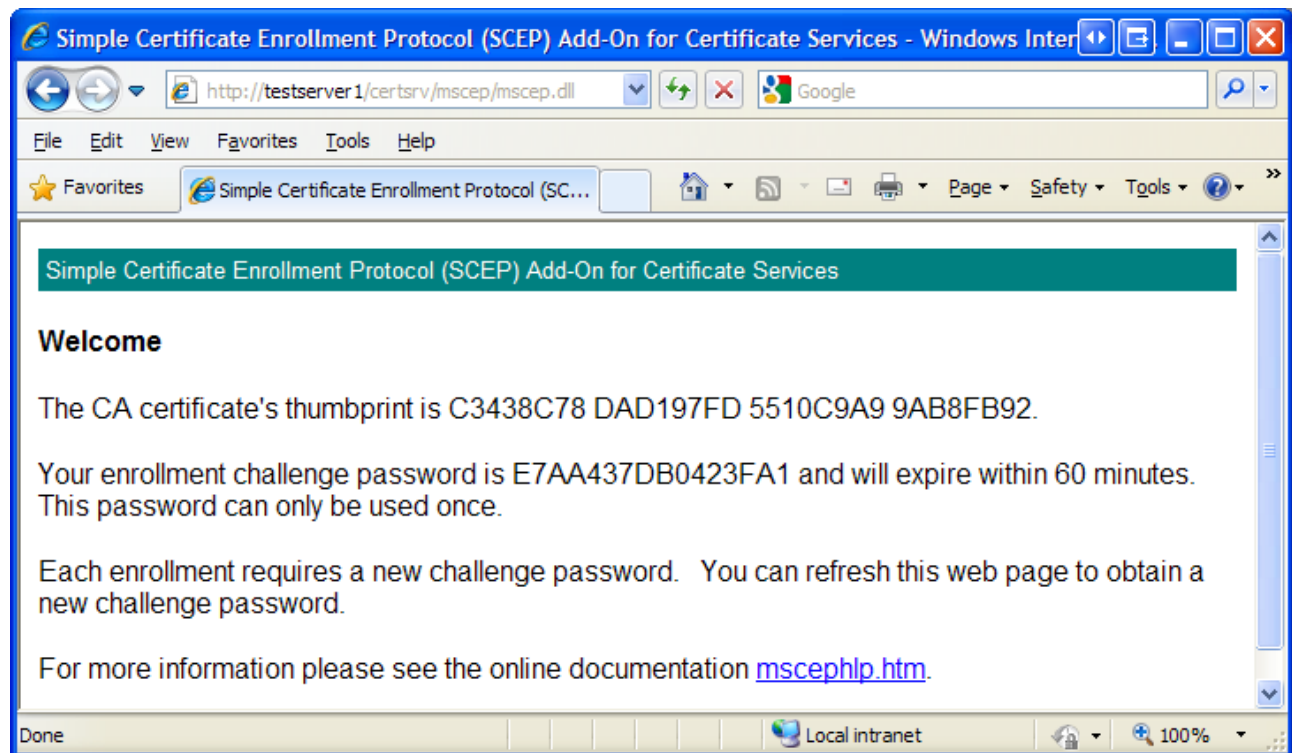
| Parameter | Setting  | Description                                 |
|-----------|----------|---------------------------------------------|
| APN:      | Your_APN | Enter the APN given by the 3G/GPRS provider |
| PIN:      | SIM_PIN  | Enter your SIM card PIN (if required)       |

## 5.4 Creating the Private Key and Certificate Request

Obtain a Challenge Password for the Certificate Request.

From a PC browse to the Microsoft® CA server web page using URL

<http://<hostname>/certsrv/mscep/mscep.dll> (as detailed in “Microsoft® 2003 server Configuration) and make a note of the challenge password.



### 5.4.1 Configure the Certificate Request page

Browse to **CONFIGURATION → SECURITY → CERTIFICATES → CERTIFICATE REQUEST**

Enter the above challenge password and configure all other fields as appropriate. These details will form part of the certificate request and thus form part of the signed public key certificate

**NOTE:** The **Common Name** (case sensitive) field is important as this will be used as the ID for the device for the IKE negotiations.

**Administration - X.509 Certificate Management > IPsec/SSH/HTTPS Certificates**

**Enrollment**

SCEP Server IP address: 10.1.10.249 Port: 0

Path: certsrv/mscep/mscep.dll (Microsoft)

Application: pkident.exe

CA identifier: testca

CA certificate: TESTCA-CA

CA encryption certificate: TESTCA-MSCEP-RA

CA signature certificate: TESTCA-MSCEP-RA

RSA Private Key: ☒ Use Existing Key  
☐ Generate new key with size 1024 bits

Private key filename: privdem2.pe

Enrollment Password: 4BE12AE4AE41D3D3

Common Name (CN): WR44

Country Code (C): UK

State or Province (ST): Yorkshire

Locality (L): Ilkley

Organisation (O): Digi International

Organisational unit (OU): Tech Support

E-mail: uksupport@digicom

Unstructured name: (Optional)

Digest Algorithm: MD5

☐ Ignore NONCE in SCEP response

**Enroll**

| Parameter            | Setting            | Description                                                                  |
|----------------------|--------------------|------------------------------------------------------------------------------|
| Challenge Password:  | 4BE12AE4AE41D3D3   | Enter the Challenge Password issued by the SCEP server                       |
| Country:             | UK                 | Enter a two character representation of the country                          |
| Common Name:         | WR44               | Enter a Common Name of your choice for the router's ID (case sensitive).     |
| Locality:            | Ilkley             | The Location of the router                                                   |
| Organisation:        | Digi International | An appropriate Company name                                                  |
| Organisational Unit: | Tech Support       | An appropriate organisational unit                                           |
| State:               | Yorkshire          | State or County or Province                                                  |
| Email Address:       | uksupport@digi.com | An appropriate email Address                                                 |
| Unstructured Name:   |                    | Optional descriptive text                                                    |
| Digest Algorithm:    | MD5                | Choose either MD5 or SHA1. This is used when signing the certificate request |

#### 5.4.2 Create the Private Key and Certificate Request Files

Now the details for the certificate request have been entered, the TransPort must create a Private Key and from this the certificate request will be created.

**NOTE:** This method assumes that a private key does NOT already exist. Both the private key and certificate request will be created simultaneously. If the **New key size:** parameter is set to **OFF** then a private key will not be generated.

Browse to **Administrator – X.509 Certificate Management > Key Generation**.



**Administration - X.509 Certificate Management > Key Generation**

▼ **Key Generation**

Key filename:

Key size:  bits

☐ Save in SSHv1 format

| Parameter             | Setting      | Description                                                                                |
|-----------------------|--------------|--------------------------------------------------------------------------------------------|
| New Key Size:         | 1024         | Size of the private key in bits                                                            |
| Private Key filename: | privdem2.pem | Enter a name for the private key (must be prefixed with “priv” and have a .pem extension). |

Click the **Generate Key** button. You will see some indication of the progress as the TransPort generates the Private Key file and certificate request as follows;

**Administration - X.509 Certificate Management > Key Generation**

**Key Generation Results**

Starting 1024 bit key generation. Please wait. This may take some time...

Key generated, saving to FLASH file privdem2.pem

Closing file

Private key file created

All tasks completed

## 5.5 Using SCEP to retrieve the CA certificates

Ensure the TransPort router is able to connect to the CA Server.

Browse to **Administration - X.509 Certificate Management > Certificate Authorities (CAs)**.

**Administration - X.509 Certificate Management > Certificate Authorities (CAs)**

Obtain CA certificates from a SCEP Server

SCEP Server IP address:  Port:

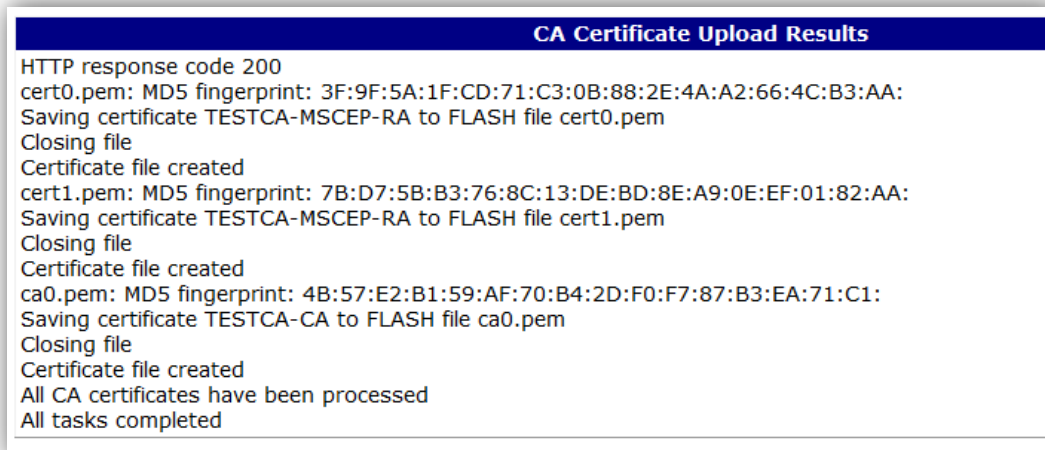
Path:  ▼

Application:

CA identifier:

| Parameter      | Setting                 | Description                                                                            |
|----------------|-------------------------|----------------------------------------------------------------------------------------|
| Host:          | 10.1.10.249             | The IP address/hostname of your CA server                                              |
| Remote port:   | 0                       | MS SCEP uses HTTP port 80 to carry the requests unless you specify otherwise here.     |
| Path:          | certsrv/mscep/mscep.dll | Select 'Microsoft SCEP' from drop down list and the path will be entered automatically |
| Application:   | pkiclient.exe           | This represents the SCEP application on the server                                     |
| CA Identifier: | testca                  | CA identifier                                                                          |

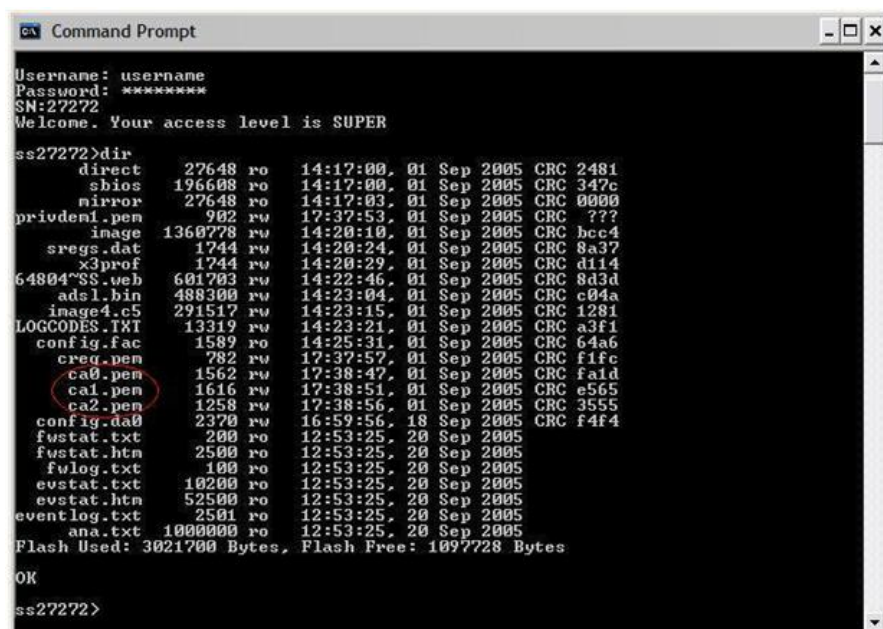
Click the **Get Ca certificate/s** button to retrieve the CA certificates from the Microsoft® 2003 Server. An indication of progress will be shown as follows;



The fingerprint of each certificate is displayed. This fingerprint of the CA certificate should be checked (using some out of band mechanism) against the fingerprint of the CA certificates as advertised by the server. For the Microsoft® server the CA certificate fingerprint is displayed when the page <http://<hostname>/certsrv/mscep/mscep.dll> is accessed.

If the fingerprints do not match, it possibly means that you have some attacker sitting between the router and the server.

If you open telnet session to the router and issue the **dir** command, you will see the CA certificates with the ca file prefix.



## 5.6 Using SCEP to Enroll the Certificate Request

Next send the certificate request to the CA server for signing. This will be the router's 'public key'. The SCEP configuration page can be completed in order to enroll the certificate request.

Browse to **CONFIGURATION → SECURITY → CERTIFICATES → SCEP**.

The screenshot shows the 'Enrollment' page under 'Administration - X.509 Certificate Management > IPsec/SSH/HTTPS Certificates'. The page contains the following fields and options:

- SCEP Server IP address: 10.1.10.249
- Port: 0
- Path: certsrv/mscep/mscep.dll (Microsoft)
- Application: pkident.exe
- CA identifier: testca
- CA certificate: TESTCA-CA
- CA encryption certificate: TESTCA-MSCEP-RA
- CA signature certificate: TESTCA-MSCEP-RA
- RSA Private Key: ☒ Use Existing Key, ☐ Generate new key with size 1024 bits
- Private key filename: privdem2.pe
- Enrollment Password: 4BE12AE4AE41D3D3
- Common Name (CN): WR44
- Country Code (C): UK
- State or Province (ST): Yorkshire
- Locality (L): Ilkley
- Organisation (O): Digi International
- Organisational unit (OU): Tech Support
- E-mail: uksupport@digicom
- Unstructured name: (Optional)
- Digest Algorithm: MD5
- ☐ Ignore NONCE in SCEP response

An 'Enroll' button is located at the bottom left of the form.

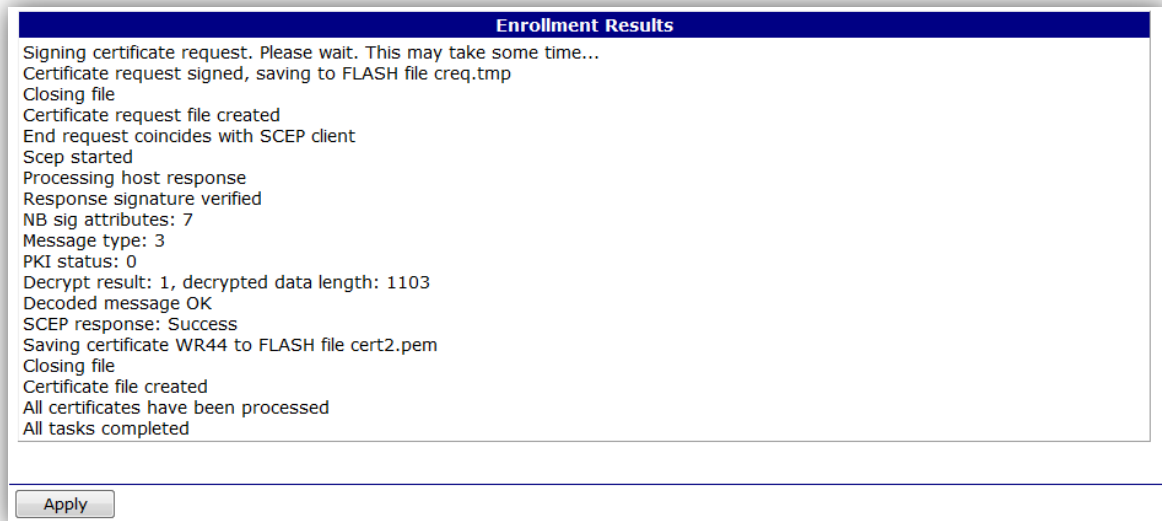
| Parameter                           | Setting                 | Description                                                                          |
|-------------------------------------|-------------------------|--------------------------------------------------------------------------------------|
| Host:                               | 10.1.10.249             | The IP address/hostname of your CA server                                            |
| Remote port:                        | 0                       | MS SCEP uses HTTP port 80 to carry the requests unless you specify otherwise here.   |
| Path:                               | certsrv/mscep/mscep.dll | Select Microsoft SCEP from drop down list and the path will be entered automatically |
| Application:                        | pkiclient.exe           | This represents the SCEP application on the server                                   |
| CA Identifier:                      | Testca                  | CA identifier                                                                        |
| Private Key filename :              | privdem2.pem            | The name of the private key created earlier                                          |
| CA certificate filename:            | ca2.pem                 | Enter the name of the CA certificate.                                                |
| CA encryption certificate filename: | ca1.pem                 | Enter the name of the CA encryption certificate.                                     |
| CA signature certificate filename:  | ca0.pem                 | Enter The name of the CA signature certificate                                       |

### 5.6.1 Identifying the CA certificates

See “Identifying the CA certificates” in **section 5.6.1**

### 5.6.2 Signing the certificate request

Once the SCEP configuration page has been completed click the **Enroll Certificate Request** button.



You should receive one of three responses. In this example the CA Server has returned a **Success** message.

**Failure** - The request failed. Check that the correct CA certificates have been used. Check that the challenge password is correct. Check that the correct certificate request has been specified, and that the correct private key has been used. Check the server logs to see what the problem is.

**Success** - The response should contain the signed certificate.

**Pending** - The server has our request, but hasn't signed it yet. It may require some input by the System Administrator. The unit should poll the server occasionally until the certificate is returned. However, if you know that the certificate request has been allowed having contacted the System Administrator you can simply press the **Enroll Certificate Request** button again rather than wait for the TransPort to re-poll.

**NB:** *If you are the CA Server Administrator and you have received the **Pending** enrollment result, see **section 5.7** to see how you would issue and approve or deny a certificate request. Otherwise skip to paragraph 7.*

## 6 CONFIGURE IKE AND IPSEC – VPN RESPONDER

### 6.1 Configure IKE (Internet Key Exchange)

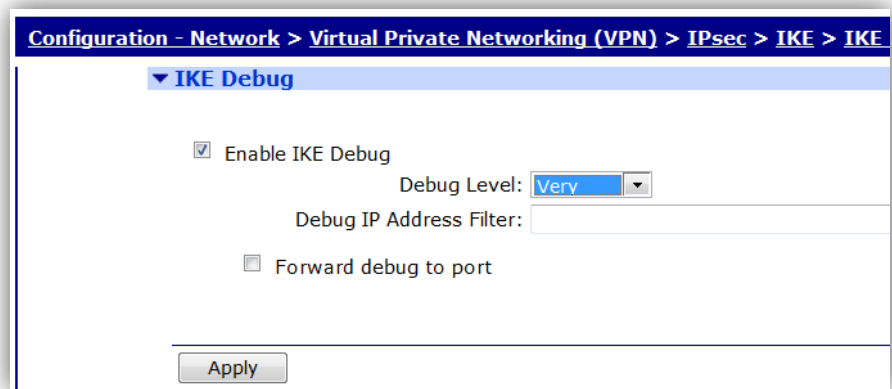
IKE is the first stage in establishing a secure link between two endpoints. The VPN Responder will act as the IKE ‘responder’ and as such will not initiate VPN tunnels. By default the DR6410 MKII responder setup is configured to accept the full range of authentication and encryption algorithms available.

Browse to **Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Responder**

The screenshot shows the 'IKE Responder' configuration page. The breadcrumb trail at the top is 'Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Responder'. The page has two main sections: 'IKE Responder' and 'Advanced'. In the 'IKE Responder' section, the 'Enable IKE Responder' checkbox is checked. Below it, 'Accept IKE Requests with' shows encryption algorithms (DES, 3DES, AES 128/192/256 bit) and authentication algorithms (MD5, SHA1) all checked. The 'MODP Group' is set between 1 (768) and 5. The 'Renegotiate after' time is 0 hrs, 20 mins, and 0 secs. The 'Advanced' section includes 'Stop IKE negotiation if no packet received for' set to 30 seconds. Several checkboxes are checked: 'Enable NAT-Traversal', 'Send INITIAL-CONTACT notifications', and 'Send RESPONDER-LIFETIME notifications'. 'Retain phase 1 SA after failed phase 2 negotiation' is unchecked. The 'RSA private key file' is set to 'privdem1.pem'. 'SA Removal Mode' is set to 'Normal'. The 'Delete SAs when invalid SPI notifications are received' checkbox is unchecked. An 'Apply' button is at the bottom.

| Parameter             | Setting      | Description                            |
|-----------------------|--------------|----------------------------------------|
| RSA private key file: | privdem1.pem | Enter the name of the private key file |

Browse to : **Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Debug**



| Parameter        | Setting   | Description                                        |
|------------------|-----------|----------------------------------------------------|
| Enable IKE Debug | Tick      | Allow debug of IKE                                 |
| Debug level:     | Very High | Set the maximum debug level for the analyser trace |

## 6.2 Configure IPSEC

The IPSEC itself is configured in the eroutes (encrypted routes). The eroutes define the characteristics of the encrypted routes i.e. local and remote subnets, authentication and encryption methods etc.

Browse to

**Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0**



Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0

▼ IPsec 0

Description:

The IP address or hostname of the remote unit

Use  as a backup unit

| Local LAN                                                                                                                                                                                                                                                                             | Remote LAN                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="radio"/> Use these settings for the local LAN<br>IP Address: <input type="text" value="172.16.0.0"/><br>Mask: <input type="text" value="255.255.0.0"/><br><input type="radio"/> Use interface <input type="text" value="PPP"/> <input type="text" value="0"/> | <input checked="" type="radio"/> Use these settings for the remote LAN<br>IP Address: <input type="text" value="192.168.0.0"/><br>Mask: <input type="text" value="255.255.255.0"/><br><input type="radio"/> Remote Subnet ID: <input type="text"/> |

Use the following security on this tunnel

☐ Off
 ☐ Preshared Keys
 ☐ XAUTH Init Preshared Keys
 ☒ RSA Signatures
 ☐ XAUTH Init RSA

RSA Key File:

Our ID:

Our ID type: ☒ IKE ID ☐ FQDN ☐ User FQDN ☐ IPv4 Address

Remote ID:

Use  encryption on this tunnel

Use  authentication on this tunnel

Use Diffie Hellman group

Use IKE  to negotiate this tunnel

Use IKE configuration:

Bring this tunnel up

☐ All the time  
☐ Whenever a route to the destination is available  
☒ On demand

If the tunnel is down and a packet is ready to be sent

Bring this tunnel down if it is idle for  hrs  mins  secs

Renew the tunnel after

hrs  mins  secs  
 KBytes of traffic

| Parameter                     | Setting        | Description                                         |
|-------------------------------|----------------|-----------------------------------------------------|
| Peer ID:                      | WR44           | Common name specified in the peer's public key *    |
| Our ID:                       | DR6000         | Common name specified in our public key *           |
| Local subnet IP address:      | 172.16.0.0     | Enter the local subnet IP address                   |
| Local subnet mask:            | 255.255.0.0    | Enter the local subnet mask                         |
| Remote subnet IP address:     | 192.168.0.0    | Enter the remote subnet IP address                  |
| Remote subnet mask:           | 255.255.255.0  | Enter the remote subnet mask                        |
| ESP authentication algorithm: | MD5            | Select MD5 as the authentication algorithm **       |
| ESP encryption algorithm:     | AES            | Select AES as the encryption algorithm **           |
| Duration (s):                 | 1200           | Enter 1200 seconds for the IPSEC lifetime           |
| Authentication method:        | RSA Signatures | Select RSA signatures for the authentication method |

\* If you wish to check the common name used in the public key you can view the contents of the public key as follows;

Browse to **CONFIGURATION → SECURITY → CERTIFICATES → SCEP**

In the **Certificate filename** drop-down list select the public key certificate (certdem1.pem in this case) and click **view**. You will then be able to view the certificate and see the entry in the **common name** field.

\*\* The **authentication** and **encryption** algorithms must match exactly the settings in the peer IPSEC router.

## 7 CONFIGURE IKE AND IPSEC – VPN CLIENT

### 7.1 Configure IKE (Internet Key Exchange)

IKE is the first stage in establishing a secure link between two endpoints. The VPN client will act as the IKE ‘initiator’ and as such will make first contact with the VPN responder. This is because the 3G/GPRS device is issued with a dynamic IP address from the provider which will change over time. This therefore makes it impossible for the VPN responder to know the clients IP address unless the client initiates the VPN connection. The client’s current IP address will be included each time IKE is negotiated.

Browse to

**Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0**

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0

**▼ IKE 0**

Use the following settings for negotiation

Encryption: ☐ None ☐ DES ☒ 3DES ☐ AES (128 bit) ☐ AES (192 bit) ☐ AES (256 bit)

Authentication: ☐ None ☐ MD5 ☒ SHA1

Mode: ☒ Main ☐ Aggressive

MODP Group for Phase 1: 1 (768)

MODP Group for Phase 2: No PFS

Renegotiate after 8 hrs 0 mins 0 secs

**▼ Advanced**

Retransmit a frame if no response after 10 seconds

Stop IKE negotiation after 2 retransmissions

Stop IKE negotiation if no packet received for 30 seconds

☒ Enable Dead Peer Detection

☒ Enable NAT-Traversal

☒ Send INITIAL-CONTACT notifications

☐ Retain phase 1 SA after failed phase 2 negotiation

RSA private key file: privdem2.pem

SA Removal Mode: Normal

☐ Delete SAs when invalid SPI notifications are received

Apply

| Parameter                 | Setting | Description                                    |
|---------------------------|---------|------------------------------------------------|
| Encryption algorithm:     | 3DES    | Select 3DES for the IKE encryption algorithm * |
| Authentication algorithm: | SHA1    | Select SHA1 for the IKE Authentication         |

|                        |              |                                            |
|------------------------|--------------|--------------------------------------------|
|                        |              | algorithm *                                |
| Duration (s):          | 1200         | Enter 1200 seconds for the IKE lifetime ** |
| RSA private key file:  | privdem2.pem | Enter the name of the private key file     |
| NAT traversal enabled: | YES          | Enable NAT traversal                       |

\* The encryption/authentication algorithms must be within the threshold set by the VPN responder.

\*\* It is advisable to set the IKE duration set to the same or lesser value to that of the VPN Responder.

Browse to : **Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Debug**

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Debug

▼ IKE Debug

☒ Enable IKE Debug

Debug Level: Very

Debug IP Address Filter:

☐ Forward debug to port

Apply

| Parameter        | Setting   | Description                                        |
|------------------|-----------|----------------------------------------------------|
| Enable IKE Debug | Tick      | Allow debug of IKE                                 |
| Debug level:     | Very High | Set the maximum debug level for the analyser trace |

## 7.2 Configure IPSEC

Browse to **CONFIGURATION → VPN → IPSEC → IPSEC EROUTES → EROUTE 0 - 9 → EROUTE 0**.

**Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0**

**IPsec 0**

Description: Initiator

The IP address or hostname of the remote unit 213.152.58.85

Use as a backup unit

| Local LAN                                                             | Remote LAN                                                             |
|-----------------------------------------------------------------------|------------------------------------------------------------------------|
| <input checked="" type="radio"/> Use these settings for the local LAN | <input checked="" type="radio"/> Use these settings for the remote LAN |
| IP Address: 192.168.0.0                                               | IP Address: 172.16.0.0                                                 |
| Mask: 255.255.255.0                                                   | Mask: 255.255.0.0                                                      |
| <input type="radio"/> Use interface PPP 0                             | <input type="radio"/> Remote Subnet ID:                                |

Use the following security on this tunnel

☐ Off ☐ Preshared Keys ☐ XAUTH Init Preshared Keys ☒ RSA Signatures ☐ XAUTH Init RSA

RSA Key File: --edit--

Our ID: WR44

Our ID type ☒ IKE ID ☐ FQDN ☐ User FQDN ☐ IPv4 Address

Remote ID: DR6400

Use AES (128 bit keys) encryption on this tunnel

Use MD5 authentication on this tunnel

Use Diffie Hellman group No PFS

Use IKE v1 to negotiate this tunnel

Use IKE configuration: 0

Bring this tunnel up

☒ All the time

☐ Whenever a route to the destination is available

☐ On demand

If the tunnel is down and a packet is ready to be sent bring the tunnel up

Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs

Renew the tunnel after

8 hrs 20 mins 0 secs

0 KBytes of traffic

| Parameter                     | Setting        | Description                                                  |
|-------------------------------|----------------|--------------------------------------------------------------|
| Peer IP/Hostname:             | 213.152.58.85  | Enter the WAN IP address of <u>your</u> VPN responder router |
| Peer ID:                      | DR6400         | Common name specified in the peer's public key *             |
| Our ID:                       | WR44           | Common name specified in our public key *                    |
| Local subnet IP address:      | 192.168.0.0    | Enter the local subnet IP address                            |
| Local subnet mask:            | 255.255.255.0  | Enter the local subnet mask                                  |
| Remote subnet IP address:     | 172.16.0.0     | Enter the remote subnet IP address                           |
| Remote subnet mask:           | 255.255.0.0    | Enter the remote subnet mask                                 |
| ESP authentication algorithm: | MD5            | Select MD5 as the authentication algorithm **                |
| ESP encryption algorithm:     | AES            | Select AES as the encryption algorithm **                    |
| Duration (s):                 | 1200           | Enter 1200 seconds for the IPSEC lifetime                    |
| No SA action                  | Use IKE        | If no SA action then Use IKE                                 |
| Create SA's automatically     | Yes            | Create Security Associations automatically                   |
| Authentication method:        | RSA Signatures | Select RSA signatures for the authentication method          |

\* If you wish to check the common name used in the public key you can view the contents of the public key as follows:

Browse to CONFIGURE → CERTIFICATES → SCEP

In the **Certificate filename** drop-down list select the public key certificate (certdem2.pem in this case) and click **view**. You will then be able to view the certificate and see the entry in the **common name** field.

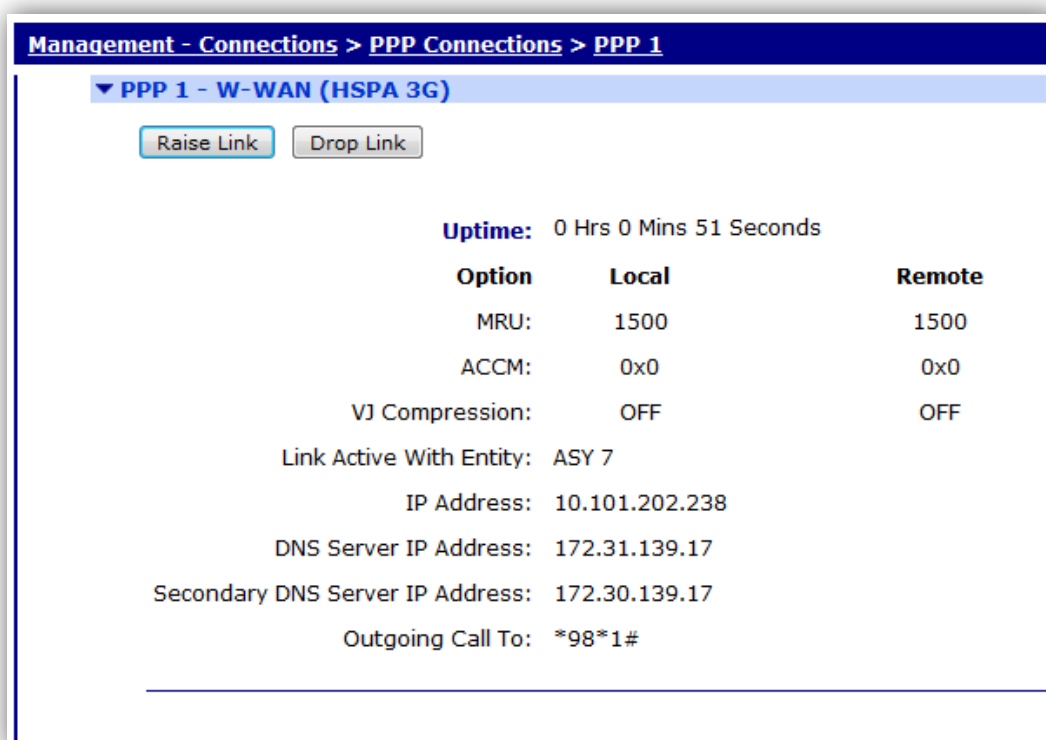
\*\* The **authentication** and **encryption** algorithms must be within the threshold set by the VPN responder

## 8 TESTING

### 8.1 Check the WAN Link is Active

When browsing the TransPort's web interface you can view the status of any interface. The following screen shot shows the status of the WR44 Wireless WAN interface. The presence of an IP address in the **IP Address** field shows the ADSL link is up.

Browse to **Management - Connections > PPP Connections > PPP 1**



**NB:** The default PPP instance for the WAN interface may differ depending on the type of router.

### 8.2 Check the IPSEC Tunnel is Active

#### 8.2.1 IPSEC PEERS

The IPsec Peers shows the WAN address of all the VPN Clients/Hosts that are currently in session.

Browse to STATUS → IPSEC → IPSEC PEERS



| Diagnostics - Status > IPsec > IPsec Peers |        |         |                               |                 |                  |
|--------------------------------------------|--------|---------|-------------------------------|-----------------|------------------|
| IPSec Peers                                |        |         |                               |                 |                  |
| Peer IP                                    | Our ID | Peer ID | DPD                           | NATT local port | NATT remote port |
| 213.152.85.8                               | WR44   | DR6000  | Inactive. Next REQ in 30 secs | 4500            | 4500             |
| Remove all unused                          |        |         |                               |                 |                  |

## 8.2.2 IKE SA's

The IKE SA's status page shows the current active IKE security associations.

Browse to STATUS → IPSEC → IKE SA's

| Diagnostics - Status > IPsec > IKE SAs |         |              |               |            |           |             |        |
|----------------------------------------|---------|--------------|---------------|------------|-----------|-------------|--------|
| IKE Status                             |         |              |               |            |           |             |        |
| V1 SAs                                 |         |              |               |            |           |             |        |
| Our ID                                 | Peer ID | Peer IP      | Our IP        | Session ID | Time Left | Internal ID |        |
| WR44                                   | DR6000  | 213.152.85.8 | 10.47.137.109 | 0x0        | 338       | 70          | Remove |
| Remove All V1 SAs                      |         |              |               |            |           |             |        |

## 8.2.3 IPSEC SA's

The IPsec SA's status page shows the current active IPSEC security associations. Each IPSEC VPN tunnel has IPSEC security associations for both inbound and outbound traffic.

Browse to STATUS → IPSEC → IPSEC SA's

| Diagnostics - Status > IPsec > IPsec SAs |       |               |               |                |     |          |          |        |                  |             |           |           |        |
|------------------------------------------|-------|---------------|---------------|----------------|-----|----------|----------|--------|------------------|-------------|-----------|-----------|--------|
| IPSec Status: Routes 0 -> 4              |       |               |               |                |     |          |          |        |                  |             |           |           |        |
| Outbound V1 SAs                          |       |               |               |                |     |          |          |        |                  |             |           |           |        |
| SPI                                      | Route | Peer IP       | Rem. selector | Loc. selector  | AH  | ESP Auth | ESP Enc  | IPCOMP | KBytes Delivered | KBytes Left | Time Left | Interface |        |
| ea640a4b                                 | 0     | 213.152.58.85 | 172.16.0.0/16 | 192.168.0.0/24 | N/A | MD5      | AES(128) | N/A    | 0                | 0           | 903       | PPP 1     | Remove |
| Remove All                               |       |               |               |                |     |          |          |        |                  |             |           |           |        |
| Inbound V1 SAs                           |       |               |               |                |     |          |          |        |                  |             |           |           |        |
| SPI                                      | Route | Peer IP       | Rem. selector | Loc. selector  | AH  | ESP Auth | ESP Enc  | IPCOMP | KBytes Delivered | KBytes Left | Time Left | Interface |        |
| e35e651a                                 | 0     | 213.152.58.85 | 172.16.0.0/16 | 192.168.0.0/24 | N/A | MD5      | AES(128) | N/A    | 0                | 0           | 903       | PPP 1     | Remove |
| Remove All                               |       |               |               |                |     |          |          |        |                  |             |           |           |        |
| Outbound V2 SAs                          |       |               |               |                |     |          |          |        |                  |             |           |           |        |
| List Empty                               |       |               |               |                |     |          |          |        |                  |             |           |           |        |
| Inbound V2 SAs                           |       |               |               |                |     |          |          |        |                  |             |           |           |        |
| List Empty                               |       |               |               |                |     |          |          |        |                  |             |           |           |        |

## 8.2.4 Eventlog

You can also check the eventlog to see if the VPN tunnel establishes

Browse to **DIAGNOSTICS → EVENTLOG**.

```
15:59:16, 04 Jan 2010,Eroute 0 VPN up peer: DR6000
15:59:16, 04 Jan 2010,New IPsec SA created by DR6000
15:59:15, 04 Jan 2010,(2) IKE Notification: Initial Contact,RX
15:59:15, 04 Jan 2010,Event delay,Logger busy
15:59:15, 04 Jan 2010,(3) IKE Notification: Responder Lifetime,RX
15:59:15, 04 Jan 2010,(2) New Phase 2 IKE Session 213.152.58.85,Initiator
15:59:15, 04 Jan 2010,(1) IKE Keys Negotiated. Peer:
15:59:14, 04 Jan 2010,(1) New Phase 1 IKE Session 213.152.58.85,Initiator
15:59:14, 04 Jan 2010,IKE Request Received From Eroute 0
15:59:14, 04 Jan 2010,Default Route 0 Available,Activation
```

## 8.3 Test the IPSEC Routing

When an IP packet is received by a VPN Responder/Client TransPort it must meet certain criteria for it to be passed through the VPN tunnel. I.e. the source and destination IP address **MUST** match that of one of the configured eroutes and IPSEC SA's.

In brief, the VPN tunnel in this application note will pass data from network on subnet **192.168.0.0/24** to network on subnet **172.16.0.0/16** and vice versa (see diagram on page 3).

Using the TransPort's analyser trace we will see evidence of data being routed through the IPSEC VPN Tunnel. In this example **computer A** (192.168.0.10) will ping **Server B** (172.16.0.10).

**NOTE:** The WR44 3G Router has been issued with a private (NAT'ed) IP address (10.16.33.234) from the wireless network as is usually the case in the UK. Hence **NAT Traversal** is being used.

To view the analyser trace browse to **DIAGNOSTICS → ANALYSER → ANALYSER TRACE**.

Items of particular interest have been highlighted in **red** in the decoded IP packets.

The WR44 VPN Client receives a PING (echo request) on interface Ethernet 0 from **computer A** (192.168.0.10), which is to be routed over the VPN tunnel to **Server B** (172.16.0.10).

```
----- 27-10-2005 11:36:19.810 -----
 45 00 00 3C 9C 67 00 00 80 01 31 8D C0 A8 00 0A    E...æg...€.1•.``..
AC 10 00 0A 08 00 41 5C 02 00 0A 00 61 62 63 64    .....A.....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74    efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69              uvwabcdeghi

IP (In) From REM TO LOC      IFACE: ETH 0
```

```

45          IP Ver:      4
          Hdr Len:      20
00          TOS:        Routine
          Delay:        Normal
          Throughput:    Normal
          Reliability:   Normal
00 3C       Length:      60
9C 67       ID:          40039
00 00       Frag Offset: 0
          Congestion:    Normal
          May Fragment
          Last Fragment

80          TTL:        128
01          Proto:      ICMP
31 8D       Checksum:    12685
C0 A8 00 0A Src IP:      192.168.0.10
AC 10 00 0A Dst IP:      172.16.0.10
ICMP:
08          Type:        ECHO REQ
00          Code:        0
41 5C       Checksum:    16732
-----

```

The PING is passed to the **PPP 1** interface for routing over the wireless network.

```

----- 27-10-2005 11:36:19.810 -----
45 00 00 3C 9C 67 00 00 7F 01 32 8D C0 A8 00 0A   E...æg....2•.``..
AC 10 00 0A 08 00 41 5C 02 00 0A 00 61 62 63 64   .....A.....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74   efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69              uvwabcdefghi

```

```

ER 0 From LOC TO REM          IFACE: PPP 1
45          IP Ver:      4
          Hdr Len:      20
00          TOS:        Routine
          Delay:        Normal
          Throughput:    Normal
          Reliability:   Normal
00 3C       Length:      60
9C 67       ID:          40039

```

```

00 00      Frag Offset:    0
           Congestion:    Normal
                               May Fragment
                               Last Fragment
7F         TTL:           127
01         Proto:         ICMP
32 8D      Checksum:      12941
C0 A8 00 0A Src IP:       192.168.0.10
AC 10 00 0A Dst IP:       172.16.0.10
ICMP:
08         Type:          ECHO REQ
00         Code:          0
41 5C      Checksum:      16732
-----

```

The PING is then encapsulated in a UDP IKE FLOAT (NAT-Traversal) Packet.

Note: the source IP addresses of the NAT-Traversal packet is that of the WAN interface of VPN Client (10.16.33.234) and the destination IP address is that of the WAN Interface of the VPN Responder (213.152.85.8).

```

----- 27-10-2005 11:36:19.820 -----
45 00 00 80 00 0E 00 00 FA 11 84 77 0A 10 21 EA    E..€.....w....
D5 98 3A 55 11 94 11 94 00 6C 00 00 B1 40 BB 91    ...U."."."l....»‘
00 00 00 0E 25 5E 10 DD B5 4E D7 EC 95 23 D9 10    .....ÝµN.ì....
64 BB 73 7F 94 89 CF 63 2F 0C D1 00 FE 04 A7 BB    d»s."."İc..Ń....»
F0 35 66 D5 54 FC 71 C7 C7 2F FE B8 05 E5 F4 49    .5f.T.qÇÇ...,.å.I
F0 E2 76 80 40 D6 D3 DD 30 DC AF 23 1A 6B 74 F0    .âv€..ÓÝÜü...kt.
0C C9 70 73 99 62 B4 7C 46 35 E1 06 3C 8E E6 1E    .Éps.b´.F5...Žæ.
44 A6 8D 0A D4 DF 09 B4 64 6C F6 AF 3F 42 61 58    D.♦ ....´dl...BaX

```

```

IP (Final) From LOC TO REM    IFACE: PPP 1
45         IP Ver:          4
           Hdr Len:        20
00         TOS:             Routine
           Delay:           Normal
           Throughput:      Normal
           Reliability:      Normal
00 80      Length:          128
00 0E      ID:              14
00 00      Frag Offset:     0
           Congestion:      Normal

```

```

May Fragment
Last Fragment
FA          TTL:          250
11          Proto:        UDP
84 77       Checksum:     33911
0A 10 21 EA Src IP:       10.16.33.234
D5 98 3A 55 Dst IP:       213.152.85.8
UDP:
11 94       SRC Port:     IKE FLOAT (4500)
11 94       DST Port:     IKE FLOAT (4500)
00 6C       Length:       108
00 00       Checksum:     0

```

-----  
The WR44 VPN Client receives a NAT-Traversal packet on interface PPP 1 from the DR6410 MKII VPN Responder (213.152.85.8).

```

----- 27-10-2005 11:36:20.430 -----
45 00 00 80 00 0D 00 00 E8 11 96 78 D5 98 3A 55   E..€.....-x...U
0A 10 21 EA 11 94 11 94 00 6C 00 00 03 F4 6E 4E   .....".".l....nN
00 00 00 0D BC F0 60 0A 6E 80 0F 7E 67 ED 69 DA   ....¼....n€..g.i.
4A 1D B4 87 15 3A A4 E8 EB 4F 09 FE C7 41 54 99   J.´...¸...O..ÇAT.
9B B3 CC 1F 49 98 CD 31 72 D7 DF E1 D7 33 D3 E6   .³İ.I.İ1r....3Óæ
71 72 03 A6 E0 32 C4 AD 1B 68 13 AF 43 2B 8B DC   qr..à2Ä..h..C.<Ü
E3 1C 7F CD 4C 13 70 FD 6A E9 BE A0 F6 F7 A3 3B   ...ÍL.p.j.¾ .÷f.
F2 38 03 FA F2 C7 01 B9 58 3A 78 D2 0D 93 4C 17   .8...Ç.¹X.xØ.“L.

```

```

IP (In) From REM TO LOC      IFACE: PPP 1
45          IP Ver:          4
          Hdr Len:          20
00          TOS:             Routine
          Delay:             Normal
          Throughput:        Normal
          Reliability:        Normal
00 80       Length:          128
00 0D       ID:              13
00 00       Frag Offset:     0
          Congestion:        Normal
          May Fragment
          Last Fragment
E8          TTL:             232
11          Proto:           UDP

```

```

96 78          Checksum:      38520
D5 98 3A 55    Src IP:        213.152.85.8
0A 10 21 EA    Dst IP:        10.16.33.234
UDP:
11 94          SRC Port:      IKE FLOAT (4500)
11 94          DST Port:      IKE FLOAT (4500)
00 6C          Length:        108
00 00          Checksum:      0

```

The WR44 VPN Client un-packs the encrypted (ESP) packet from the NAT-Traversal packet.

```

----- 27-10-2005 11:36:20.430 -----
45 00 00 78 00 0D 00 00 E8 32 96 5F D5 98 3A 55    E..x.....2-....U
0A 10 21 EA 03 F4 6E 4E 00 00 00 0D BC F0 60 0A    .....nN....¼...
6E 80 0F 7E 67 ED 69 DA 4A 1D B4 87 15 3A A4 E8    n€..g.i.J.´...¸.
EB 4F 09 FE C7 41 54 99 9B B3 CC 1F 49 98 CD 31    .O..ÇAT..³İ.I.İ1
72 D7 DF E1 D7 33 D3 E6 71 72 03 A6 E0 32 C4 AD    r....3Óæqr..à2Ä.
1B 68 13 AF 43 2B 8B DC E3 1C 7F CD 4C 13 70 FD    .h..C.<Ü...İL.p.
6A E9 BE A0 F6 F7 A3 3B F2 38 03 FA F2 C7 01 B9    j.¼ .÷f..8...Ç.¹
58 3A 78 D2 0D 93 4C 17                          X.xò.“L.

```

```

IP (In) From REM TO LOC      IFACE: PPP 1
45          IP Ver:          4
          Hdr Len:          20
00          TOS:             Routine
          Delay:             Normal
          Throughput:        Normal
          Reliability:       Normal
00 78        Length:         120
00 0D        ID:             13
00 00        Frag Offset:    0
          Congestion:        Normal
          May Fragment
          Last Fragment
E8          TTL:             232
32          Proto:           ESP
96 5F        Checksum:       38495
D5 98 3A 55    Src IP:        213.152.85.8
0A 10 21 EA    Dst IP:        10.16.33.234

```

-----

The Encrypted PING REPLY (Echo reply) is de-crypted.

NOTE: The source IP address is that of **Server B (172.16.0.10)** and the destination IP address is that of **Computer A (192.168.0.10)**.

```

----- 27-10-2005 11:36:20.440 -----
45 00 00 3C 02 B0 00 00 7F 01 CC 44 AC 10 00 0A   E....°....İD....
C0 A8 00 0A 00 00 49 5C 02 00 0A 00 61 62 63 64   .".....I.....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74   efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69               uvwabcdefghi

```

```

IP (Cont) From REM TO LOC      IFACE: PPP 1
45                               IP Ver:      4
                               Hdr Len:      20
00                               TOS:          Routine
                               Delay:         Normal
                               Throughput:     Normal
                               Reliability:     Normal
00 3C                           Length:        60
02 B0                           ID:            688
00 00                           Frag offset:   0
                               Congestion:     Normal
                               May Fragment
                               Last Fragment
7F                               TTL:          127
01                               Proto:         ICMP
CC 44                           Checksum:      52292
AC 10 00 0A                     Src IP:        172.16.0.10
C0 A8 00 0A                     Dst IP:        192.168.0.10
ICMP:
00                               Type:         ECHO REPLY
00                               Code:          0
49 5C                           Checksum:     18780

```

The PING REPLY is routed out of interface Ethernet 0 to **Computer A (192.168.0.10)**.

```

----- 27-10-2005 11:36:20.440 -----
45 00 00 3C 02 B0 00 00 7E 01 CD 44 AC 10 00 0A   E....°....İD....
C0 A8 00 0A 00 00 49 5C 02 00 0A 00 61 62 63 64   .".....I.....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74   efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69               uvwabcdefghi

```

```

IP (Final) From LOC TO REM      IFACE: ETH 0

```

|             |              |               |
|-------------|--------------|---------------|
| 45          | IP Ver:      | 4             |
|             | Hdr Len:     | 20            |
| 00          | TOS:         | Routine       |
|             | Delay:       | Normal        |
|             | Throughput:  | Normal        |
|             | Reliability: | Normal        |
| 00 3C       | Length:      | 60            |
| 02 B0       | ID:          | 688           |
| 00 00       | Frag Offset: | 0             |
|             | Congestion:  | Normal        |
|             |              | May Fragment  |
|             |              | Last Fragment |
| 7E          | TTL:         | 126           |
| 01          | Proto:       | ICMP          |
| CD 44       | Checksum:    | 52548         |
| AC 10 00 0A | Src IP:      | 172.16.0.10   |
| C0 A8 00 0A | Dst IP:      | 192.168.0.10  |
| ICMP:       |              |               |
| 00          | Type:        | ECHO REPLY    |
| 00          | Code:        | 0             |
| 49 5C       | Checksum:    | 18780         |
| -----       |              |               |



## 9 CONFIGURATION FILES

### 9.1 Digi Transport Configuration Files

This is the configuration file from the VPN Responder (DR6410 MkII) used in this application note.

```
eth 0 IPaddr "172.16.0.254"
eth 0 mask "255.255.0.0"
eth 0 bridge ON
eth 0 ipanon ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 3 asyport 7
lapb 3 mux_0710 ON
lapb 4 dtemode 0
lapb 4 dlc 1
lapb 4 asyport 7
lapb 4 virt_async "mux0"
lapb 4 mux_0710 ON
lapb 5 dtemode 0
lapb 5 dlc 2
lapb 5 asyport 7
lapb 5 virt_async "mux1"
lapb 5 mux_0710 ON
lapb 6 dtemode 0
lapb 6 dlc 3
lapb 6 asyport 7
lapb 6 virt_async "mux2"
lapb 6 mux_0710 ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
def_route 1 ll_ent "PPP"
def_route 1 ll_add 3
def_route 2 ll_ent "PPP"
def_route 2 ll_add 2
eroute 0 peerid "WR44"
eroute 0 ourid "DR6000"
eroute 0 locip "172.16.0.0"
eroute 0 locmsk "255.255.0.0"
eroute 0 remip "192.168.0.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "MD5"
eroute 0 ESPenc "AES"
eroute 0 lkbytes 0
eroute 0 authmeth "RSA"
dhcp 0 IPmin "172.16.0.1"
dhcp 0 mask "255.255.0.0"
dhcp 0 gateway "172.16.0.254"
dhcp 0 DNS "172.16.0.254"
dhcp 0 wifionly ON
ppp 0 timeout 300
ppp 1 IPaddr "0.0.0.0"
ppp 1 username "Enter ADSL Username"
ppp 1 timeout 0
```

```

ppp 1 aodion 1
ppp 1 immoos ON
ppp 1 autoassert 1
ppp 1 ipsec 2
ppp 1 echo 10
ppp 1 echodropcnt 5
ppp 1 l1iface "AAL"
ppp 2 l_pap OFF
ppp 2 l_chap OFF
ppp 2 l_addr ON
ppp 2 r_pap ON
ppp 2 r_chap ON
ppp 2 r_addr OFF
ppp 2 IPaddr "1.2.3.5"
ppp 2 username "Enter ISDN Username"
ppp 3 l_pap OFF
ppp 3 l_chap OFF
ppp 3 l_addr ON
ppp 3 r_chap OFF
ppp 3 r_addr OFF
ppp 3 IPaddr "0.0.0.0"
ppp 3 username "ENTER WWAN Username"
ppp 3 epassword "KD51SVJDVVg="
ppp 3 phonenum "*98*1#"
ppp 3 timeout 0
ppp 3 use_modem 1
ppp 3 aodion 1
ppp 3 immoos ON
ppp 3 autoassert 1
ppp 3 defpak 16
ppp 4 defpak 16
ike 0 privrsakey "privdem1.pem"
ike 0 deblevel 3
modemcc 0 asy_add "mux1"
modemcc 0 info_asy_add "mux2"
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "Your.APN.Goes.Here"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 init_str_2 "+CGQREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "Your.APN.Goes.Here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_interval_2 1
modemcc 1 asy_add "mux0"
modemcc 1 link_retries 10
ana 0 anon ON
ana 0 l1on ON
ana 0 lapdon 0
ana 0 ipaddfilt "~10.1.253.251"
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"

```

```

cmd 0 hostname "sarian.router"
cmd 0 tremto 1200
cmd 0 web_suffix ".wb2"
user 1 name "username"
user 1 epassword "KD51SVJDVVg="
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 access 0
local 0 transaccess 2
sslsrv 0 certfile "cert01.pem"
sslsrv 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
creq 0 challenge_pwd "8B35FC8225557E58"
creq 0 country "UK"
creq 0 commonname "DR6000"
creq 0 locality "Leeds"
creq 0 orgname "Digi International"
creq 0 org_unit "Tech Support"
creq 0 state "Yorkshire"
creq 0 email "uksupport@digicom"
creq 0 digest "MD5"
scep 0 host "10.1.253.251"
scep 0 path "certsrv/mscep/mscep.dll"
scep 0 caident "ACP"
scep 0 keyfile "privdem1.pem"
scep 0 reqfile "creq.pem"
wifinode 0 enabled OFF
wifinode 0 ssid "digi.router.SN:%s"
wifinode 0 esharedkey "KD51SVJDVVg="

```

This is the configuration file from the VPN Client (WR44) used in this application note.

```

eth 0 IPAddr "192.168.0.254"
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 descr "Initiator"
eroute 0 peerip "213.152.85.8"
eroute 0 peerid "DR6000"
eroute 0 ourid "WR44"
eroute 0 locip "192.168.0.0"

```

```

eroute 0 locmsk "255.255.255.0"
eroute 0 remip "172.16.0.0"
eroute 0 remmsk "255.255.0.0"
eroute 0 ESPauth "MD5"
eroute 0 ESPenc "AES"
eroute 0 lkbytes 0
eroute 0 authmeth "RSA"
eroute 0 nosa "TRY"
eroute 0 autosa 1
dhcp 0 IPmin "192.168.0.1"
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.0.254"
dhcp 0 DNS "192.168.0.254"
dhcp 0 respdelms 500
ppp 0 timeout 300
ppp 1 r_chap OFF
ppp 1 IPaddr "0.0.0.0"
ppp 1 phonenum "*98*1#"
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 ipsec 1
ppp 1 ipanon ON
ppp 3 defpak 16
ppp 4 defpak 16
ike 0 encalg "3DES"
ike 0 authalg "SHA1"
ike 0 privrsakey "privdem2.pem"
ike 0 deblevel 4
modemcc 0 info_asy_add 6
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "internet"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
modemcc 0 init_str_2 "+CGQREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "Your.APN.goes.here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
ana 0 anon ON
ana 0 llon ON
ana 0 lapdon 0
ana 0 asyon 1
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
user 0 access 0
user 1 name "username"

```

```
user 1 epassword "KD51SVJDVVg="
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 access 0
local 0 transaccess 2
sslsrv 0 certfile "cert01.pem"
sslsrv 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
creq 0 challenge_pwd "E7AA437DB0423FA1"
creq 0 country "UK"
creq 0 commonname "WR44"
creq 0 locality "Ilkley"
creq 0 orgname "Digi International"
creq 0 org_unit "Tech Support"
creq 0 state "Yorkshire"
creq 0 email "uksupport@digicom"
creq 0 digest "MD5"
scep 0 host "10.1.253.251"
scep 0 path "certsrv/mscep/mscep.dll"
scep 0 caident "ACP"
scep 0 keyfile "privdem2.pem"
scep 0 reqfile "creq.pem"
scep 0 certfile "certdem2.pem"
scep 0 cafile "ca2.pem"
scep 0 caencfile "ca1.pem"
scep 0 casigfile "ca0.pem"
```

## Digi Transport Versions

This is the firmware \ hardware information from the VPN Responder (DR6410 MKII) used in this application note

```
Digi TransPort DR6410-EIA Mk.II DSL2/2+ Router Ser#:92909 HW Revision: 7502a
Software Build Ver5087. Dec 23 2009 01:23:41 9W
ARM Bios Ver 5.80 v35 197MHz B128-M128-F300-0100000,0 MAC:00042d016aed
Power Up Profile: 0
Async Driver Revision: 1.19 Int clk
Ethernet Port Isolate Driver Revision: 1.11
ISDN ST 21150 Driver Revision: 1.7
Firewall Revision: 1.0
EventEdit Revision: 1.0
Timer Module Revision: 1.1
AAL Revision: 1.0
ADSL Revision: 1.0
(B)USBHOST Revision: 1.0
L2TP Revision: 1.10
PPTP Revision: 1.00
TACPLUS Revision: 1.00
MySQL Revision: 0.01
LAPB Revision: 1.12
LAPD Revision: 1.16
TEI Management Revision: 1.6
BRI Call Control Layer Revision: 1.11
X25 Layer Revision: 1.19
MACRO Revision: 1.0
PAD Revision: 1.4
X25 Switch Revision: 1.7
V120 Revision: 1.16
TPAD Interface Revision: 1.12
SCRIBATSK Revision: 1.0
BASTSK Revision: 1.0
ARM Sync Driver Revision: 1.18
TCP (HASH mode) Revision: 1.14
TCP Utils Revision: 1.13
PPP Revision: 1.19
WEB Revision: 1.5
SMTP Revision: 1.1
FTP Client Revision: 1.5
FTP Revision: 1.4
IKE Revision: 1.0
PollANS Revision: 1.2
PPPOE Revision: 1.0
BRIDGE Revision: 1.1
MODEM CC (Siemens MC75) Revision: 1.4
FLASH Write Revision: 1.2
Command Interpreter Revision: 1.38
SSLCLI Revision: 1.0
OSPF Revision: 1.0
BGP Revision: 1.0
QOS Revision: 1.0
RADIUS Client Revision: 1.0
SSH Server Revision: 1.0
SCP Revision: 1.0
CERT Revision: 1.0
```

|         |               |
|---------|---------------|
| LowPrio | Revision: 1.0 |
| Tunnel  | Revision: 1.2 |
| TEMPLOG | Revision: 1.0 |
| Wifi    | Revision: 2.0 |

This is the firmware \ hardware information from the VPN Client (WR44) used in this application note

```

ati5
Digi TransPort WR44H-XXX-A00 Ser#:127171 HW Revision: 79021
Software Build Ver5087. Dec 23 2009 00:11:28 SW
ARM Bios Ver 5.80 v39 400MHz B512-M512-F80-01,0 MAC:00042d01f0c3
Power Up Profile: 0
Async Driver          Revision: 1.19  Int clk
IX                    Revision: 1.0
Ethernet Hub Driver   Revision: 1.11
Firewall              Revision: 1.0
EventEdit             Revision: 1.0
Timer Module          Revision: 1.1
(B)USBHOST            Revision: 1.0
L2TP                  Revision: 1.10
PPTP                  Revision: 1.00
LAPB                  Revision: 1.12
X25 Layer             Revision: 1.19
MACRO                 Revision: 1.0
PAD                   Revision: 1.4
X25 Switch            Revision: 1.7
V120                  Revision: 1.16
TPAD Interface        Revision: 1.12
GPS                   Revision: 1.0
SCRIBATSK             Revision: 1.0
BASTSK                Revision: 1.0
PYTHON                Revision: 1.0
ARM Sync Driver        Revision: 1.18
TCP (HASH mode)        Revision: 1.14
TCP Utils             Revision: 1.13
PPP                   Revision: 1.19
WEB                   Revision: 1.5
SMTP                  Revision: 1.1
FTP Client             Revision: 1.5
FTP                   Revision: 1.4
IKE                   Revision: 1.0
PollANS               Revision: 1.2
PPPOE                 Revision: 1.0
BRIDGE                Revision: 1.1
MODEM CC (Ericsson 3G) Revision: 1.4
FLASH Write           Revision: 1.2
Command Interpreter    Revision: 1.38
SSLCLI                Revision: 1.0
OSPF                  Revision: 1.0
BGP                   Revision: 1.0
QOS                   Revision: 1.0
SSH Server            Revision: 1.0
SCP                   Revision: 1.0
CERT                  Revision: 1.0
LowPrio               Revision: 1.0

```

|        |               |
|--------|---------------|
| Tunnel | Revision: 1.2 |
| QDL    | Revision: 1.0 |
| Wifi   | Revision: 2.0 |