Quick Note 040

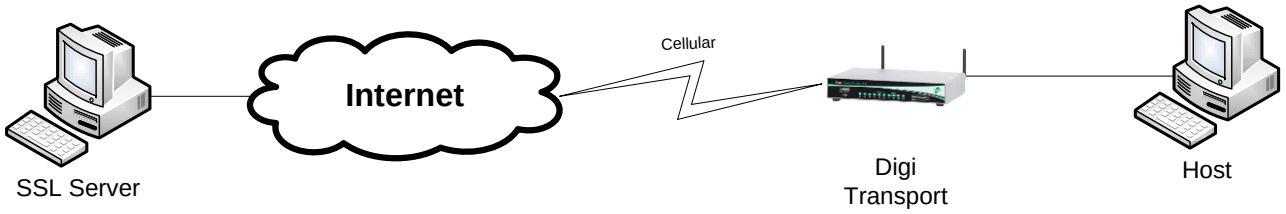
Create an SSL Tunnel with Certificates on a Digi TransPort WR router using Protocol Switch.

November 2016

Contents

1 INTRODUCTION

1.1 Outline



This document describes how to upload SSL certificates and configure a Digi TransPort WR router to create an SSL tunnel to an OpenSSL server with protocol swtich and using the uploaded certificates.

1.2 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. It also assumes a basic ability to access and navigate a Digi TransPort router.

This application note applies only to:

Model: DIGI TransPort WR41/44/21

Digi TransPort WR41 routers must have the “Protocol Switch” option
Digi TransPort WR21 routers must run Enterprise firmware

Firmware versions: 5169 and later

Please note: This application note has been specifically rewritten for firmware release 5169 and later and will not work on earlier versions of firmware. Please contact tech.support@digi.com if your require assistance in upgrading the firmware of the TransPort router.

1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: tech.support@digi.com
Requests for new application notes can be sent to the same address.

2 VERSION

Version Number	Status
1.0	Published
1.1	Rebranding + GUI update

3 CONFIGURATION

If you already have certificates available, you can skip to section 3.2

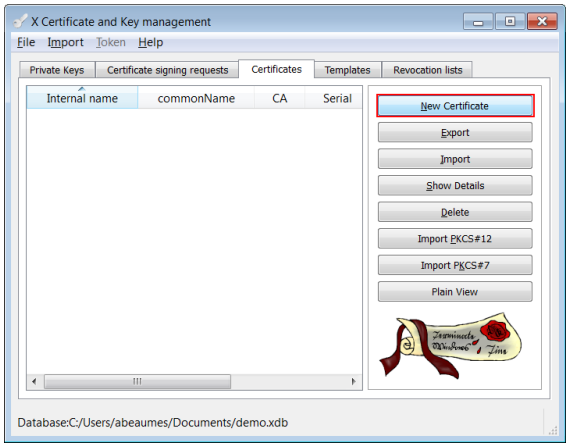
3.1 Generate Test certificates using OpenSSL and XCA

Download and install the latest release of XCA which can be found at: http://sourceforge.net/projects/xca/

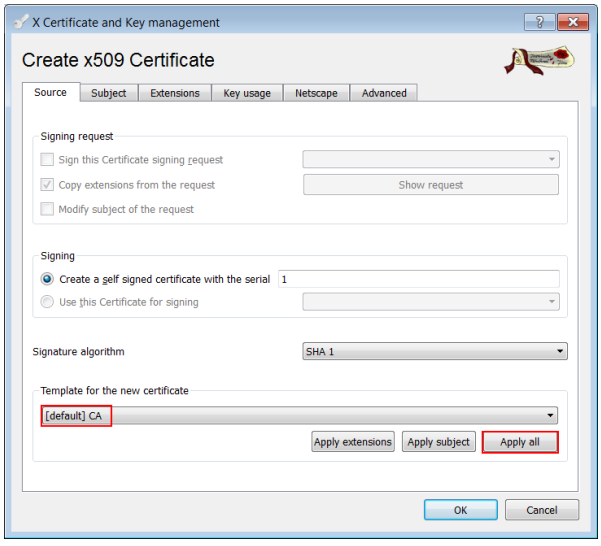
3.1.1 Create a Root CA Certificate

Open the XCA application

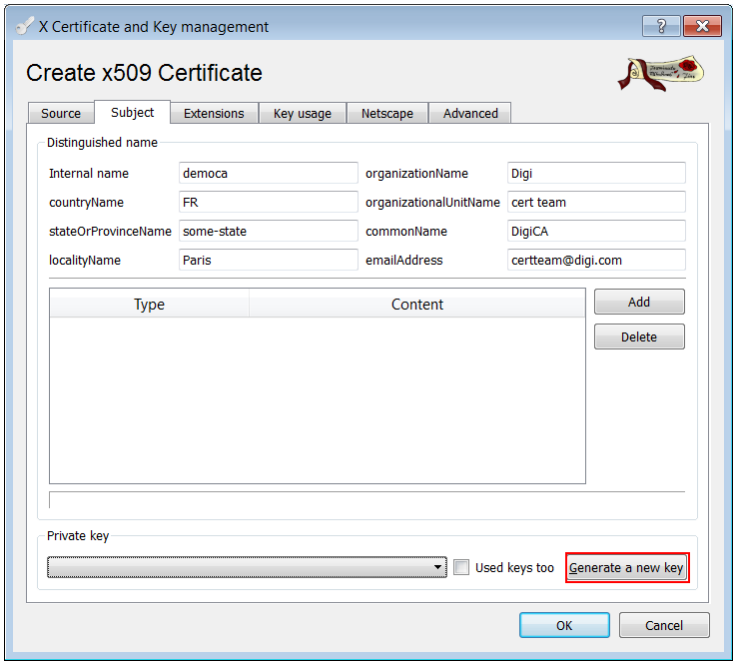
1. Click the **File** menu and select **New Database**, chose a name and click **Save.**
2. Chose a password and click **OK**
3. Click the **Certificates** tab
4. Click the **New Certificate** button



5. Under “Template for the new certificate”, select **default CA** and click **Apply all**

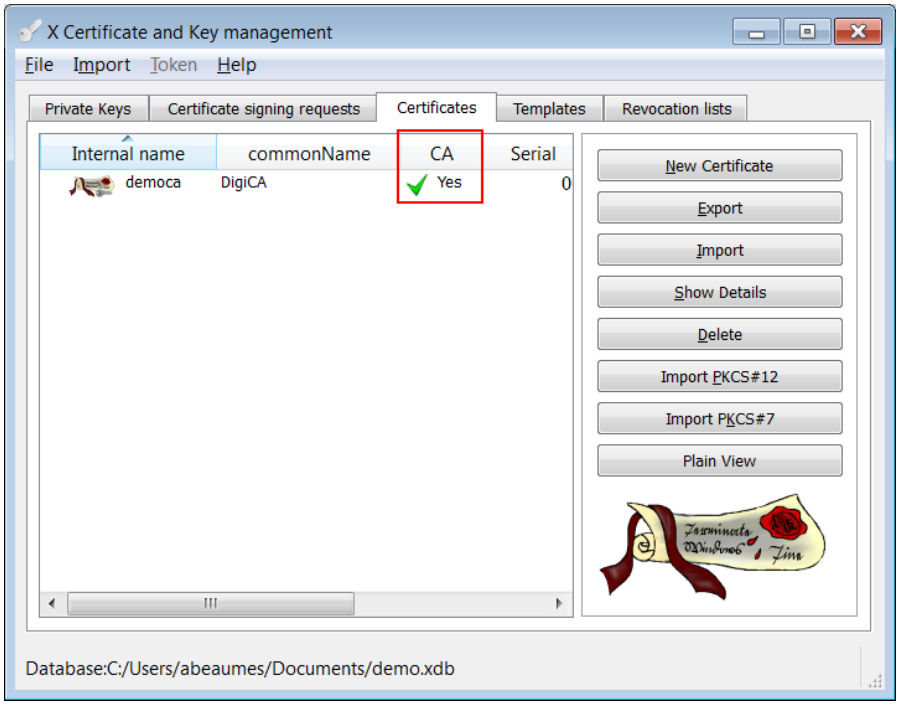


6. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**



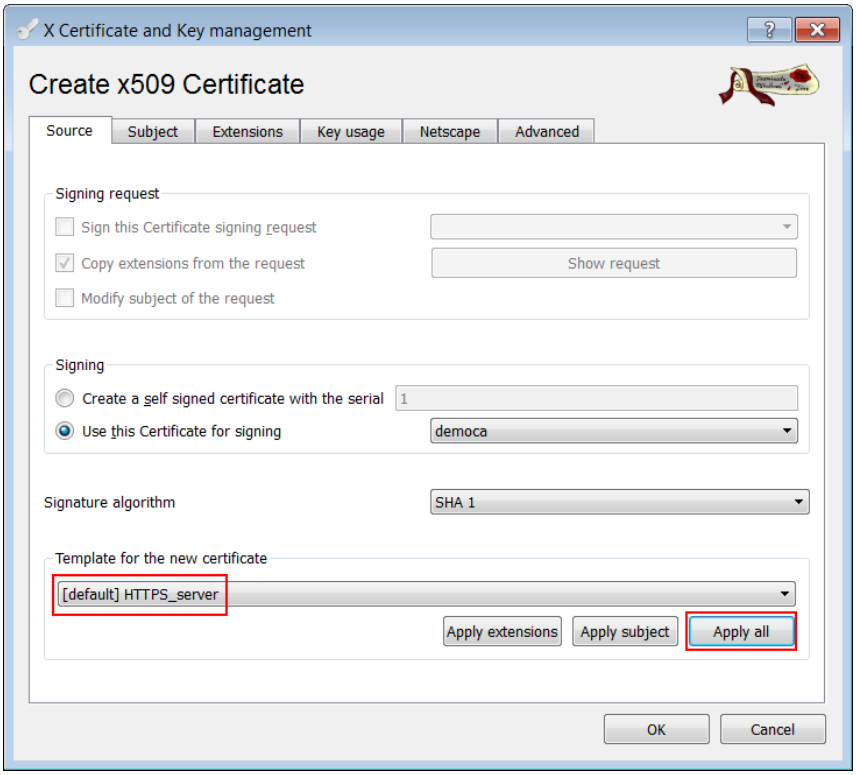
Parameter	Setting
Internal name	This is for display purposes in the tool, only
Country Name	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	The state or province where your organization is legally located. Do not abbreviate. In this example: Some-State
Locality Name	The city where your organization is legally located. Do not abbreviate. In this example: Paris
Organization Name	The exact legal name of your organization. Do not abbreviate your organization name. In this example: Digi
Organizational Unit Name	Section of the organization. Examples of sections are Marketing, Research and Development, Human Resources or Sales.
Common Name	In this example DigiCA will be used.
Email Address	Enter your organization general email address. In this example certteam@digi.com

7. The certificate should now appear in the window with the **CA : YES** confirmation. If it does not say **CA: YES,** verify that you selected CA in the template and clicked Apply All.

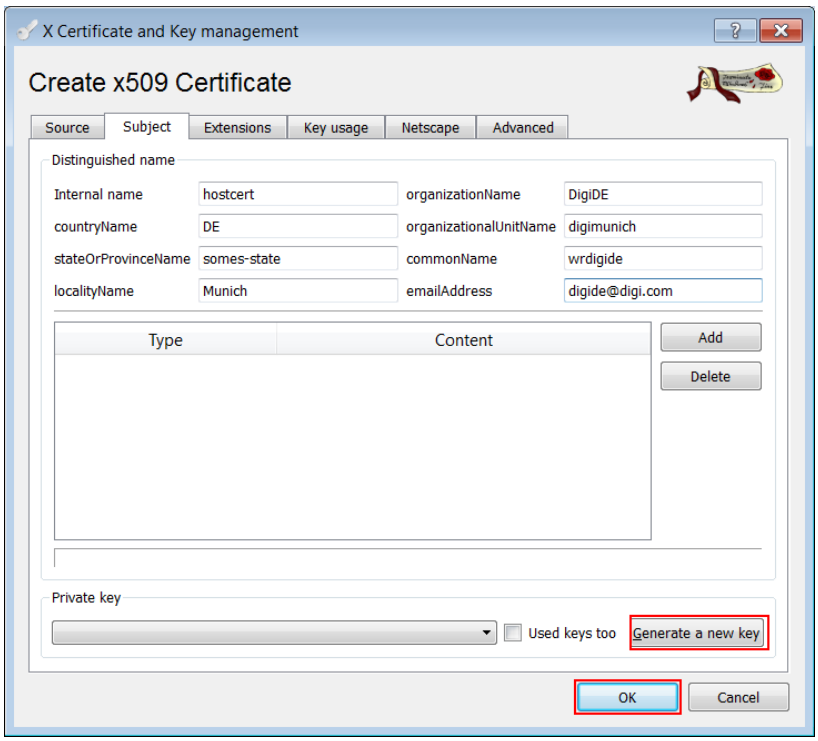


3.1.2 Create a CA-Signed Host Certificate

1. Click the **Certificates** tab
2. Click the **New Certificate** button
3. Under Signing, make sure to select "**Use this Certificate for signing"** and chose the previously created CA.
4. Under "Template for the new certificate", select **default HTTPS_server** and click **Apply all**



5. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**

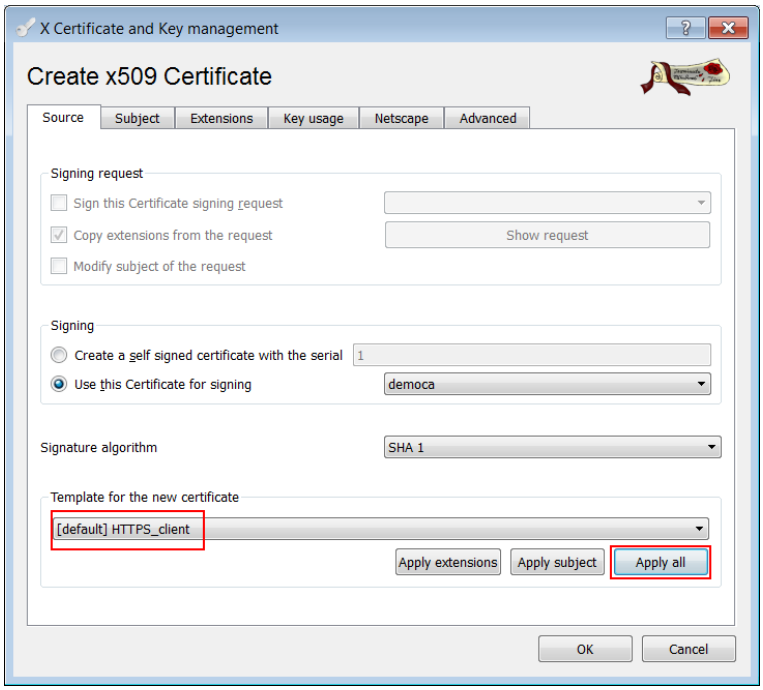


Parameter	Setting
Internal name	This is for display purposes in the tool, only
Country Name	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	The state or province where your organization is legally located. Do not abbreviate. In this example: Some-State
Locality Name	The city where your organization is legally located. Do not abbreviate. In this example: Munich
Organization Name	The exact legal name of your organization. Do not abbreviate your organization name. In this example: DigiDE
Organizational Unit Name	Section of the organization. Examples of sections are Marketing, Research and Development, Human Resources or Sales.
Common Name	In this example **wrdigide** will be used. This will be used as the router Identity for the IPSec tunnel settings
Email Address	Enter your organization general email address. In this example digide@digi.com

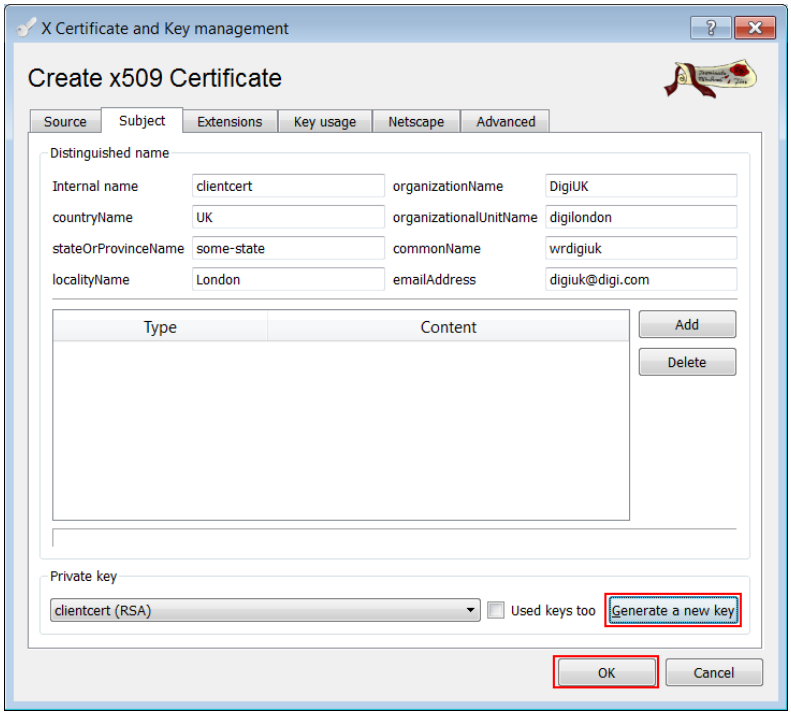
7. The certificate should now appear in the window under the CA certificate.

3.1.3 Create a CA-Signed Client Certificate

1. Click the **Certificates** tab
2. Click the **New Certificate** button
3. Under Signing, make sure to select "**Use this Certificate for signing"** and chose the previously created CA.
4. Under "Template for the new certificate", select **default HTTPS_client** and click **Apply all**

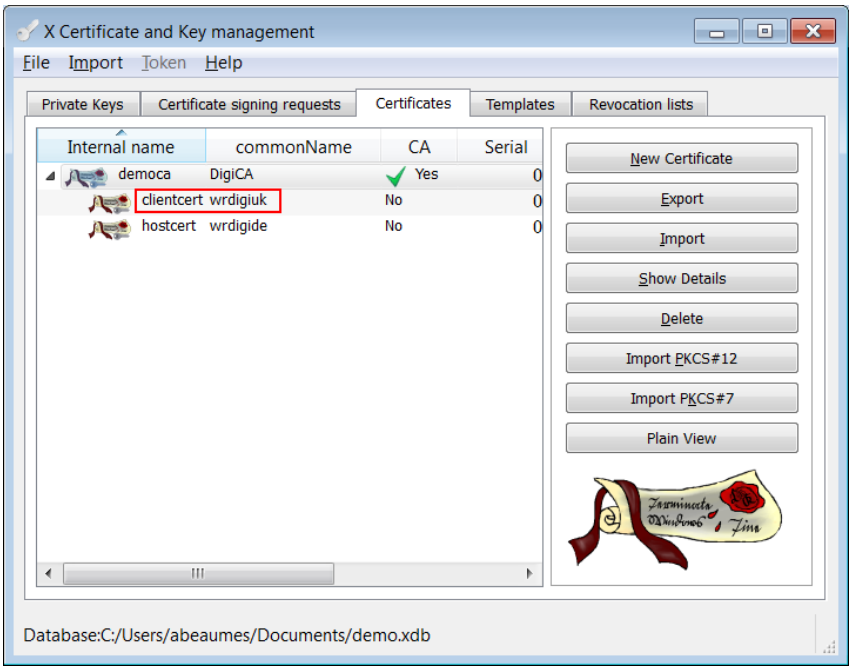


5. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**



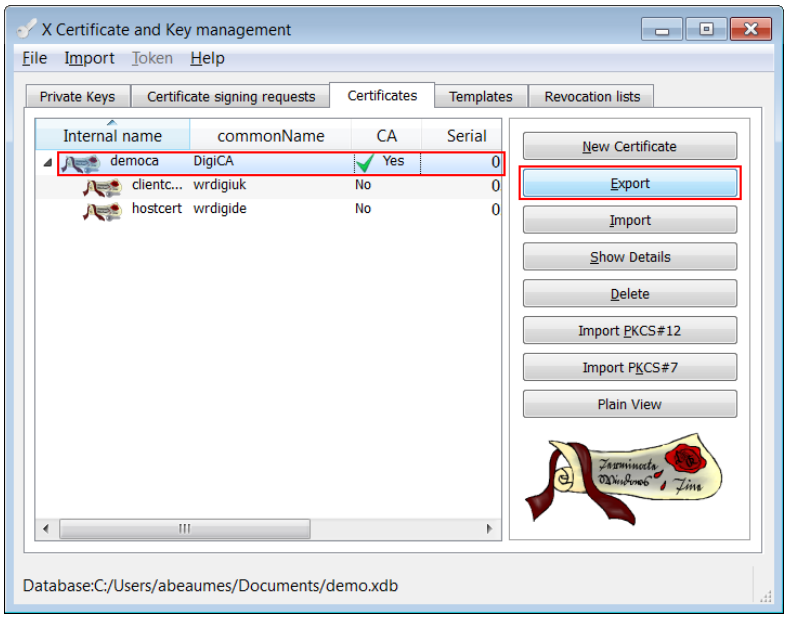
Parameter	Setting
Internal name	This is for display purposes in the tool, only
Country Name	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	The state or province where your organization is legally located. Do not abbreviate. In this example: Some-State
Locality Name	The city where your organization is legally located. Do not abbreviate. In this example: Munich
Organization Name	The exact legal name of your organization. Do not abbreviate your organization name. In this example: DigiDE
Organizational Unit Name	Section of the organization. Examples of sections are Marketing, Research and Development, Human Resources or Sales.
Common Name	In this example **wrdigide** will be used. This will be used as the router Identity for the IPSec tunnel settings
Email Address	Enter your organization general email address. In this example digide@digi.com

1. The certificate should now appear in the window under the CA certificate.

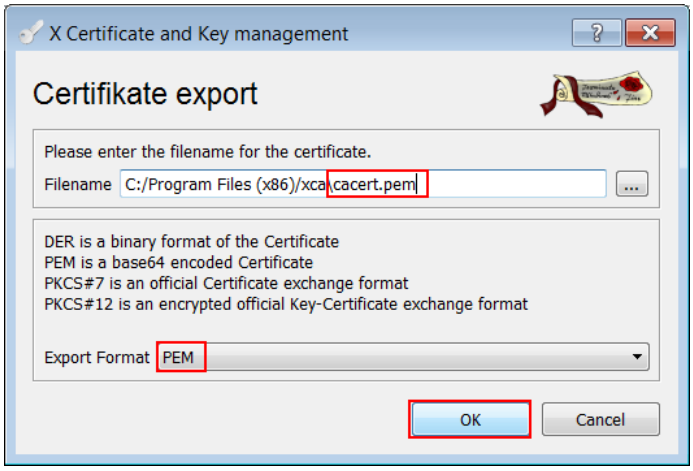


3.1.4 Export the certificates and keys in .PEM format

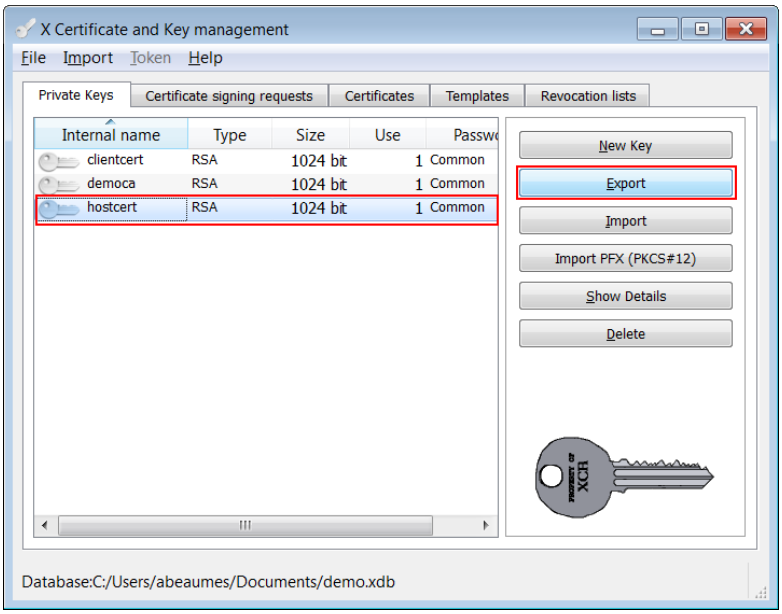
1. Select the **Certificates** Tab.
2. Highlight the DigiCA certificate and click the **Export** button



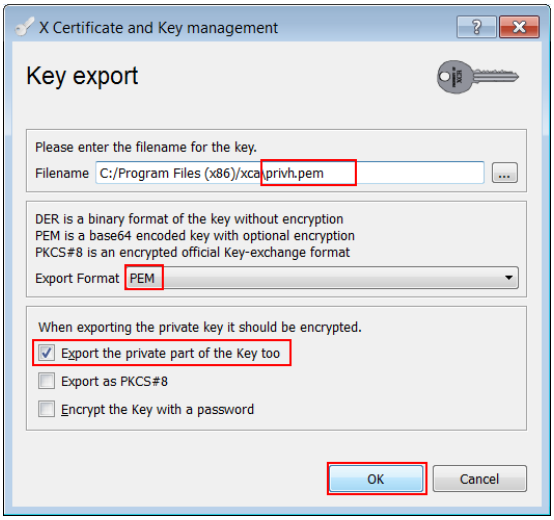
3. In the Certificate export window, select **PEM** as the export format and change the filename to **cacert.pem** and click **OK**



4. Repeat the previous step for the Client and Host certificate. Rename them **certh.pem** and **certcl.pem** .
5. Select the **Private Keys** tab.
6. Highlight the host certificate and click the **Export** button



7. In the Key export window, select **PEM** as the export format, check the box "**Export the private part of the key too**" and change the filename to **privh.pem** and click **OK**



8. Repeat the previous step for the Client key and name it **privcl.pem**.

The following files should now be available:

- cacert.pem : CA root certificate
- certh.pem : host certificate (server)
- certcl.pem : client certificate (client/router)
- privh.pem : host private key (server)
- privcl.pem : client private key (client/router)

Please note: *It is important that the file name do not exceed the 8.3 file format and to keep the file type and naming as the TransPort router will be searching for these and load them in the certificate management automatically.*

3.2 Upload SSL certificates to the router

3.2.1 Upload the certificates via FTP

Open an FTP connection to the TransPort router that you wish to update. In this example, using FileZilla.

Parameter	Setting	Description
Host	192.168.1.105	IP Address of the TransPort router
Username	username	Username with Access Level : Super to log in to the TransPort router (default : username)
Password	password	Password for the user with Access Level : Super to log in to the TransPort router (default : password)
Port	21	Default FTP port.
cacert.pem	-	CA Root certificate
certcl.pem	-	Client Certificate
privcl.pem	-	Client Private Key

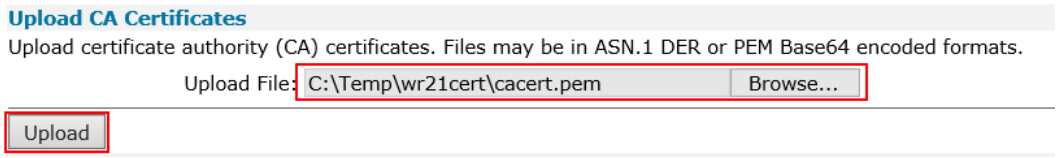
Transfer the certificates file to the root directory of the TransPort.

3.2.2 Upload the certificates via the Web GUI

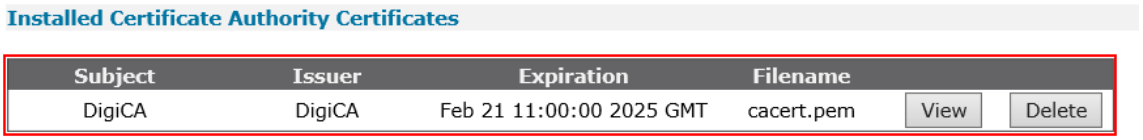
Open a web browser to the IP address of the Digi TransPort router A (initiator)

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

Click the browse button and select the file location where **cacert.pem** is located and click **Upload**

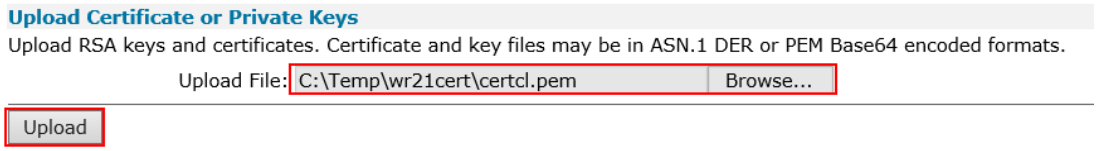


The CA Certificate should now appear under the **Installed Certificate Authority Certificates**

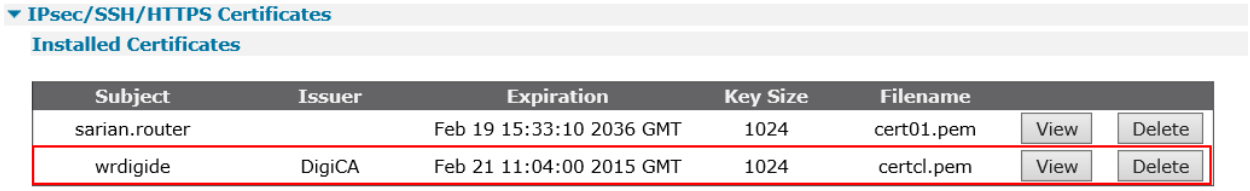


Administration > X.509 Certificate Management > IPSec/SSH/HTTPS Certificates

Click the browse button and select the file location where **certcl.pem** is located and click **Upload**

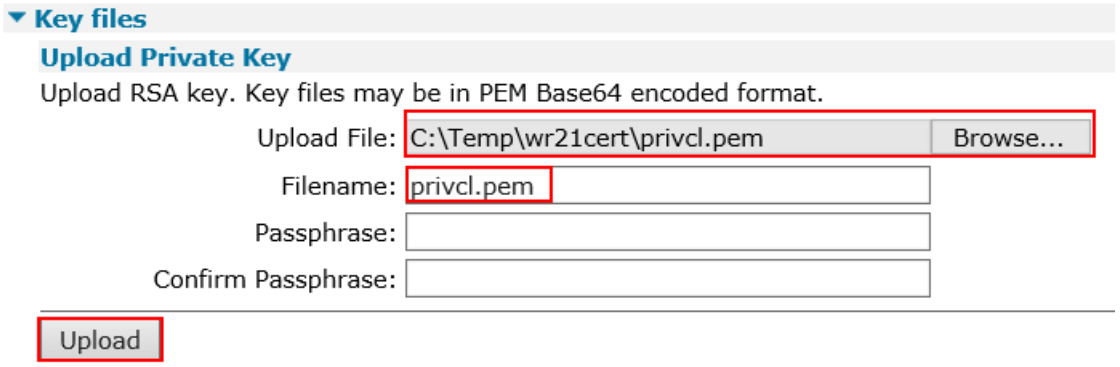


The Certificate should now appear under the **Installed Certificates**



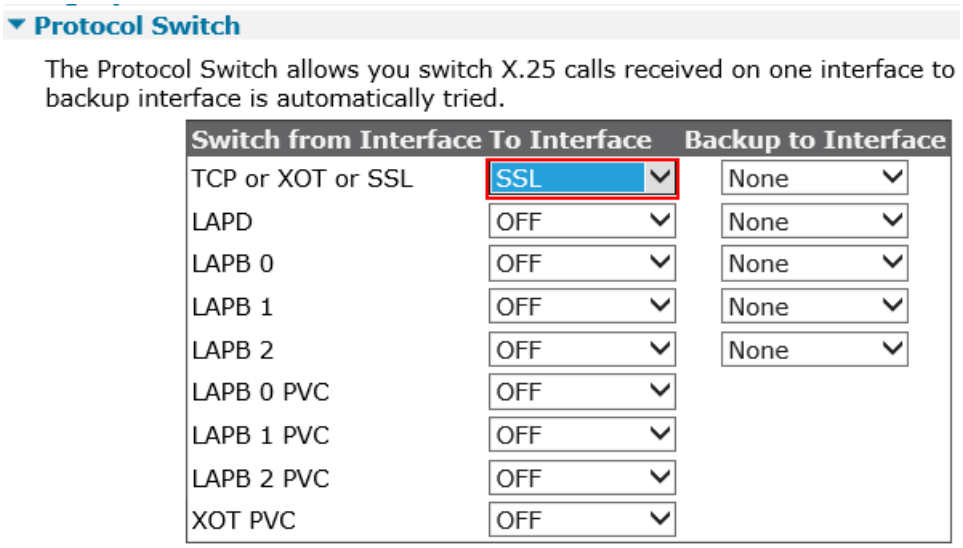
Administration > X.509 Certificate Management > Key Files

Click the browse button and select the file location where **privcl.pem** is located.
Under filename, type **privcl.pem** and click **Upload**.

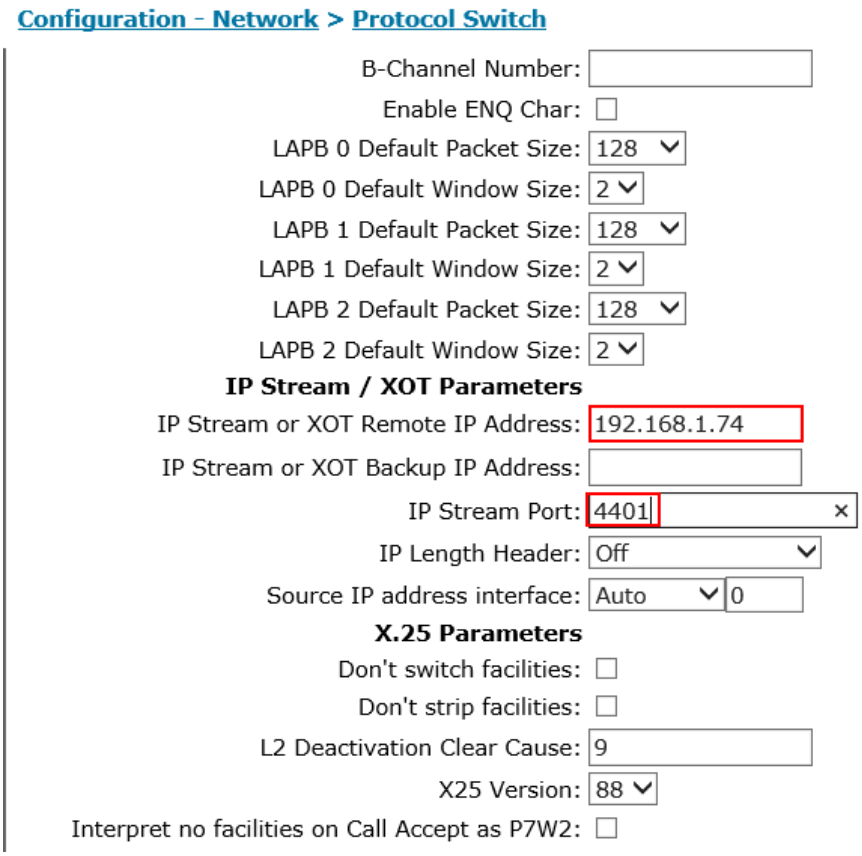


3.3 Configure the SSL socket and Protocol switch settings.

Configuration – Network > Protocol Switch

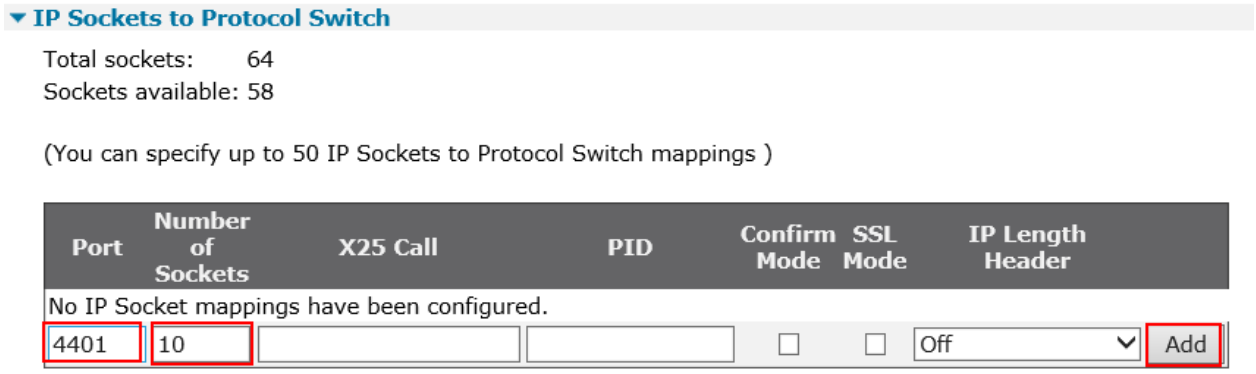


Parameter	Setting	Description
Switch from Interface	SSL	Convert TCP calls to SSL



Parameter	Setting	Description
IP Stream or XOT Remote IP Address	192.168.1.74	IP Address of the OpenSSL server to open the SSL socket with.
IP Stream Port	4401	Port to be used for the SSL socket (OpenSSL server listening port)

Configuration – Network > Protocol Switch > IP Sockets to Protocol Switch



Parameter	Setting	Description
Port	4401	TCP Listening port on the Ethernet side
Number of Sockets	10	Number of Sockets to use
Confirm Mode	Checked	Ensure that the TCP socket will not be successfully connected until the corresponding outgoing call has been connected and that no data is sent into a “black hole”

Enter the desired settings and click the **Add** button.

4 TESTING

For this test, we will use the available binaries from OpenSSL and setup a listening server. Please visit http://www.openssl.org for more information on installing OpenSSL on your operating system.

Copy the **HOST Certificates (cacert.pem, certh.pem, privh.pem)** to the **\bin** directory (for easier usage)

After installation, open a command prompt to the bin directory of OpenSSL, by default: **c:\openssl\bin**

Configure the OpenSSL Server as follow:

```
C:\OpenSSL-Win32\bin>openssl s_server -accept 4401 -cert certh.pem -key
privh.pem -CAfile cacert.pem -debug
```

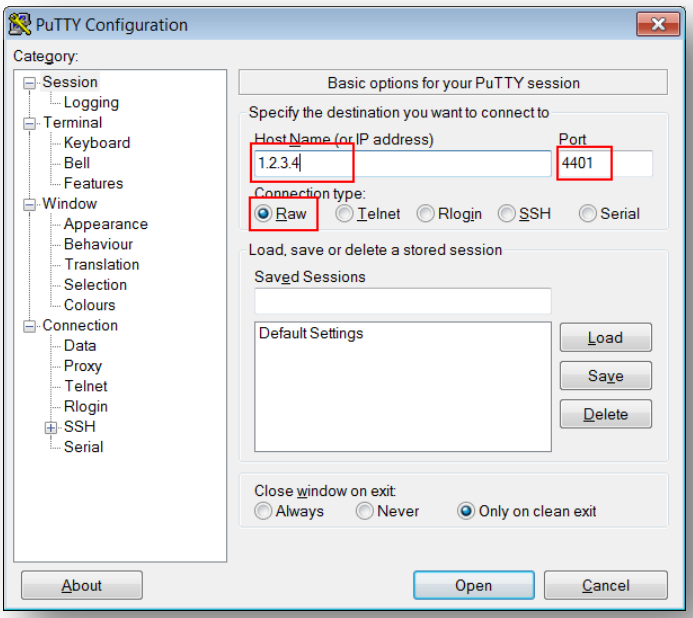
Parameter	Setting	Description
-accept	4401	Port to listen to (matching the port set in the TransPort configuration)
-cert	certh.pem	Host certificate filename/path (if in another folder)
-key	privh.pem	Host private key filename/path (if in another folder)
-CAfile	cacert.pem	CA certificate filename/path (if in another folder)
-debug	-debug	Will output debug information from the OpenSSL server during connection and data transfer. (Helpful during testing. can be removed after.)

The following should now be displayed:

```
Loading 'screen' into random state - done
Using default temp DH parameters
Using default temp ECDH parameters
ACCEPT
```

The server is now ready and listening for connections on port 4401.

On the Computer/Host connected to the Etherport of the Digi TransPort, open a terminal application such as PuTTy and configure the following:



Parameter	Setting	Description
Host name or IP address	1.2.3.4	Host Name or IP Address of the OpenSSL Server
Port	4401	Listening port on the Digi TransPort
Connection Type	Raw	Raw TCP connection type (TCP to SSL conversion being done by the Protocol switch on the Digi TransPort)

Press **Open**

If the **debug** parameter was used, a lot of information should start to be displayed on the screen, which is the certificate exchange. This part will confirm that the tunnel is now established:

```
-----BEGIN SSL SESSION PARAMETERS-----
MHUCAQECAgMBBAIAOQQga5YPIXrIkgvXfAWNEZq546BbiNgSyeoY/H8X2c+/yroE
MNNPNStrI6ONr0NxiiCkGHadPVWLuYu3eLHPlRw9419babjMy4zL0budsSJ6i4ZT
x6EGAgRTFcrsogQCAgEspAYEBAEAAAA=
-----END SSL SESSION PARAMETERS-----
Shared ciphers:DHE-RSA-AES256-SHA:AES256-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:D
HE-RSA-AES128-SHA:AES128-SHA:RC4-SHA:RC4-MD5:EDH-RSA-DES-CBC-SHA:DES-CBC-SHA:EXP
-EDH-RSA-DES-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC4-MD5
CIPHER is DHE-RSA-AES256-SHA
Secure Renegotiation IS NOT supported
```

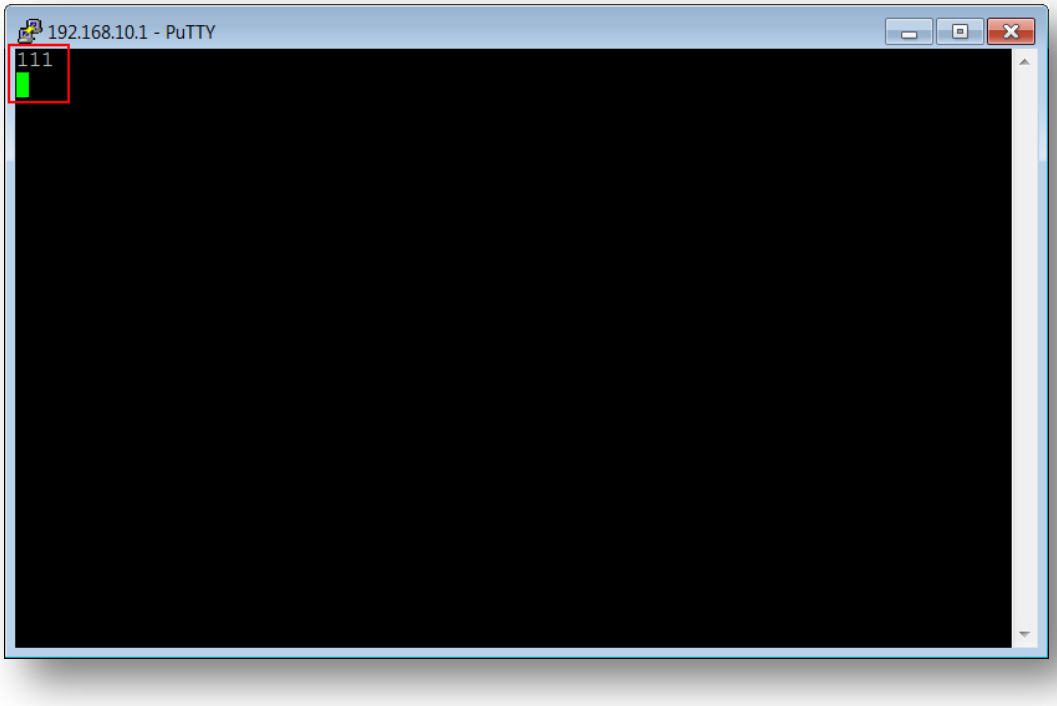
Check the Digi TransPort router event log:

Management – Event Log >

```
12:51:16, 04 Mar 2014,GP socket connected: 192.168.10.1:4401 ->
192.168.10.5:56963
12:51:16, 04 Mar 2014,XSW 20 Call req connect
12:51:10, 04 Mar 2014,GP socket connected: 37.80.2.241:1108 -> 92.92.92.21:4401
12:51:08, 04 Mar 2014,1 X25 Calls per sec
12:51:07, 04 Mar 2014,TCP Req: 0.0.0.0:1108 -> 92.92.92.21:4401
12:51:07, 04 Mar 2014,XSW 20 X25 Call req #: 567
12:51:07, 04 Mar 2014,XSW 0 Inc X25 call #:
```

The tunnel is established.

Sending data in the Terminal/PuTTy Window will appear in the debug window of the OpenSSL server:




```
read from 0x1526590 [0x1563acb] (5 bytes => 5 (0x5))
0000 - 17 03 01                                          ...
0005 - <SPACES/NULS>
read from 0x1526590 [0x1563ad0] (32 bytes => 32 (0x20))
0000 - f0 3c 7f bf 35 53 30 ac-8f f8 ed 95 36 4f 2f 6b   .<..5S0.....6O/k
0010 - 3d d1 28 53 89 fd de 5b-64 5a bb a8 c1 00 0a f8   =.(S...[dZ......
111
```

Closing the Terminal/PuTTy window will close the OpenSSL Tunnel:

```
read from 0x1526590 [0x1563acb] (5 bytes => 5 (0x5))
0000 - 15 03 01                                          ...
0005 - <SPACES/NULS>
read from 0x1526590 [0x1563ad0] (32 bytes => 32 (0x20))
0000 - 34 cd dd b2 e8 b5 1e ac-25 d8 c2 50 4a bf 23 2e   4.......%..PJ.#.
0010 - e4 b0 0c 72 78 28 bf 61-45 4f 48 85 1f d6 d2 aa   ...rx(.aEOH.....
DONE
shutting down SSL
CONNECTION CLOSED
ACCEPT
```

5 CONFIGURATION FILES

Digi TransPort WR21

```
ipx25 0 ip_port 4401
ipx25 0 nb_listens 10
ipx25 0 cnf_mode 1
x25sw 0 IPaddr "192.168.1.74"
x25sw 0 swfrxot 15
x25sw 0 ip_port 4401
x25sw 0 lapdwpar 2
x25sw 0 lapdppar 7
x25sw 0 lapb0wpar 2
x25sw 0 lapb0ppar 7
x25sw 0 lapb1wpar 2
x25sw 0 lapb1ppar 7
x25sw 0 lapb2wpar 2
x25sw 0 lapb2ppar 7
```