



Quick Note 63

How To Configure IKEv2 VPN between
TransPort WR routers using Open SSL
Certificates

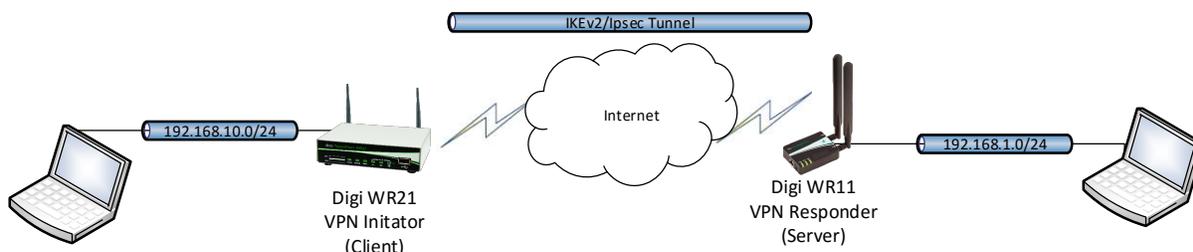
Contents

1	Introduction	3
1.1	Outline.....	3
1.2	Assumptions.....	3
1.3	Corrections.....	3
1.4	Version.....	3
2	Generate Test Certificates	4
2.1	Create a Root CA Certificate	4
2.2	Create a CA-Signed Host Certificate (Responder)	10
2.3	Create a CA-Signed Client Certificate (Initiator)	14
2.4	Export the certificates and keys in .PEM format.....	18
2.4.1	Export Certificates	18
2.4.2	Export Keys	20
3	Digi Routers Configuration	22
3.1	Responder configuration.....	22
3.1.1	Upload Certificates and Keys	22
3.1.2	VPN Configuration	27
3.2	Initiator configuration	31
3.2.1	Upload Certificates and Keys	31
3.2.2	VPN Configuration	36
4	Testing.....	40
4.1	Check the IPsec tunnel is UP	40
4.2	Check the Traffic passes through the IPsec tunnel	42
	Configuration Files.....	47

1 INTRODUCTION

1.1 Outline

This document describes how to create, upload SSL certificates and configure Digi TransPort WR routers to build a VPN tunnel using IKEv2.



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 to:

Model: DIGI TransPort WR11/WR21

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 you 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.

1.4 Version

Version	Status
1.0	Published

2 GENERATE TEST CERTIFICATES

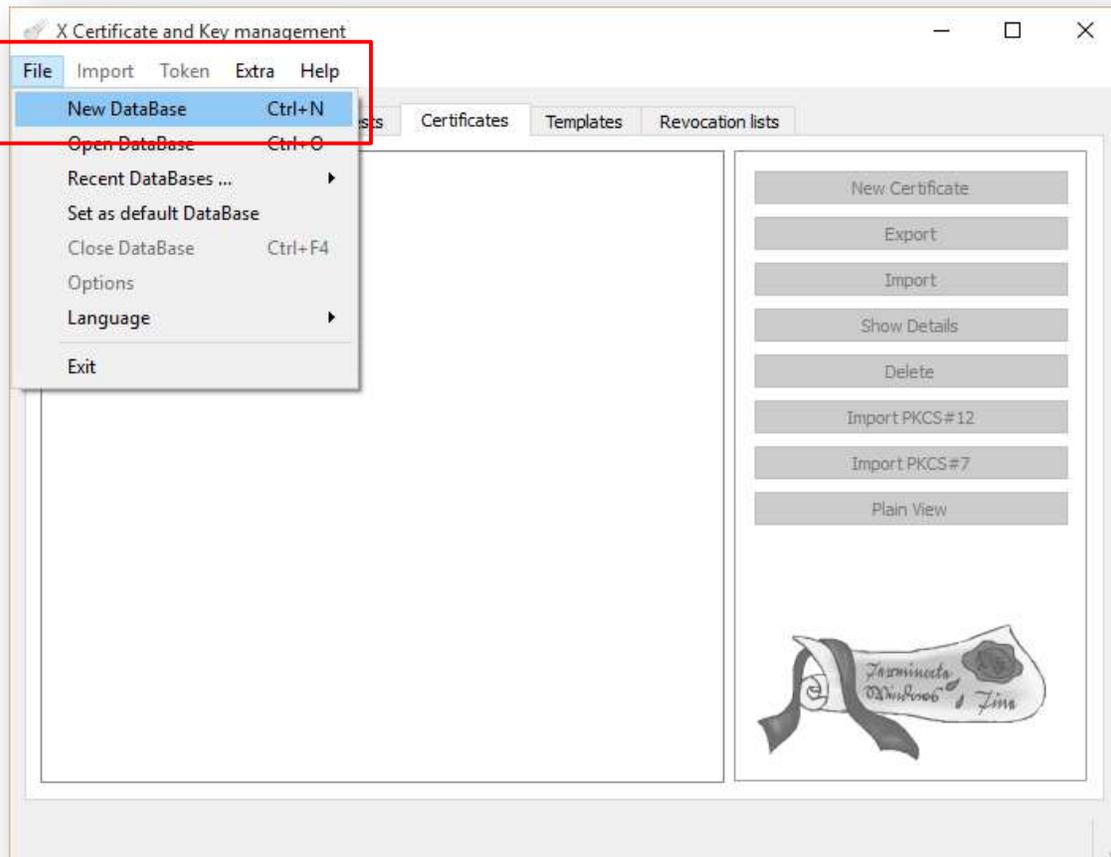
Note: If you already have certificates available, you can skip to section 3

In order to create the certificates that will be used in the IKEv2 VPN, XCA application can be used. The first step is to download and install the latest release of XCA which can be found at: <http://sourceforge.net/projects/xca/>.

In this section will be explained how to create the Root CA certificate, the CA-Signed Host Certificates for both the Responder and the Initiator, and all the related Keys. Will be also shown how to export those certificates and keys in order to be then uploaded on the Transport routers.

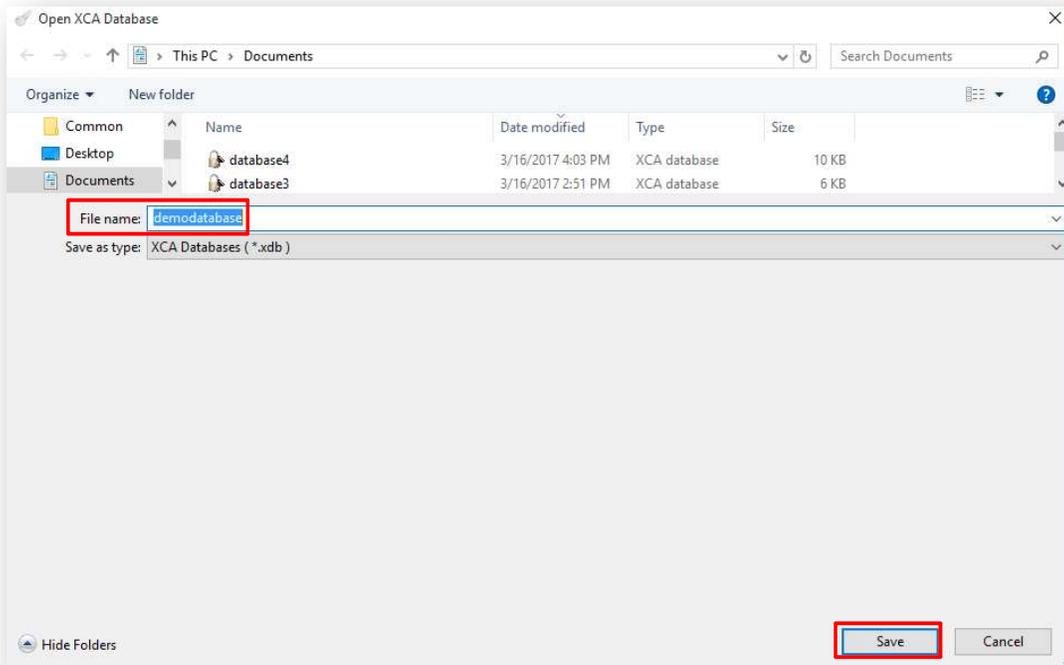
2.1 Create a Root CA Certificate

Open the XCA application, click on **File > New Database:**

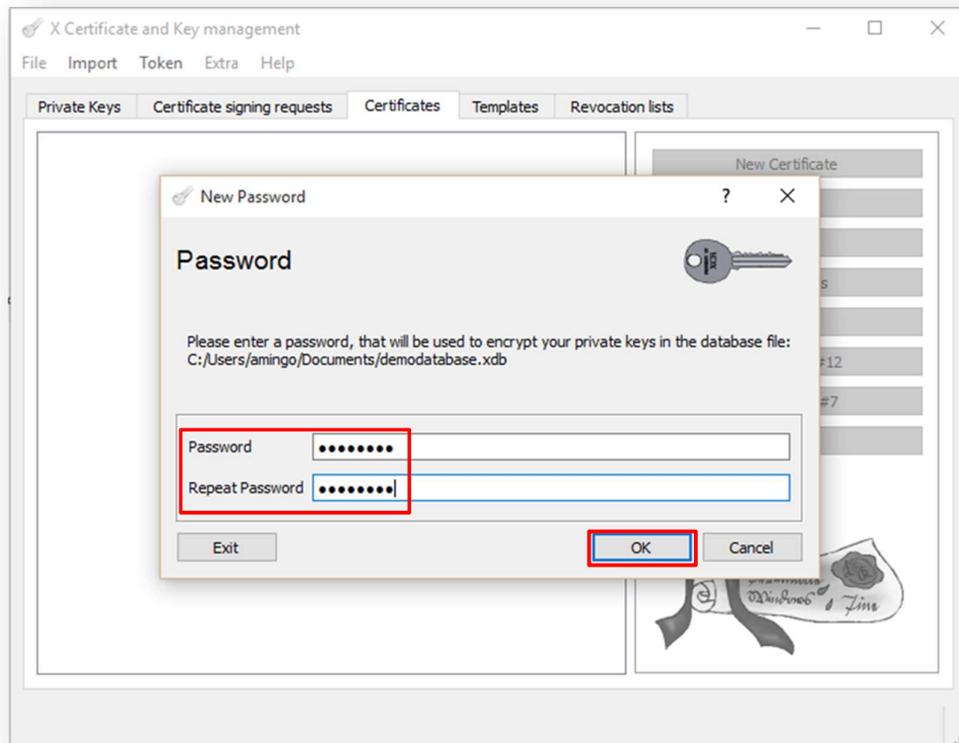


How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Chose a name for the Database and click **“Save”**:

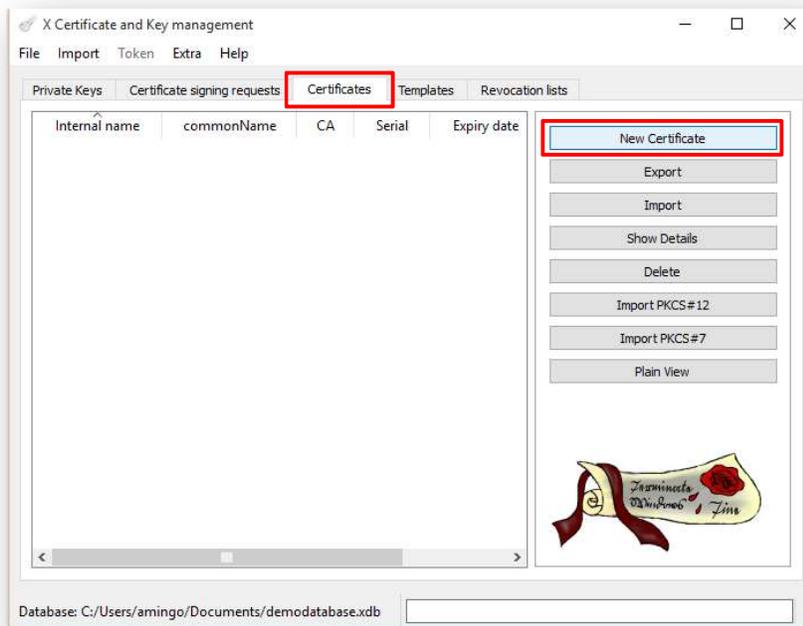


Chose a password for the Database and click **“OK”**:

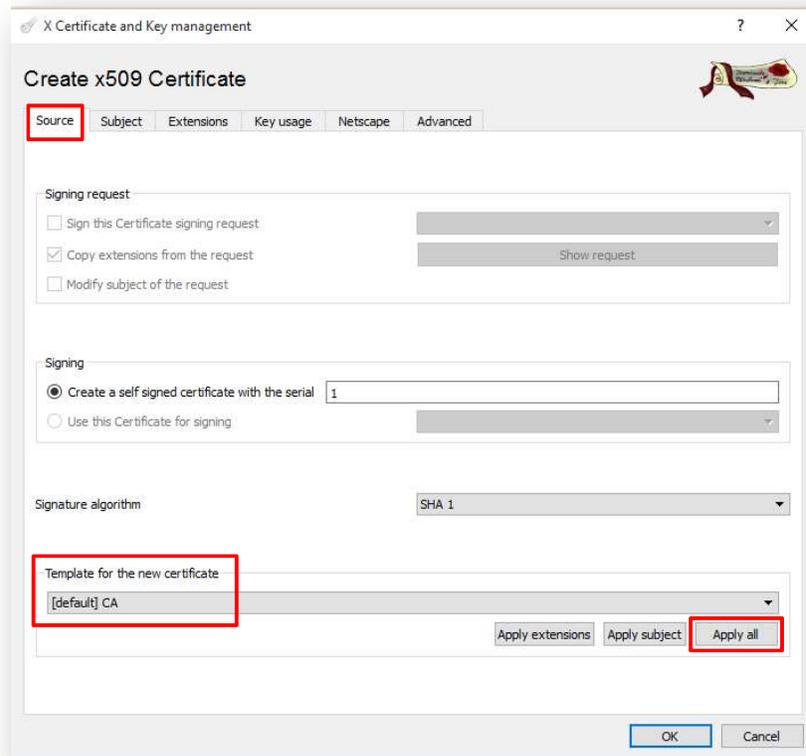


How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Under the “**Certificates**” tab, click on “**New Certificate**”:



The “**Create x509 certificate**” window will be shown. In the “**Source**” tab check the “**Template for the new certificate**” and ensure that “[**default**] CA” is selected. Then click on “**Apply all**”



How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

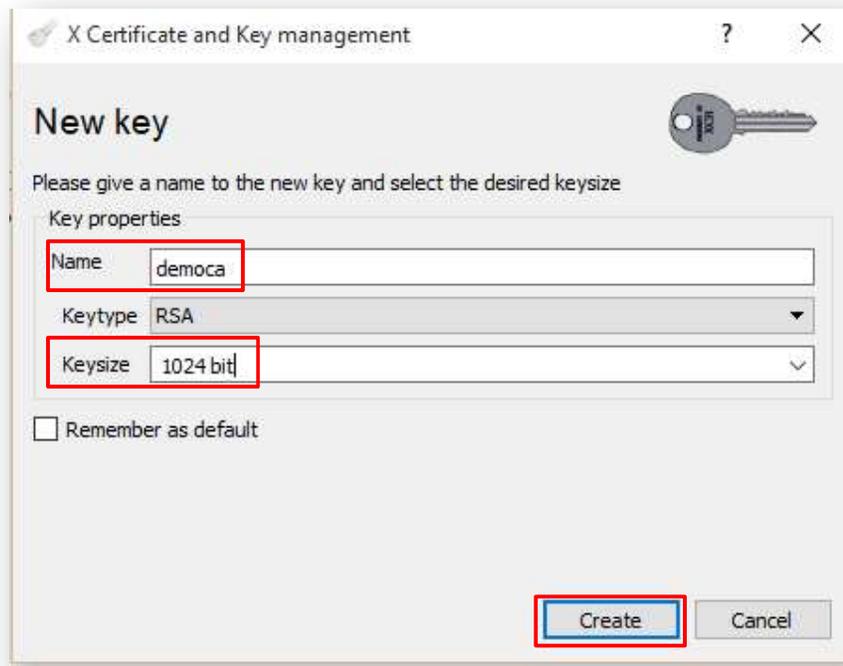
Go to the **“Subject”** tab, fill in all the information then click the **“Generate a new key”** button:

Where:

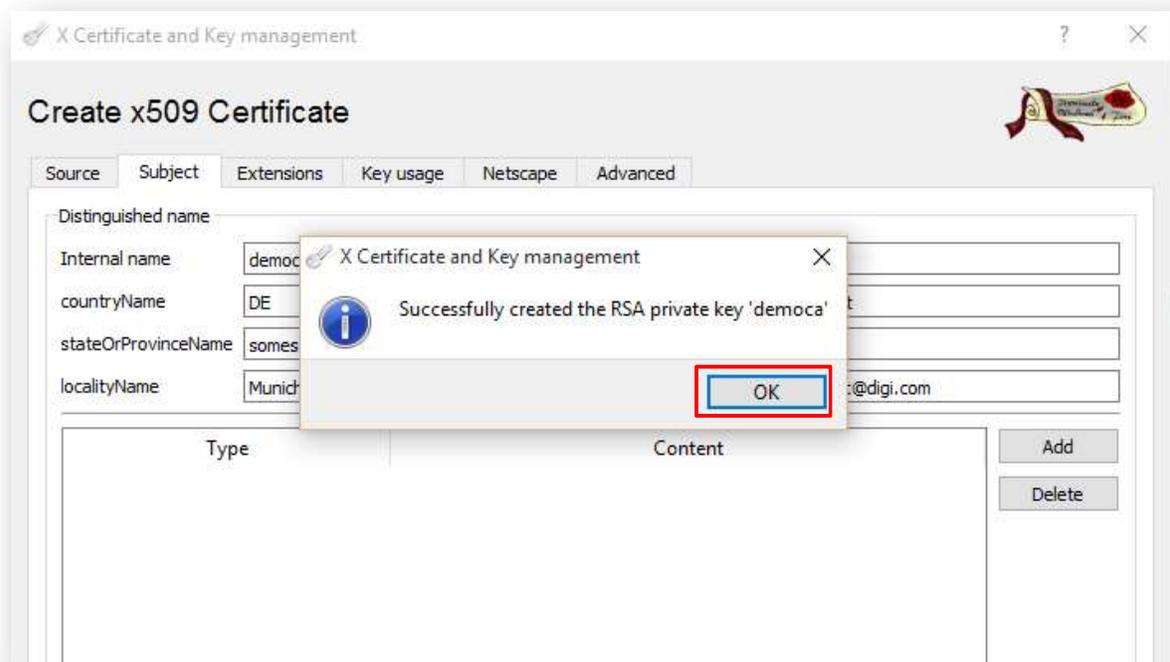
Parameter	Setting	Description
Internal name	democa	This is for display purposes in the tool only
Country Name	DE	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	somestate	The state or province where your organization is legally located. Do not abbreviate.
Locality Name	Munich	The city where your organization is legally located. Do not abbreviate.
Organization Name	Digi	The exact legal name of your organization. Do not abbreviate your organization name.
Organizational Unit Name	Support	Section of the organization.
Common Name	DigiCA	In this example DigiCA will be used.
Email Address	support@digicom	Enter your organization general email address.

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

The “**New Key**” window will be shown, chose the name and Keysize and click on “Create”:

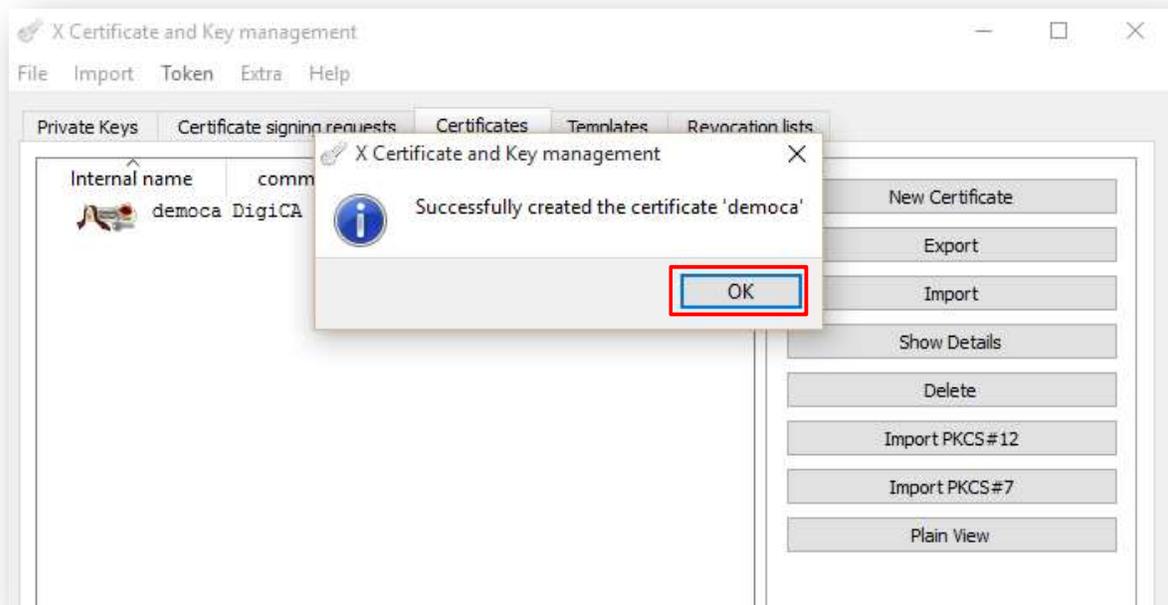


A pop-up window will show up as a confirmation of the Key creation:

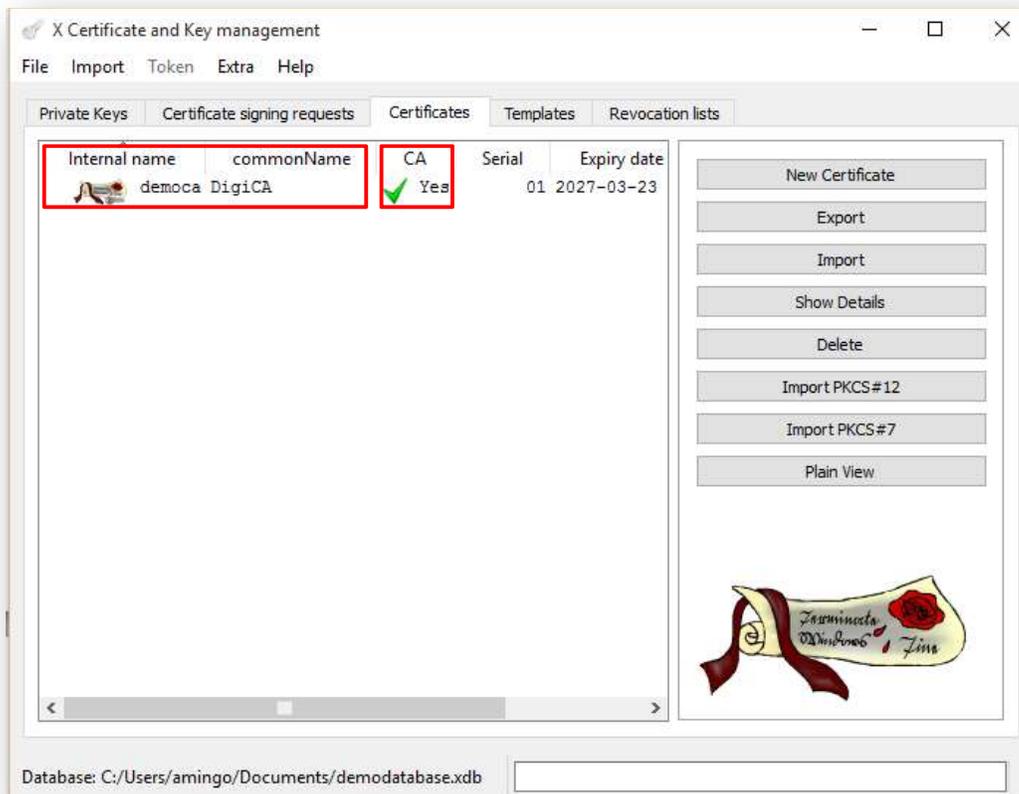


Click “**OK**” to close this and click again “**OK**” in the main “**Create x509 certificate**” window to complete the creation of certificate. Again, a pop-up window will show up as a confirmation of the Certificate creation:

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates



Click “**OK**” to close this and the certificate should now appear in the XCA main 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.

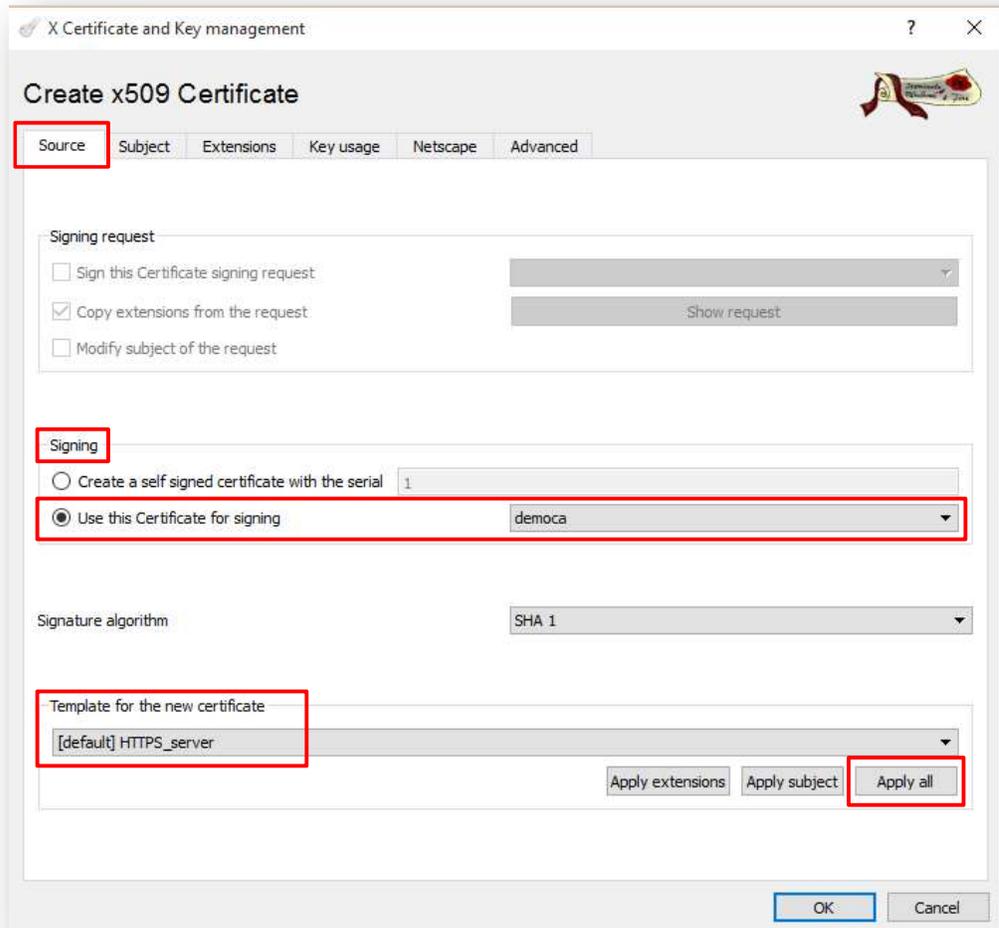


2.2 Create a CA-Signed Host Certificate (Responder)

Under the “**Certificates**” tab, click again on “**New Certificate**” and the “**Create x509 certificate**” window will be shown.

In the “**Source**” tab check the “**Signing**” section and make sure to select “**Use this Certificate for signing**” and chose the previously created CA.

Under “**Template for the new certificate**” select “[**default**] HTTPS_server” and click “**Apply all**”:



How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

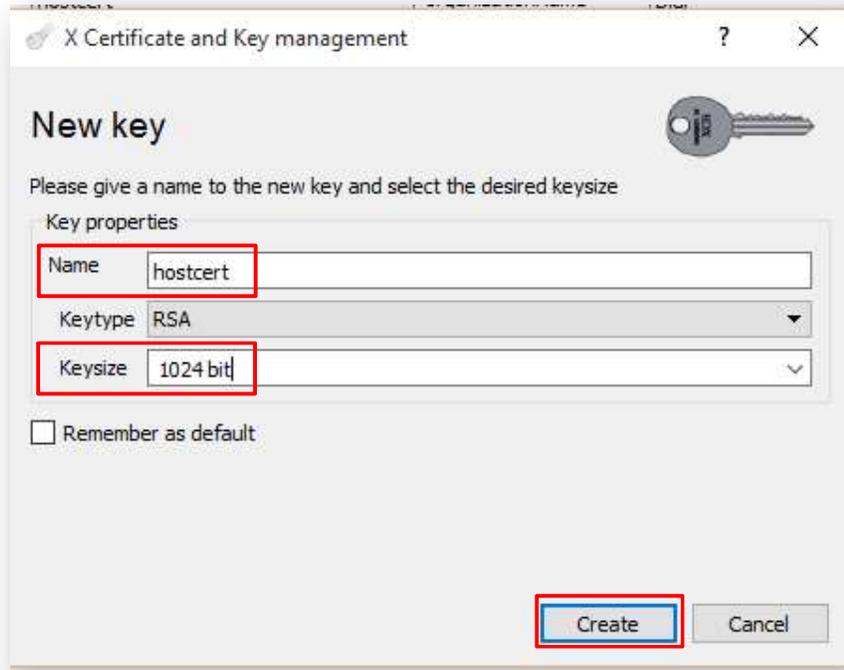
Go to the “**Subject**” tab, fill in all the information then click the “**Generate a new key**” button:

Where:

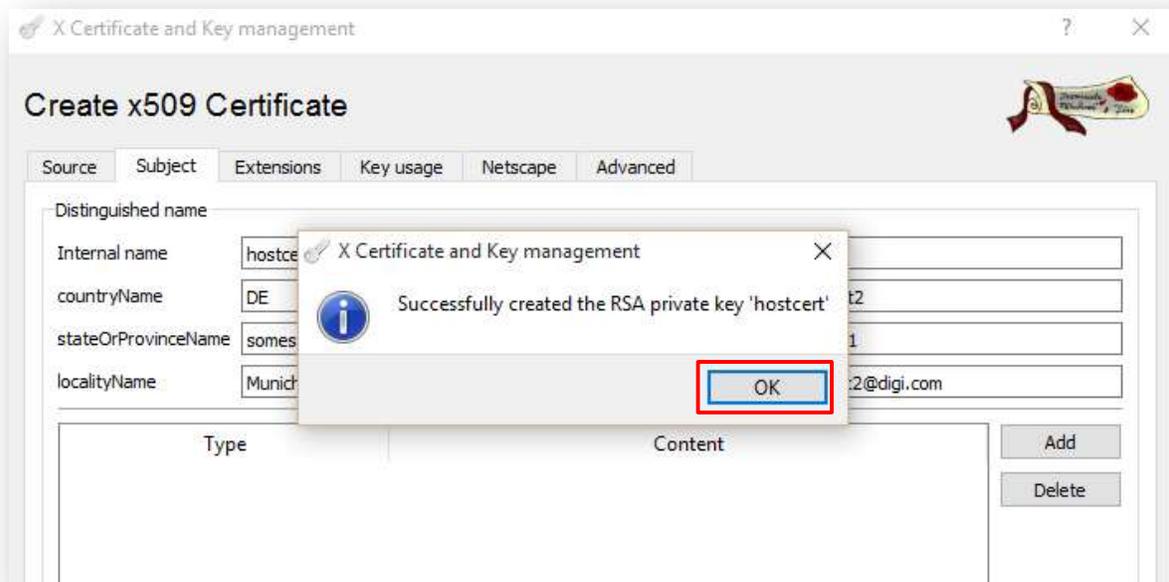
Parameter	Setting	Description
Internal name	hostcert	This is for display purposes in the tool, only
Country Name	DE	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	somestate	The state or province where your organization is legally located. Do not abbreviate.
Locality Name	Munich	The city where your organization is legally located. Do not abbreviate.
Organization Name	Digi	The exact legal name of your organization. Do not abbreviate your organization name.
Organizational Unit Name	Support2	Section of the organization.
Common Name	digiwr11	In this example digiwr11 will be used. This will be used as the router Identity for the IPSec tunnel settings on the responder
Email Address	support2@digi.com	Enter your organization general email address.

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

The “New Key” window will be shown, chose the name and Keysize and click on “Create”:

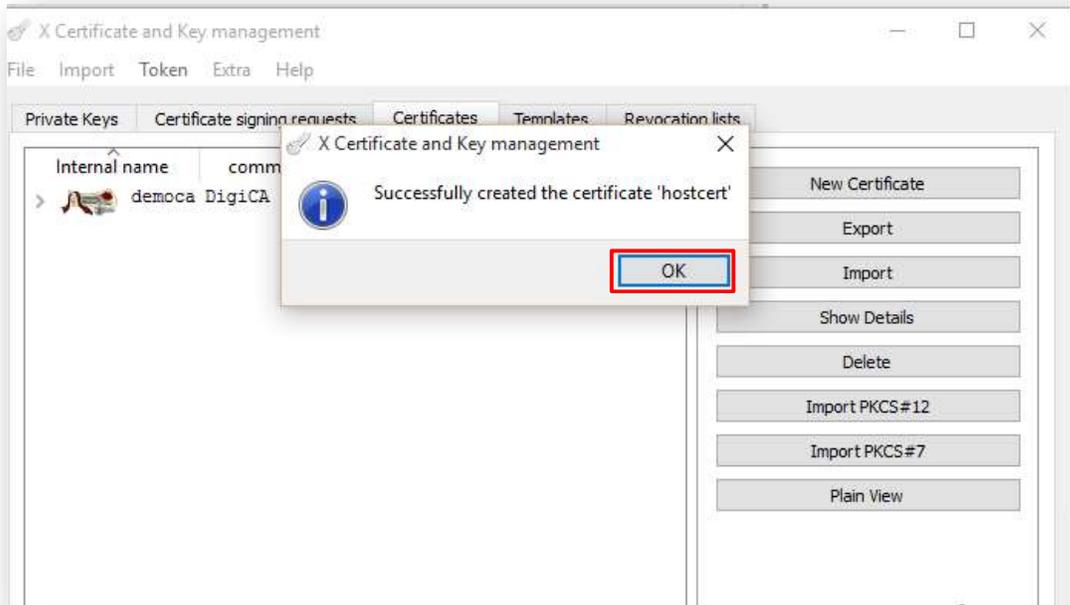


A pop-up window will show up as a confirmation of the Key creation:



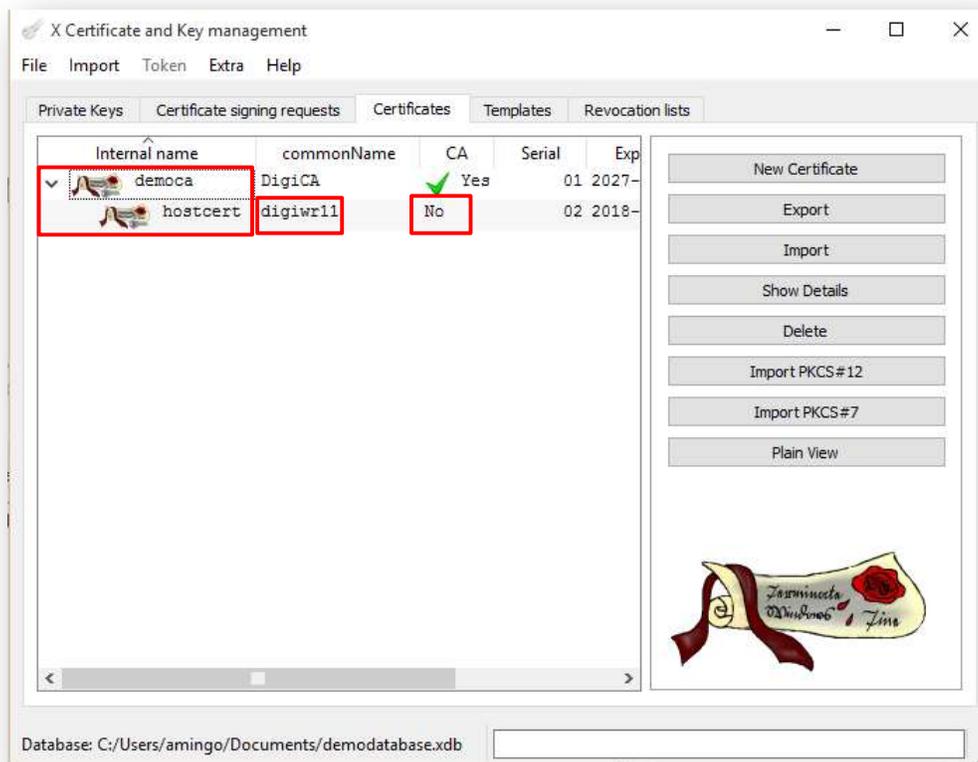
Click “OK” to close this and click again “OK” in the main “Create x509 certificate” window to complete the creation of certificate. Again, a pop-up window will show up as a confirmation of the Certificate creation:

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates



Click “**OK**” to close this and the certificate should now appear in the window under the CA certificate.

Please Note: the value in the Common Name field for this certificate, will be used as Responder ID in the IPsec tunnel settings.

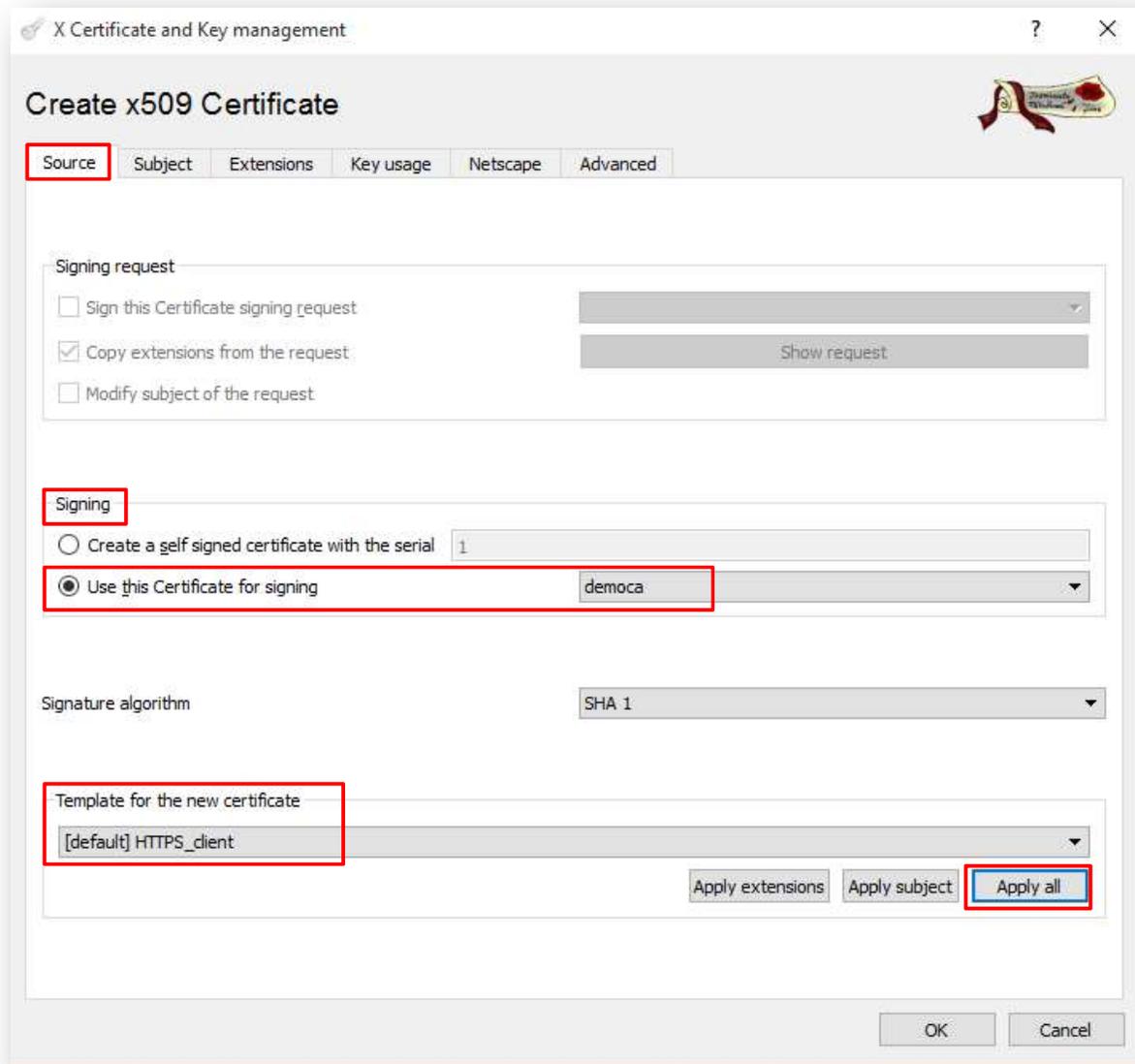


2.3 Create a CA-Signed Client Certificate (Initiator)

Under the “**Certificates**” tab, click again on “**New Certificate**” and the “**Create x509 certificate**” window will be shown.

In the “**Source**” tab check the “**Signing**” section and make sure to select “**Use this Certificate for signing**” and chose the previously created CA.

Under “**Template for the new certificate**” select “[**default**] HTTPS_client” and click “**Apply all**”:



How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

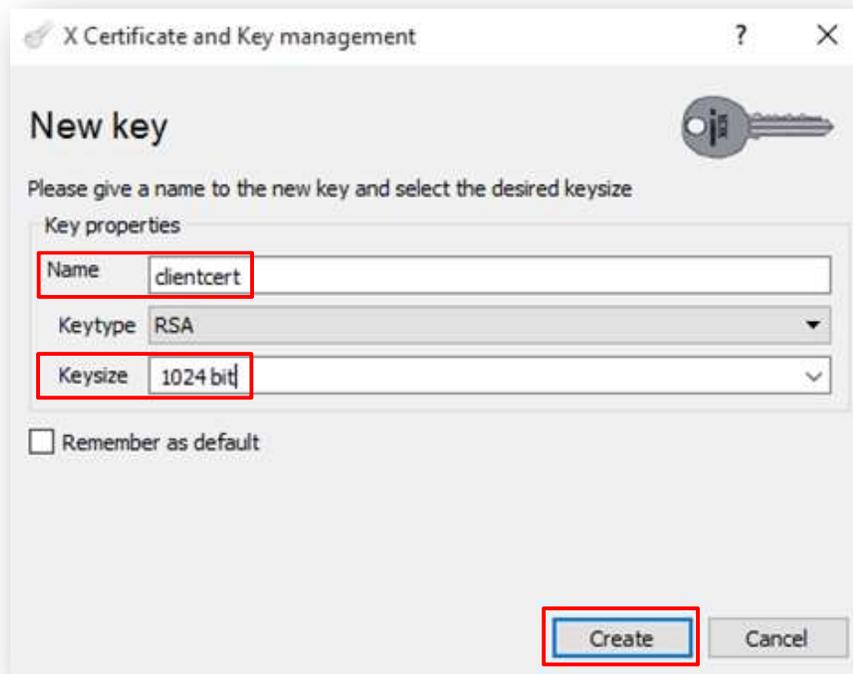
Go to the “Subject” tab, fill in all the information then click the “Generate a new key” button:

Where:

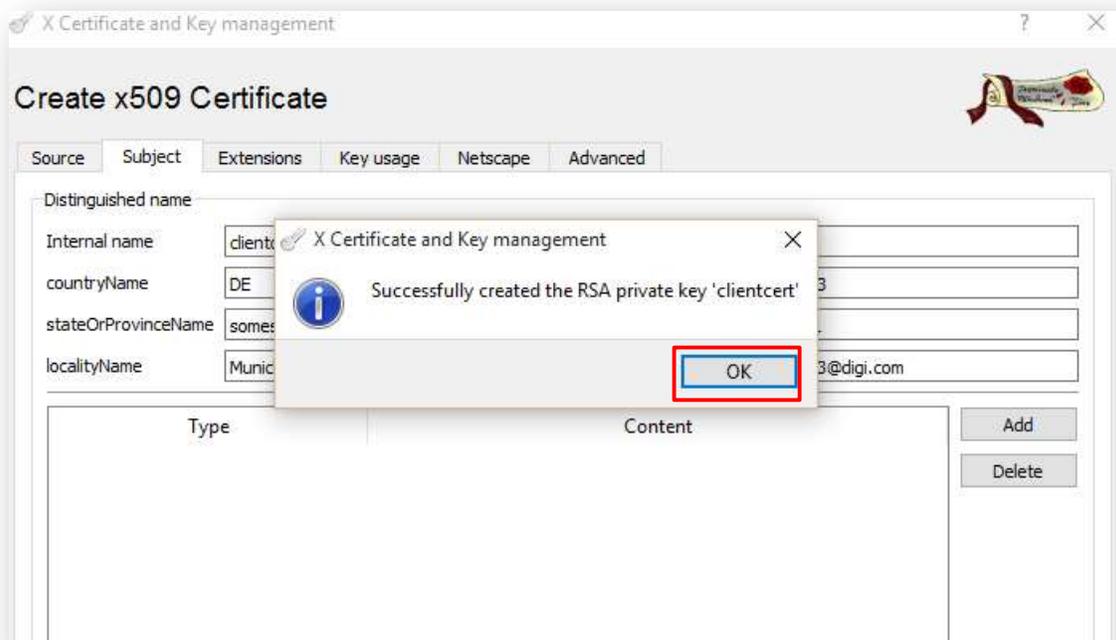
Parameter	Setting	Description
Internal name	clientcert	This is for display purposes in the tool only
Country Name	DE	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	Somestate	The state or province where your organization is legally located. Do not abbreviate.
Locality Name	Munich	The city where your organization is legally located. Do not abbreviate.
Organization Name	Digi	The exact legal name of your organization. Do not abbreviate your organization name.
Organizational Unit Name	Support3	Section of the organization.
Common Name	digiwr21	In this example digiwr21 will be used. This will be used as the router Identity for the IPSec tunnel settings on the initiator
Email Address	Support3@digicom	Enter your organization general email address.

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

The “**New Key**” window will be shown, chose the name and Keysize and click on “Create”:

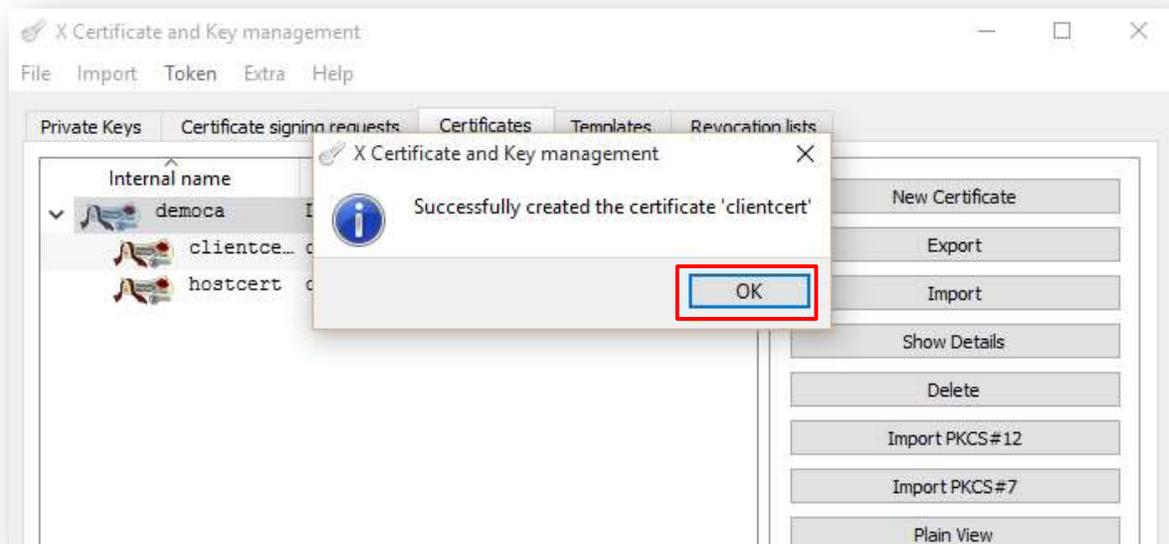


A pop-up window will show up as a confirmation of the Key creation:



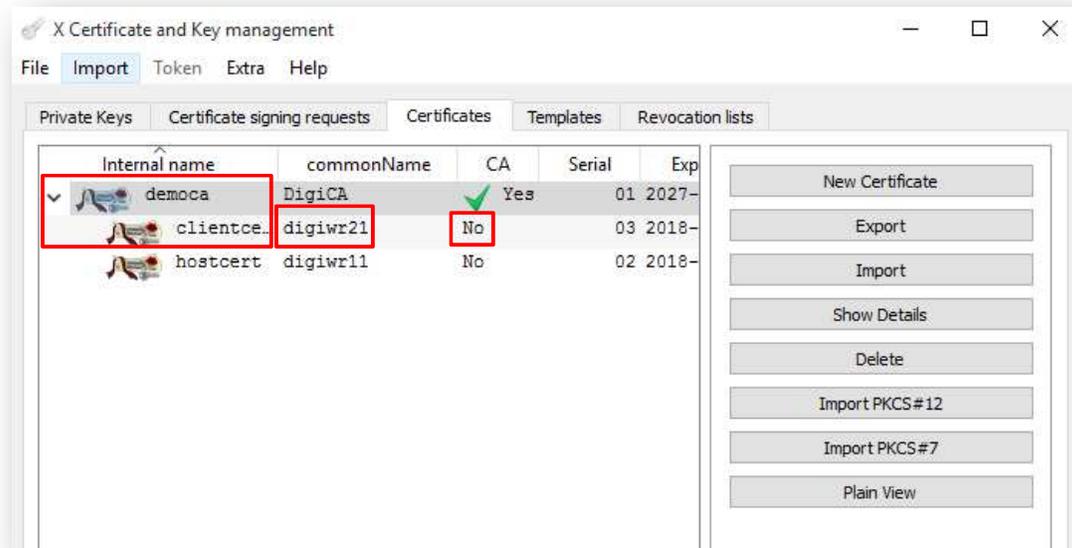
Click “**OK**” to close this and click again “**OK**” in the main “**Create x509 certificate**” window to complete the creation of certificate. Again, a pop-up window will show up as a confirmation of the Certificate creation:

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates



Click “**OK**” to close this and the certificate should now appear in the window under the CA certificate:

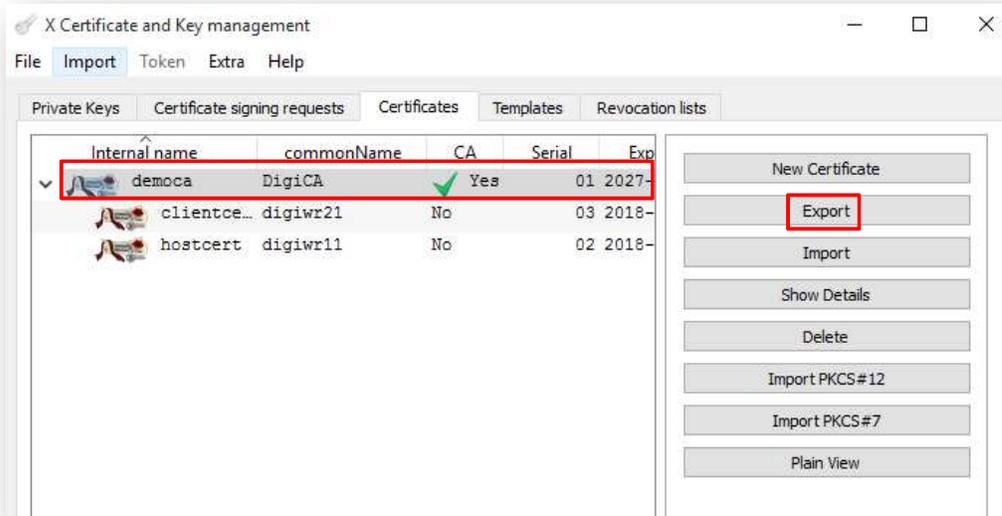
Please Note: the value in the Common Name field for this certificate, will be used as Initiator ID in the IPsec tunnel settings.



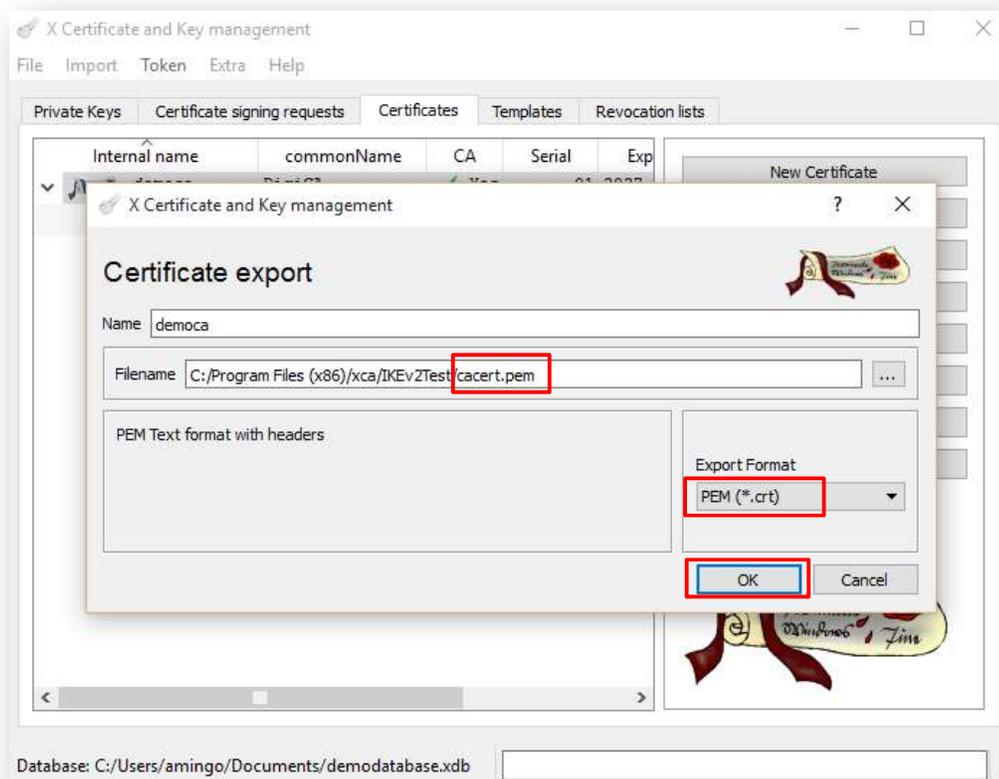
2.4 Export the certificates and keys in .PEM format

2.4.1 Export Certificates

In the "Certificates" tab, highlight the CA certificate and click on "Export":

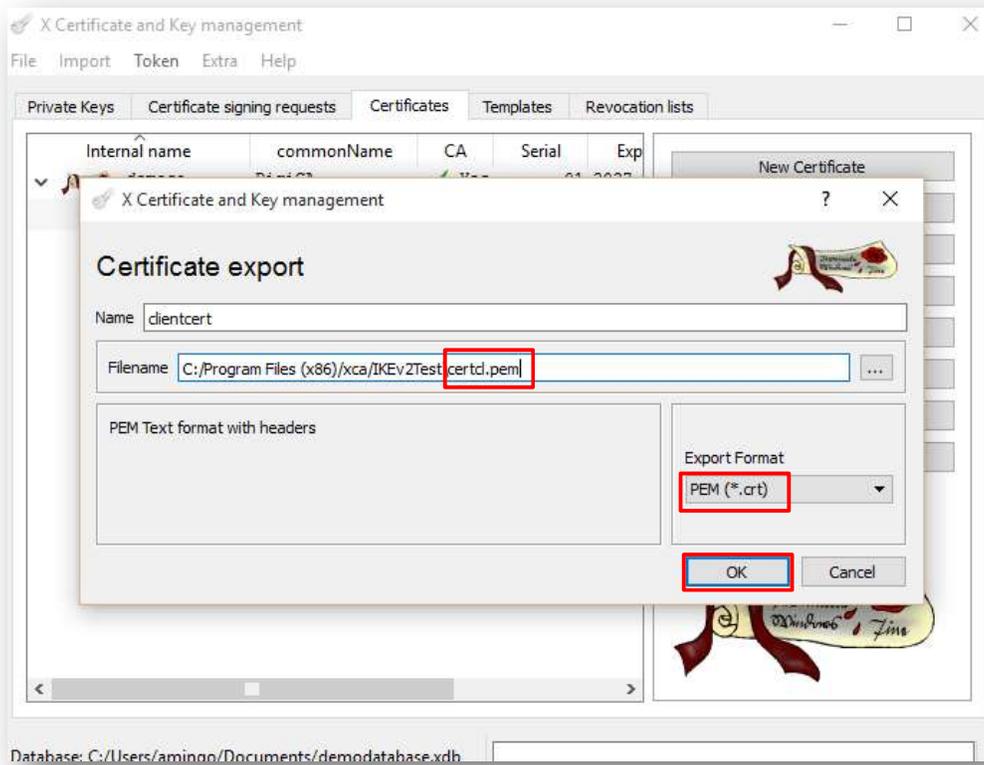
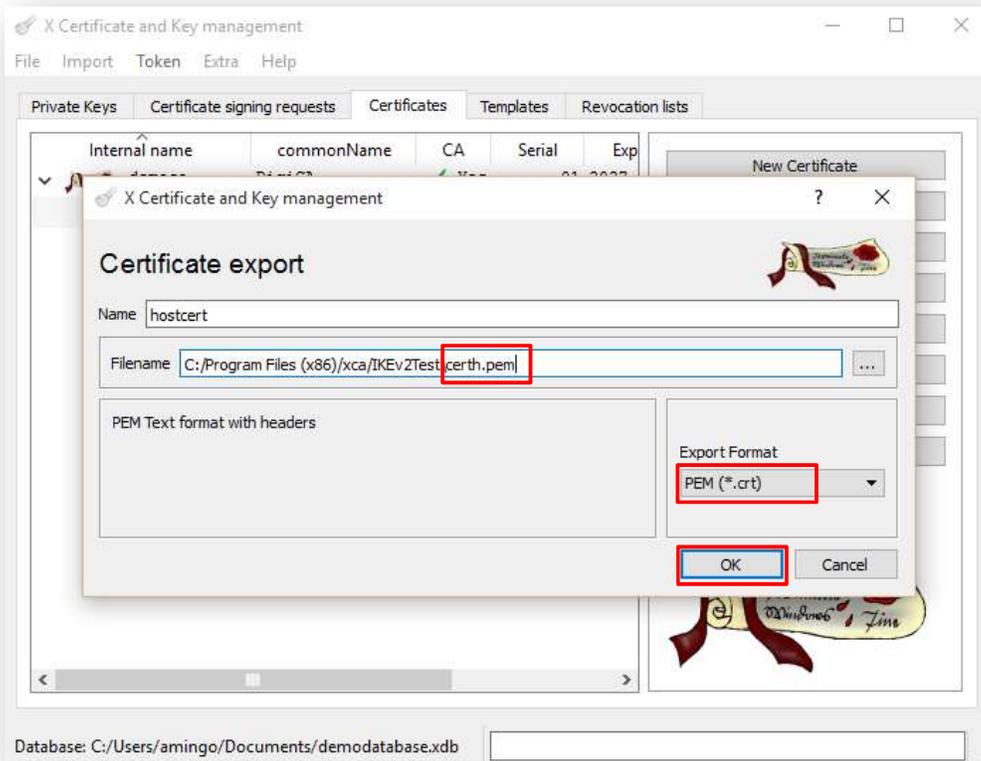


In the "Certificate export" window, select **PEM (*.cert)** as the export format and change the filename to **cacert.pem** and click "OK":



How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

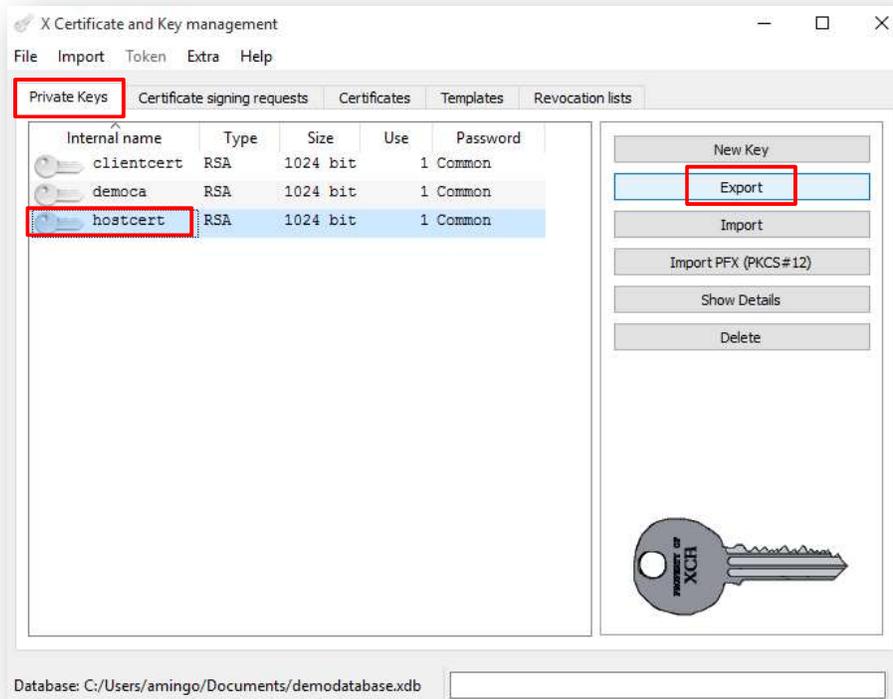
Repeat the previous step for the Client and Host certificate. Rename them **certh.pem** and **certcl.pem** :



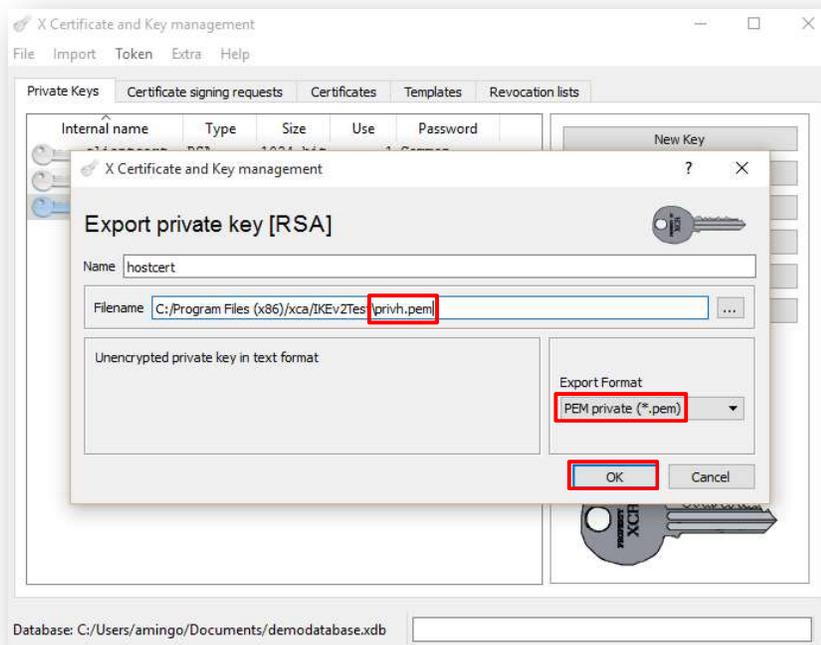
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

2.4.2 Export Keys

From the main XCA window, select the “**Private Keys**” tab, highlight the host certificate key and click the “**Export**” button:

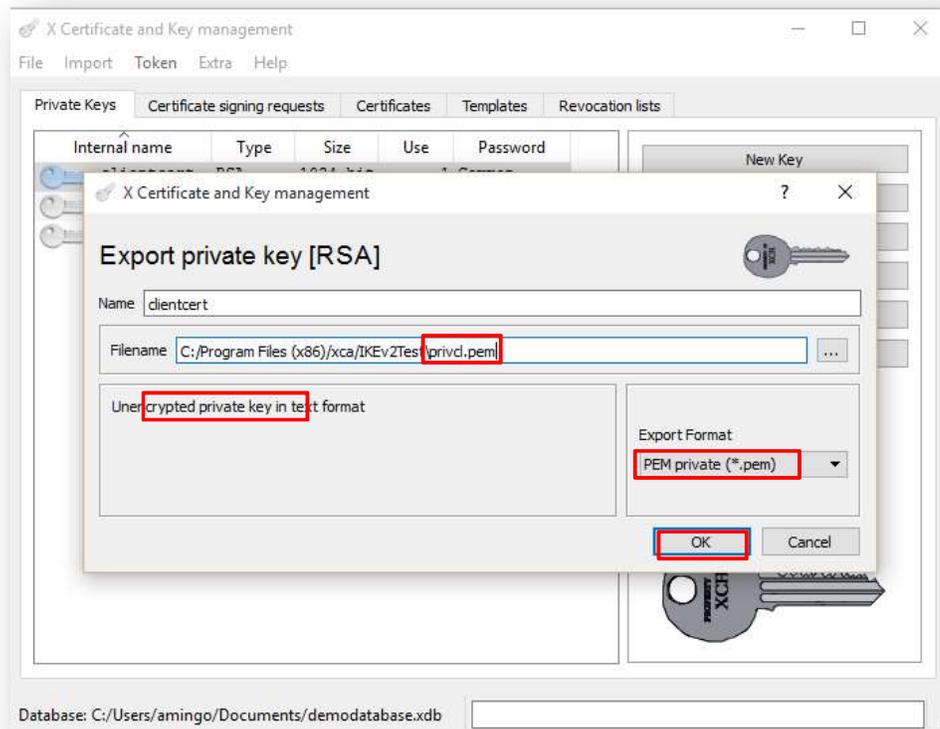


In the “**Export Private Key [RSA]**” window, select **PEM private (*.pem)** as the export format and change the filename to **privh.pem** and click “**OK**”:



How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

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



After all the above steps are completed, the following files should now be available:

- **ca-cert.pem** : CA root certificate
- **certth.pem** : Responder certificate
- **certcl.pem** : Initiator certificate
- **privh.pem** : Responder private key
- **privcl.pem** : Initiator private key

Please note: It is important that each 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 DIGI ROUTERS CONFIGURATION

3.1 Responder configuration

The Responder configuration consists in uploading the certificates and the keys on the router, and then set UP the IKEv2 VPN to use them in the negotiation with the Initiator. All this aspects will be explained in the subsections below.

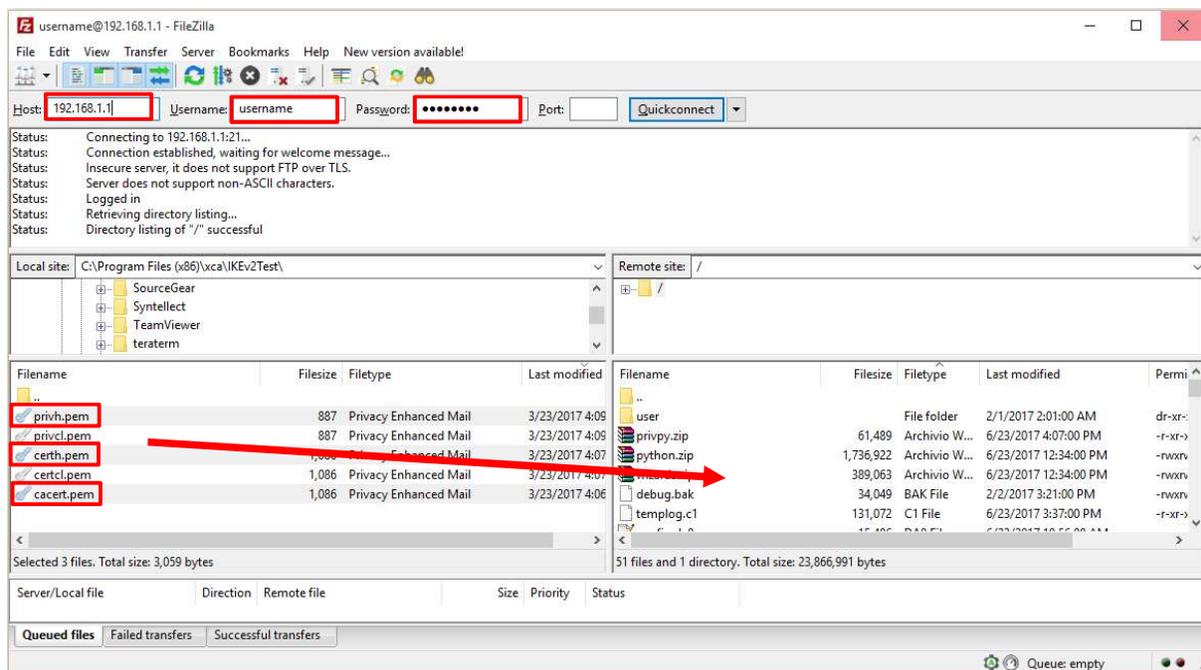
3.1.1 Upload Certificates and Keys

The upload of Certificates and Keys can be performed using an FTP client like Filezilla or using the TransPort WEB User Interface.

In this example, in order to upload the files, the connection to the Transport is done on the local LAN (so using the ETH o IP address of the router).

FTP:

Open an FTP connection (In this example, using FileZilla) to the TransPort router that acts as responder and Transfer the certificates and Key files to the root directory:



How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Where:

Parameter	Setting	Description
Host	192.168.1.1	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)
cacert.pem	-	CA Root certificate
certh.pem	-	Host Certificate
privh.pem	-	Host Private Key

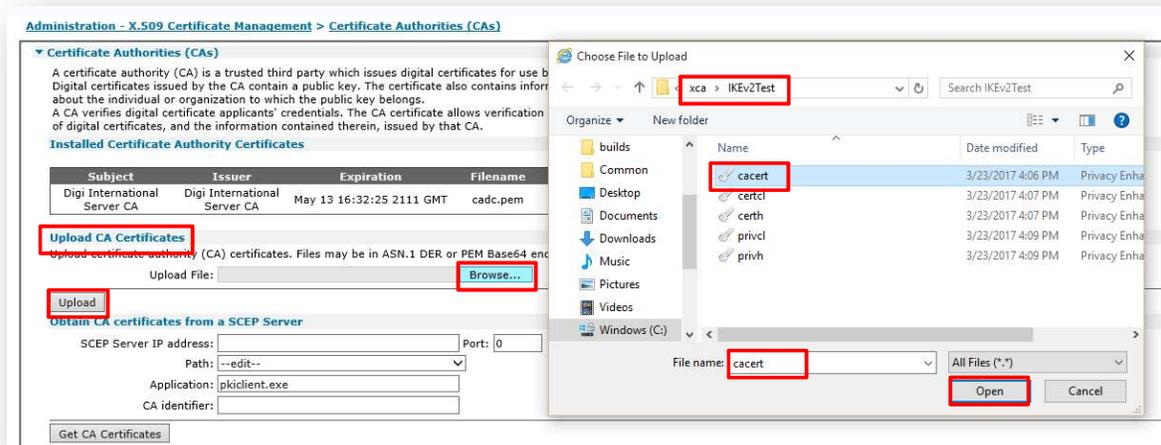
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Web GUI:

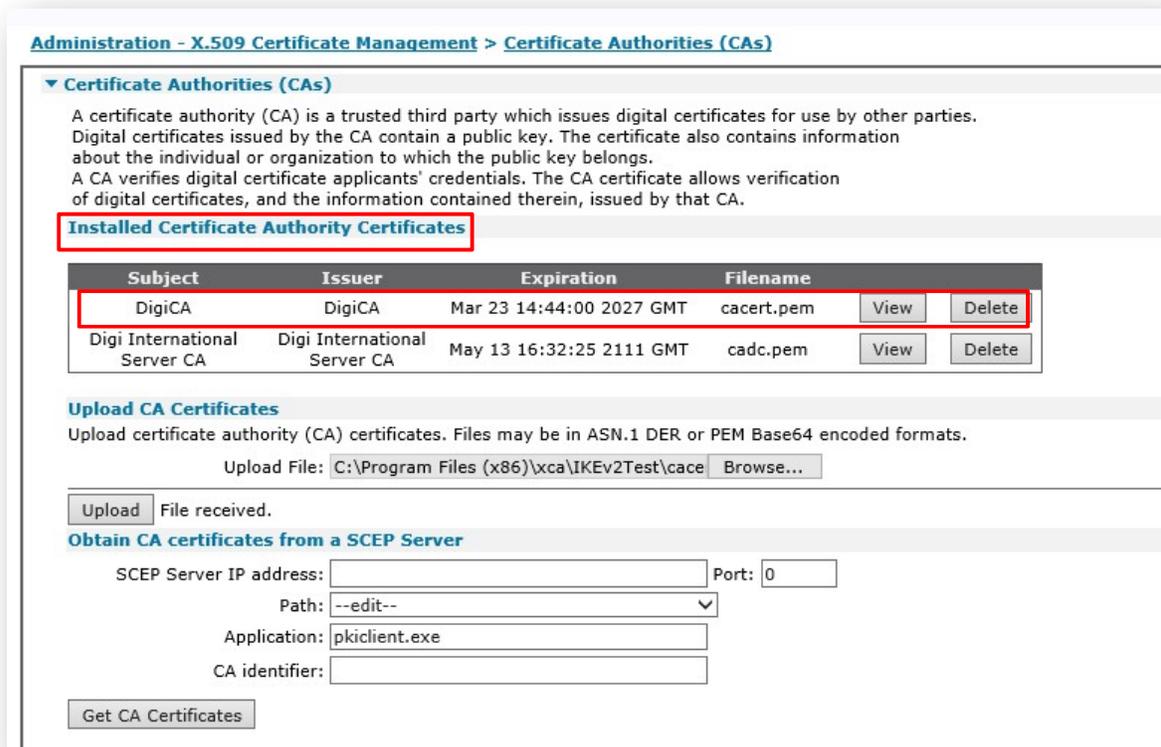
Open a web browser to the IP address of the TransPort router that acts as responder and do the following steps to upload each file:

ADMINISTRATION > X.509 CERTIFICATE MANAGEMENT > CERTIFICATE AUTHORITIES (CAs)

In the “Upload CA Certificates” section, click the “Browse” button, go to the file location where **cacert.pem** is located, select the file, click “Open” and then click **Upload**:



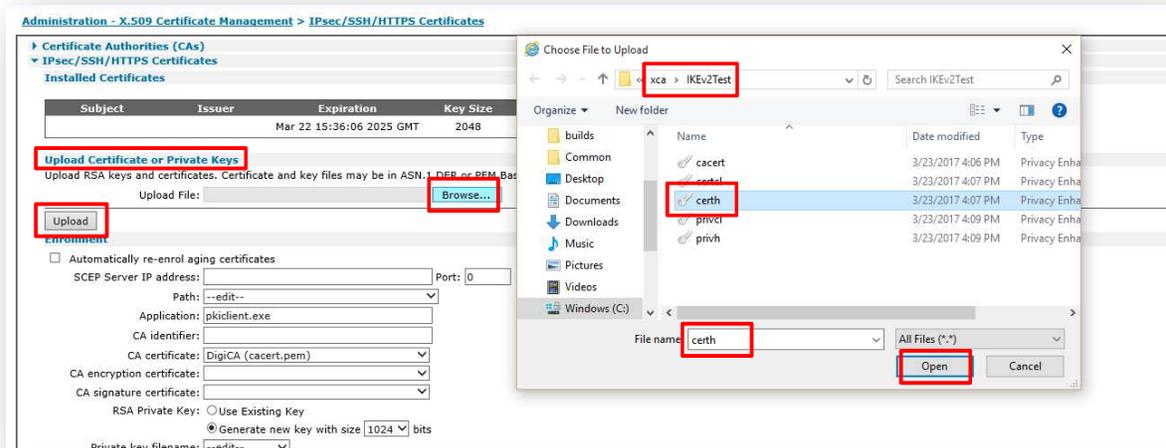
The **CA Certificate** should now appear under the **Installed Certificate Authority Certificates**



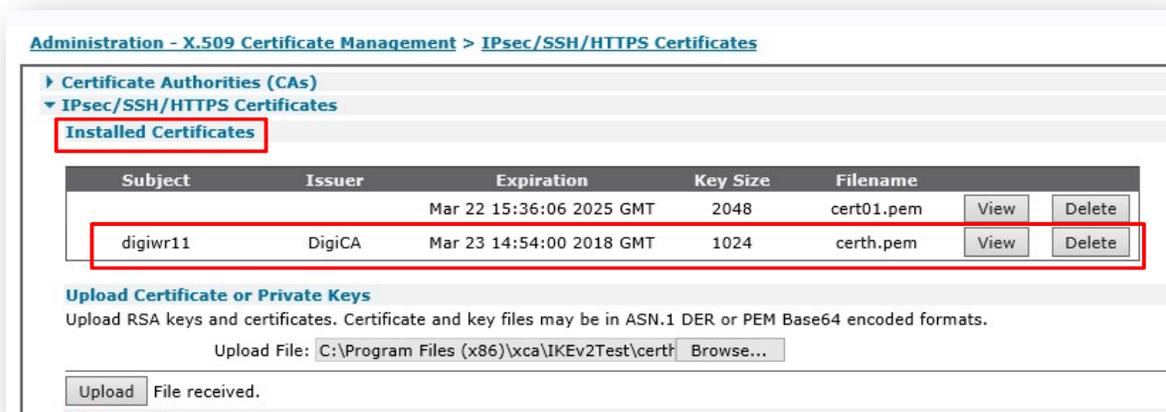
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

ADMINISTRATION > X.509 CERTIFICATE MANAGEMENT > IPSEC/SSH/HTTPS CERTIFICATES

In the **“Upload Certificates or Private Keys”** section, click the **“Browse”** button, go to the file location where **certh.pem** is located, select the file, click **“Open”** and then click **“Upload”**:



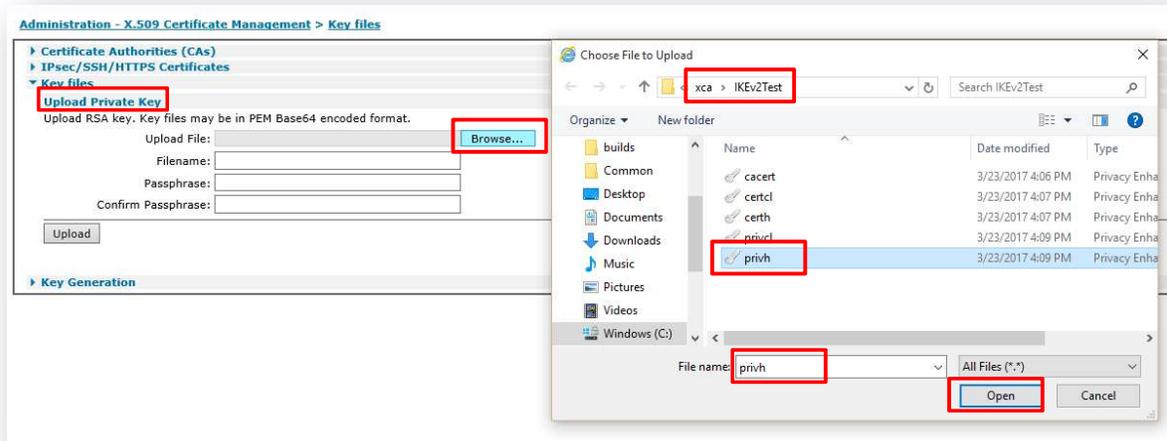
The Certificate should now appear under the **Installed Certificates**:



How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

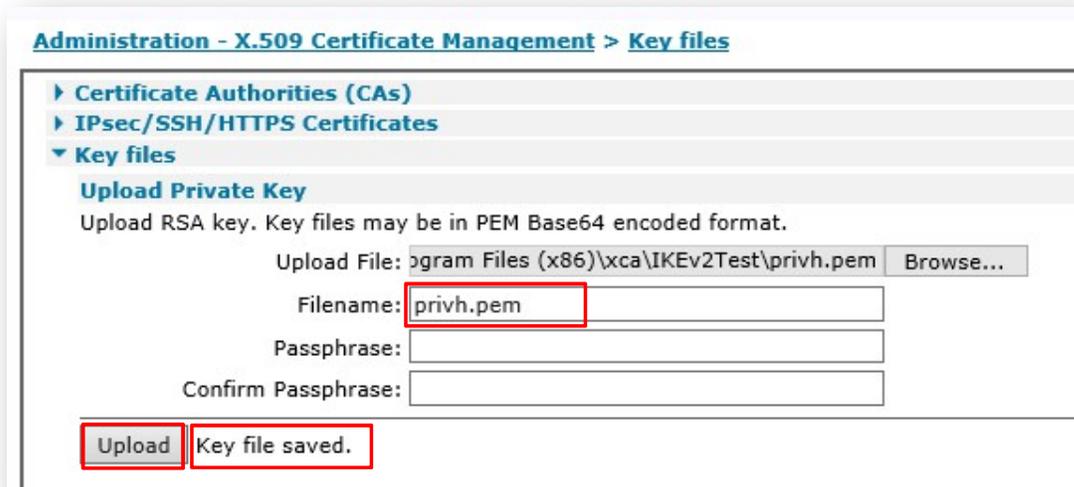
ADMINISTRATION > X.509 CERTIFICATE MANAGEMENT > KEY FILES

In the “**Upload Private Key**” section, click the “**Browse**” button, go to the file location where **privh.pem** is located, select the file, click “**Open**”



Type the file name “**privh.pem**” in the Filename field and click on “**Upload**”.

Before leaving the page, wait for the message “**Key file saved**” to be displayed to be sure that the upload is successful:



3.1.2 VPN Configuration

In this example the WAN Interface of the responder is the Mobile one, so on the PPP 1 interface the IPsec must be enabled:

CONFIGURATION – NETWORK > INTERFACES > MOBILE

Configuration - Network > Interfaces > Mobile

Service Plan / APN:

Use backup APN Retry the main APN after minutes

SIM PIN: (Optional)

Confirm SIM PIN:

Username: (Optional)

Password: (Optional)

Confirm Password:

Mobile Connection Settings

Re-establish connection when no data is received for a period of time

Mobile Network Settings

Enable NAT on this interface
● IP address ○ IP address and Port

Enable IPsec on this interface

Parameter	Setting	Description
Service Plan/APN	internet	Enter the APN of your mobile provider
Enable IPsec on this interface	✓	Enable IPsec on PPP 1 interface

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Then, the IPsec tunnel must be configured with the following settings:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 0-9 > IPSEC 0

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

IPsec Tunnels
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	<input checked="" type="radio"/> Use these settings for the remote LAN
IP Address: <input type="text" value="192.168.1.0"/>	IP Address: <input type="text" value="192.168.10.0"/>
Mask: <input type="text" value="255.255.255.0"/>	Mask: <input type="text" value="255.255.255.0"/>
<input type="radio"/> Use interface <input type="text" value="PPP"/> <input type="text" value="0"/>	<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

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Parameter	Setting	Description
Description	Ikev2 with Certs	Description of the IPsec tunnel
Local LAN IP Address	192.168.1.0	Use this IP address for the local LAN subnet. This is usually the IP address of the router's Ethernet interface or that of a specific device on the local subnet
Local LAN Mask	255.255.255.0	Use this IP mask for the local LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Remote LAN IP Address	192.168.10.0	Use this IP address for the remote LAN subnet. This is usually the IP address of the peer's Ethernet interface or that of a specific device on the local subnet
Remote LAN Mask	255.255.255.0	Use this IP mask for the remote LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Use the following security on this tunnel	RSA Signatures	Select RSA signature security for this tunnel to use the uploaded certificates
RSA Key File	privh.pem	Private key file used for the responder
Our ID	digjwr11	ID that is matching the CN of the certificate in the first router (responder)
Our ID type	IKE ID	Defines how the remote peer is to process the Our ID configuration. Set to IKE ID to match the information used in the certificate
Remote ID	digjwr21	Remote ID that is matching the CN in the second router certificate (initiator)
Use () encryption on this tunnel	AES (256 bit keys)	The ESP encryption protocol to use with this IPsec tunnel
Use () Authentication on this tunnel	SHA1	The ESP authentication algorithm to use with this IPsec tunnel
Use Diffie Hellman group ()	2	The Diffie Hellman (DH) group to use when negotiating new IPsec SAs.
Use IKE n to negotiate this tunnel	v2	The IKE version to use to negotiate this IPsec tunnel.
Use IKE configuration	0	The IKE configuration instance to use with this Eroute when the router is configured as an Initiator (so left as default in this case, it makes no difference as this router will no act as initiator)
Bring this tunnel up	On Demand	Controls how the IPsec tunnel is brought up.
If this tunnel is down and a packet is ready to be sent	Drop the packet	Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Then, the IKEv2 responder section must be configured with the following settings:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IKEv2 > IKEv2 RESPONDER and > ADVANCED

▼ IKEv2

- ▶ IKEv2 0
- ▶ IKEv2 1
- ▶ IKEv2 2
- ▶ IKEv2 3
- ▶ IKEv2 4
- ▼ **IKEv2 Responder**
 - Enable IKEv2 Responder
 - Accept IKEv2 Requests with
 - Encryption: DES 3DES AES (128 bit) AES (192 bit) AES (256 bit)
 - Authentication: MD5 SHA1 SHA256
 - PRF Algorithm: MD5 SHA1 SHA256
 - MODP Group between: 1 (768) and 2 (1024)
 - Renegotiate after 8 hrs 0 mins 0 secs
 - Rekey after 0 hrs 0 mins 0 secs
 - ▼ **Advanced**
 - Stop IKE negotiation if no packet received for 30 seconds
 - Enable Dead Peer Detection
 - Enable NAT-Traversal
 - NAT traversal keep-alive interval: 20 seconds
 - RSA private key file:

Parameter	Setting	Description
Encryption	AES (256 bit)	Defines the encryption algorithm used
Authentication	SHA1	Defines the authentication algorithm used.
PRF Algorithm	SHA1	Defines the PRF (Pseudo Random Function) algorithm used
MODP Group between x and y	1(778) and 2(1024)	The acceptable range for MODP group.
Advanced > RSA private key file	privh.pem	The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. In this case is the Private key file used for the responder

3.2 Initiator configuration

The Initiator configuration consists in uploading the certificates and the keys on the router, and then set UP the IKEv2 VPN to use them in the negotiation with the Responder. All these aspects will be explained in the subsections below.

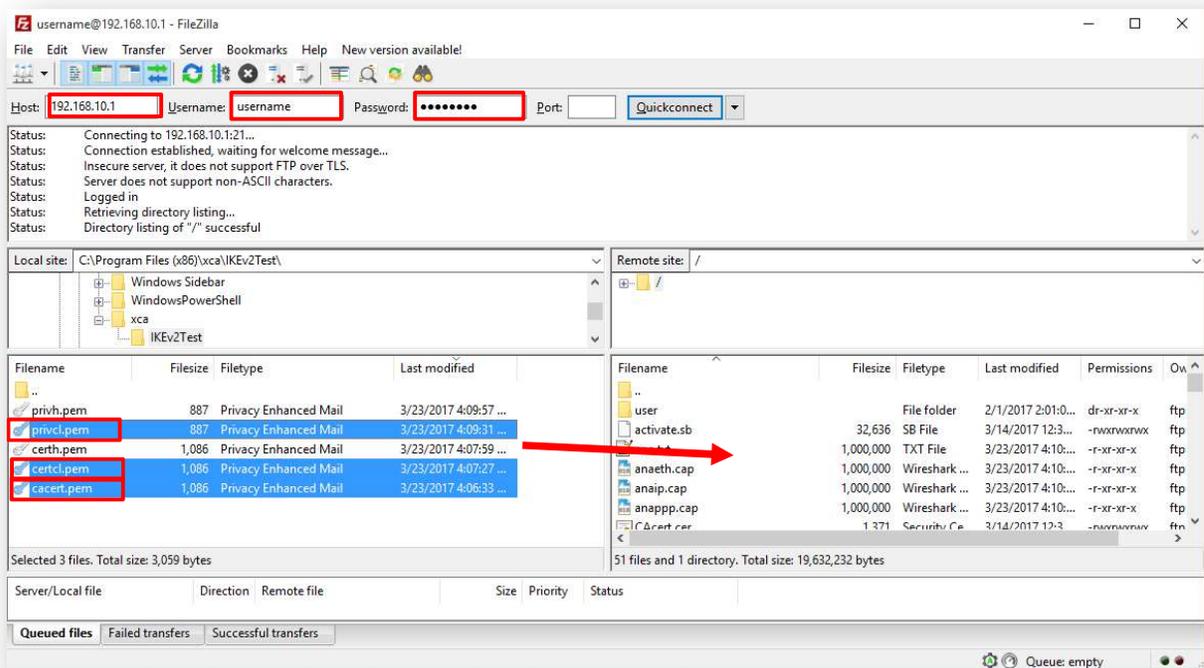
3.2.1 Upload Certificates and Keys

The upload of Certificates and Keys can be performed using an FTP client like Filezilla or using the TransPort WEB User Interface.

In this example, in order to upload the files, the connection to the Transport is done on the local LAN (so using the ETH o IP address of the router).

FTP:

Open an FTP connection (In this example, using FileZilla) to the TransPort router that acts as initiator and transfer the certificates and Key files to the root directory:



How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Where:

Parameter	Setting	Description
Host	192.168.10.1	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)
cacert.pem	-	CA Root certificate
certcl.pem	-	Host Certificate
privcl.pem	-	Host Private Key

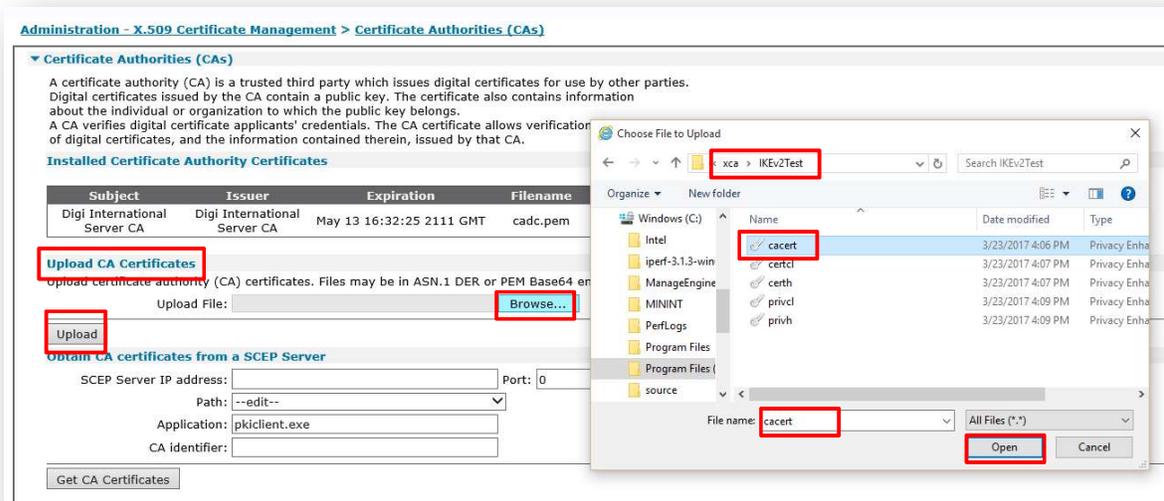
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Web GUI:

Open a web browser to the IP address of the TransPort router that acts as initiator and do the following steps to upload each file:

ADMINISTRATION > X.509 CERTIFICATE MANAGEMENT > CERTIFICATE AUTHORITIES (CAs)

In the “**Upload CA Certificates**” section, click the “**Browse**” button, go to the file location where **cacert.pem** is located, select the file, click “**Open**” and then click **Upload**:



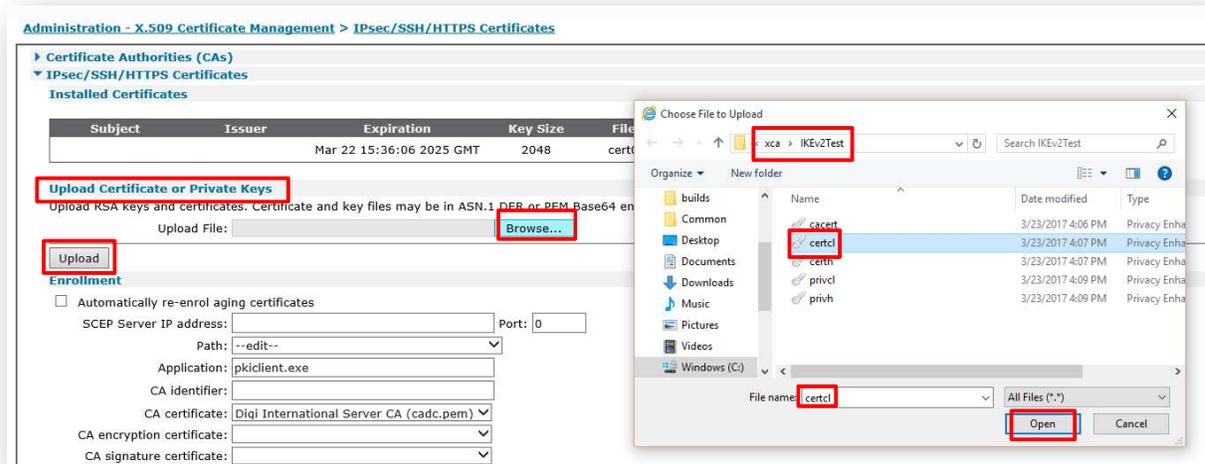
The **CA Certificate** should now appear under the **Installed Certificate Authority Certificates**



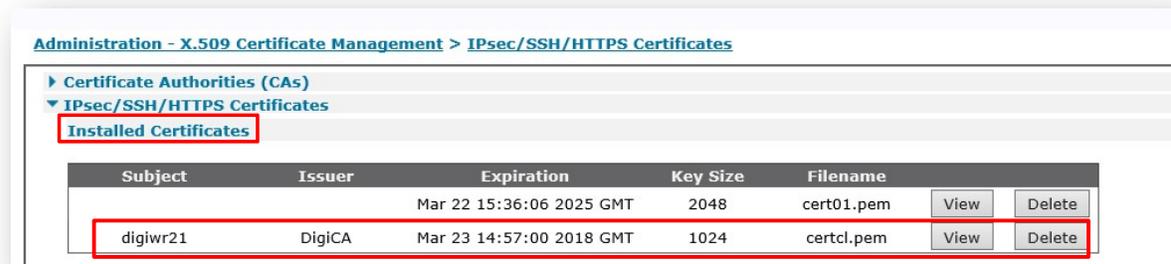
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

ADMINISTRATION > X.509 CERTIFICATE MANAGEMENT > IPSEC/SSH/HTTPS CERTIFICATES

In the “**Upload Certificates or Private Keys**” section, click the “**Browse**” button, go to the file location where **certcl.pem** is located, select the file, click “**Open**” and then click “**Upload**”:



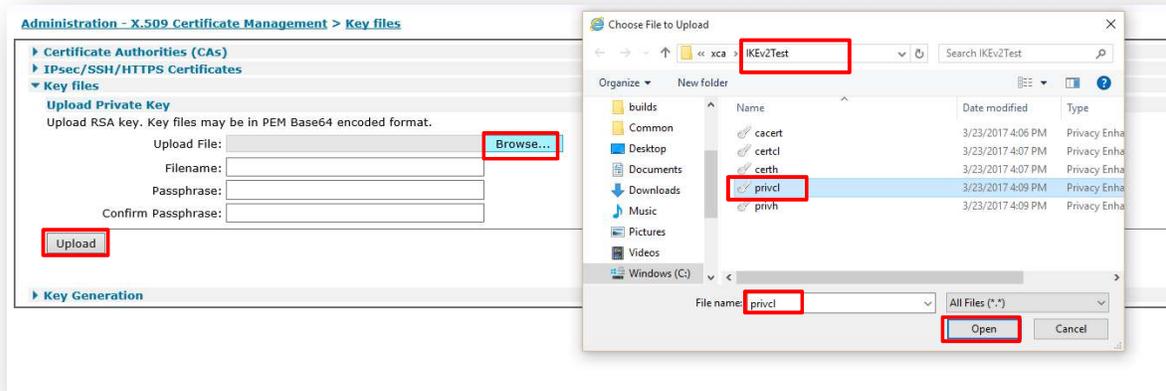
The Certificate should now appear under the **Installed Certificates**:



How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

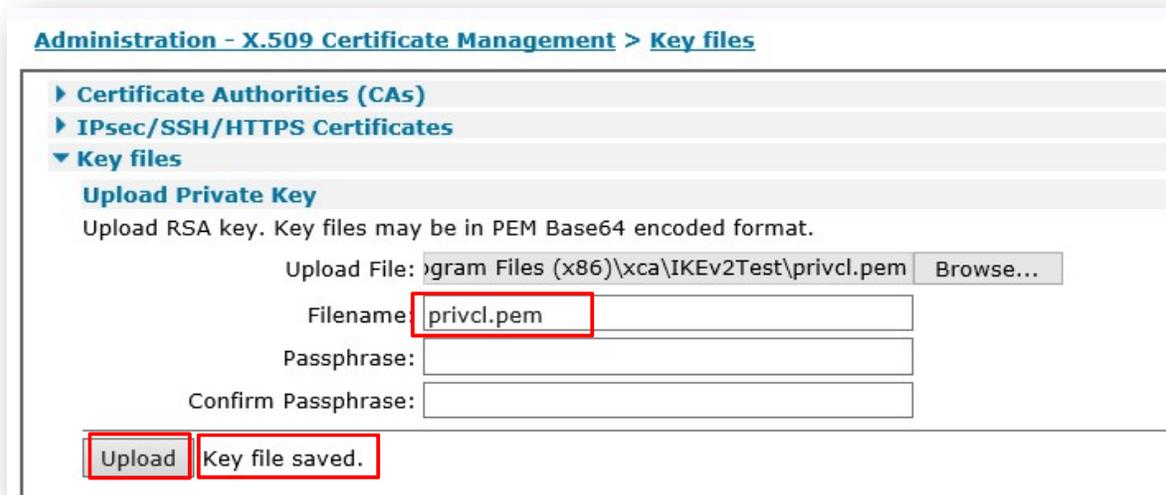
ADMINISTRATION > X.509 CERTIFICATE MANAGEMENT > KEY FILES

In the “**Upload Private Key**” section, click the “**Browse**” button, go to the file location where **privcl.pem** is located, select the file, click “**Open**”



Type the file name “**privcl.pem**” in the Filename field and click on “**Upload**”.

Before leaving the page, wait for the message “**Key file saved**” to be displayed to be sure that the upload is successful:



3.2.2 VPN Configuration

In this example the WAN Interface of the responder is the Mobile one, so on the PPP 1 interface the IPsec must be enabled:

CONFIGURATION - NETWORK > INTERFACES > MOBILE

Configuration - Network > Interfaces > Mobile

Service Plan / APN:

Use backup APN Retry the main APN after minutes

SIM PIN: (Optional)

Confirm SIM PIN:

Username: (Optional)

Password: (Optional)

Confirm Password:

Mobile Connection Settings

Re-establish connection when no data is received for a period of time

Mobile Network Settings

Enable NAT on this interface

IP address IP address and Port

Enable IPsec on this interface

Parameter	Setting	Description
Service Plan/APN	internet	Enter the APN of your mobile provider
Enable IPsec on this interface	✓	Enable IPsec on PPP 1 interface

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Then, the IPsec tunnel must be configured with the following settings:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 0-9 > IPSEC 0

IPsec Tunnels
IPsec 0 - IKEv2 with Certs

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	<input checked="" type="radio"/> Use these settings for the remote LAN
IP Address: <input type="text" value="192.168.10.0"/>	IP Address: <input type="text" value="192.168.1.0"/>
Mask: <input type="text" value="255.255.255.0"/>	Mask: <input type="text" value="255.255.255.0"/>
<input type="radio"/> Use interface <input type="text" value="PPP"/> <input type="text" value="0"/>	<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

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Where:

Parameter	Setting	Description
Description	Ikev2 with Certs	Description of the IPsec tunnel
The IP address or hostname of the remote unit	37.85.24.187	The IP address or hostname of the remote IPsec peer that a VPN will be initiated to.
Local LAN IP Address	192.168.10.0	Use this IP address for the local LAN subnet. This is usually the IP address of the router's Ethernet interface or that of a specific device on the local subnet
Local LAN Mask	255.255.255.0	Use this IP mask for the local LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Remote LAN IP Address	192.168.1.0	Use this IP address for the remote LAN subnet. This is usually the IP address of the peer's Ethernet interface or that of a specific device on the local subnet
Remote LAN Mask	255.255.255.0	Use this IP mask for the remote LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Use the following security on this tunnel	RSA Signatures	Select RSA signature security for this tunnel to use the uploaded certificates
RSA Key File	privcl.pem	Private key file used for the responder
Our ID	digiwr21	ID that is matching the CN of the certificate in the first router (initiator)
Our ID type	IKE ID	Defines how the remote peer is to process the Our ID configuration. Set to IKE ID to match the information used in the certificate
Remote ID	digiwr11	Remote ID that is matching the CN in the second router certificate (responder)
Use () encryption on this tunnel	AES (256 bit keys)	The ESP encryption protocol to use with this IPsec tunnel
Use () Authentication on this tunnel	SHA1	The ESP authentication algorithm to use with this IPsec tunnel
Use Diffie Hellman group ()	2	The Diffie Hellman (DH) group to use when negotiating new IPsec SAs.
Use IKE n to negotiate this tunnel	v2	The IKE version to use to negotiate this IPsec tunnel.
Use IKE configuration	0	The IKE configuration instance to use with this Eroute when the router is configured as an Initiator
Bring this tunnel up	All the time	This controls how the IPsec tunnel is brought up, for the initiator "All the time" option is chosen
If this tunnel is down and a packet is ready to be sent	Bring the tunnel up	Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent. For the initiator in this AN the "bring the tunnel up" option is chosen

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

CONFIGURATION – NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IKEv2 > IKEv2 0 and > ADVANCED

▼ IKEv2
▼ IKEv2 0

Use the following settings for negotiation

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

Authentication: None MD5 SHA1 SHA256

PRF Algorithm: None MD5 SHA1 SHA256

MODP Group for Phase 1: 2 (1024) ▼

Renegotiate after 8 hrs 0 mins 0 secs

Rekey after 0 hrs 0 mins 0 secs

▼ Advanced

Retransmit a frame if no response after 10 seconds

Stop IKE negotiation after 3 retransmissions

Stop IKE negotiation if no packet received for 30 seconds

Enable Dead Peer Detection

Enable NAT-Traversal

NAT traversal keep-alive interval: 20 seconds

RSA private key file: privcl.pem

Apply

Parameter	Setting	Description
Encryption	AES (256 bit)	The encryption algorithm used
Authentication	SHA1	The authentication algorithm used
PRF Algorithm	SHA1	The PRF (Pseudo Random Function) algorithm used
MODP Group for Phase 1	2 (1024)	Sets the key length used in the IKE Diffie-Hellman exchange to 768 bits (group 1) or 1024 bits (group 2). In this example group 2 is chosen to enable a 1024 bit key length
Advanced > RSA private key file	privcl.pem	The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. In this case is the Private key file used for the initiator.

4 TESTING

4.1 Check the IPsec tunnel is UP

This section will show that the IPsec tunnel has been established between the Initiator and the Responder.

The Event log will show the IKEv2 negotiation start and ends successfully in both routers:

MANAGEMENT - EVENT LOG

Initiator:

```

Management - Event Log
08:10:14, 24 Mar 2017, (2) IKEv2 Negotiation completed pe, Initiator
08:10:14, 24 Mar 2017, Eroute 0 VPN up peer: digiwr11
08:10:14, 24 Mar 2017, New IPsec SA created by digiwr11
08:10:14, 24 Mar 2017, (2) IKE Notification: AUTH_LIFETIME, RX
08:10:13, 24 Mar 2017, (2) IKE Keys Negotiated. Peer:
08:10:13, 24 Mar 2017, (2) IKE Notification: Initial Contact, RX
08:10:13, 24 Mar 2017, (2) IKE Notification: NATD dest. IP, RX
08:10:13, 24 Mar 2017, (2) IKE Notification: NATD source IP, RX
08:10:10, 24 Mar 2017, (2) New IKEv2 Negotiation peer 37.85.24.187, Initiator (Init)
08:10:10, 24 Mar 2017, IKE Request Received From Eroute 0
    
```

Responder:

```

Management - Event Log
08:10:51, 24 Mar 2017, WEB Login OK by username lvl 0
08:10:13, 24 Mar 2017, (1) IKEv2 Negotiation completed pe, Responder
08:10:13, 24 Mar 2017, Eroute 0 VPN up peer: digiwr21
08:10:13, 24 Mar 2017, New IPsec SA created by digiwr21
08:10:12, 24 Mar 2017, (1) IKE Keys Negotiated. Peer:
08:10:12, 24 Mar 2017, (1) IKE Notification: Initial Contact, RX
08:10:12, 24 Mar 2017, (1) IKE Notification: NATD dest. IP, RX
08:10:12, 24 Mar 2017, (1) IKE Notification: NATD source IP, RX
08:10:12, 24 Mar 2017, (0) New IKEv2 Negotiation peer 37.81.60.128, Responder (Init)
    
```

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

After that, in the connections status section IPsec and IKE v2 SAs will be displayed:

MANAGEMENT - CONNECTIONS > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS

Initiator:

▼ IPsec Tunnels

Outbound V1 SAs
No Tunnels

Inbound V1 SAs
No Tunnels

Outbound V2 SAs

#	Peer IP	First Rem. IP	Last Rem. IP	First Loc. IP	Last Loc. IP	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left	Interface	
0	37.85.24.187	192.168.1.0	192.168.1.255	192.168.10.0	192.168.10.255	N/A	SHA1	AES(256)	N/A	0	0	28732	PPP 1	Remove

Remove All

Inbound V2 SAs

#	Peer IP	First Rem. IP	Last Rem. IP	First Loc. IP	Last Loc. IP	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left	Interface	
0	37.85.24.187	192.168.1.0	192.168.1.255	192.168.10.0	192.168.10.255	N/A	SHA1	AES(256)	N/A	0	0	28732	PPP 1	Remove

Remove All Refresh

Responder:

▼ IPsec Tunnels

Outbound V1 SAs
No Tunnels

Inbound V1 SAs
No Tunnels

Outbound V2 SAs

#	Peer IP	First Rem. IP	Last Rem. IP	First Loc. IP	Last Loc. IP	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left	Interface	
0	37.81.60.128	192.168.10.0	192.168.10.255	192.168.1.0	192.168.1.255	N/A	SHA1	AES(256)	N/A	0	0	28694	PPP 1	Remove

Remove All

Inbound V2 SAs

#	Peer IP	First Rem. IP	Last Rem. IP	First Loc. IP	Last Loc. IP	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left	Interface	
0	37.81.60.128	192.168.10.0	192.168.10.255	192.168.1.0	192.168.1.255	N/A	SHA1	AES(256)	N/A	0	0	28694	PPP 1	Remove

Remove All Refresh

MANAGEMENT - CONNECTIONS > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IKE SAS

Initiator:

▼ IKE SAs

IKEv1 SAs
No SAs

IKEv2 SAs

Peer ID	Peer IP	Our IP	Session ID	Rekeys	Auth Alg	Enc Alg	Time Left (secs)	Internal ID	
digiwr11	37.85.24.187	37.81.60.128	0x2	0	SHA1	AES (256)	28711	2	Remove

Refresh Remove All V2 SAs

Responder:

▼ IKE SAs

IKEv1 SAs
No SAs

IKEv2 SAs

Peer ID	Peer IP	Our IP	Session ID	Rekeys	Auth Alg	Enc Alg	Time Left (secs)	Internal ID	
digiwr21	37.81.60.128	37.85.24.187	0x1	0	SHA1	AES (256)	28675	1	Remove

Refresh Remove All V2 SAs

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

In case of issues in the negotiation, take an IKE/IPsec trace following this guide: http://ftp1.digi.com/support/documentation/QN_045_How_To_setup_analyser_To_Get_IKE_IPsec_trace.pdf.

Please note that debug settings section for IKE, even if using IKEv2, is under general IKE configuration, as there is not a specific one for v2.

4.2 Check the Traffic passes through the IPsec tunnel

This section will show traffic passing across the tunnel. An easy way to test it, is to make a PING from a laptop connected to the ETH of the Initiator to one connected behind the responder. Before do that, to check how this traffic is handled by the router, the analyser section in the initiator router (but the same can be done on the responder) must be configured as follows:

MANAGEMENT - ANALYSER > SETTINGS

Management - Analyser > Settings

Settings

- Enable Analyser
 - Maximum packet capture size: bytes
 - Log size: Kbytes
- Protocol layers**
 - Layer 1 (Physical)
 - Layer 2 (Link)
 - Layer 3 (Network)
 - XOT
- Enable IKE debug
- Enable QMI trace
- LAPB Links**
 - LAPB 0 LAPB 1
- Serial Interfaces**
 - ASY 0 ASY 1 ASY 2 ASY 3 ASY 5
 - ASY 6 ASY 7 ASY 8 ASY 9 ASY 10
 - ASY 11 ASY 12 ASY 13 ASY 14 ASY 15
 - ASY 16 ASY 17 W-WAN
- Ethernet Interfaces**
 - ETH 0 ETH 1 ETH 2 ETH 3 ETH 4
 - ETH 5 ETH 6 ETH 7 ETH 8 ETH 9
- PPP Interfaces**
 - PPP 0 PPP 1 PPP 2 PPP 3 PPP 4
 - PPP 5 PPP 6 PPP 7
- IP Sources**
 - ETH 0 ETH 1 ETH 2 ETH 3 ETH 4
 - ETH 5 ETH 6 ETH 7 ETH 8 ETH 9
 - OVPN 0 OVPN 1 OVPN 2
 - PPP 0 PPP 1 PPP 2 PPP 3 PPP 4
 - PPP 5 PPP 6 PPP 7

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Once the analyser is configured, do the ping from the laptop on initiator side:

```
Select Administrator: Command Prompt

C:\windows\system32>ping 192.168.1.101 -n 1

Pinging 192.168.1.101 with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time=924ms TTL=126

Ping statistics for 192.168.1.101:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 924ms, Maximum = 924ms, Average = 924ms

C:\windows\system32>
```

Then, check the trace, it will show that the ICMP request/reply packets will be sent through the tunnel 0:

MANAGEMENT - ANALYSER > TRACE

```
----- 24-3-2017 08:28:10.110 -----
 45 00 00 3C 75 1B 00 00 80 01 38 8C C0 A8 0A 64      E..<u.....8....d
C0 A8 01 65 08 00 0E 46 00 01 3F 15 61 62 63 64      ...e...F..?.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                  uvwabcdefghijklhi

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
75 1B      ID:             29979
00 00      Frag Offset:    0
          Congestion:     Normal
          May Fragment
          Last Fragment

80          TTL:           128
01          Proto:         ICMP
38 8C      Checksum:      14476
C0 A8 0A 64  Src IP:       192.168.10.100
C0 A8 01 65  Dst IP:       192.168.1.101
ICMP:
08          Type:          ECHO REQ
00          Code:          0
0E 46      Checksum:      17934
-----
----- 24-3-2017 08:28:10.110 -----
45 00 00 3C 75 1B 00 00 7F 01 39 8C C0 A8 0A 64      E..<u.....9....d
C0 A8 01 65 08 00 0E 46 00 01 3F 15 61 62 63 64      ...e...F..?.abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74      efghijklmnopqrst
```

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

```

75 76 77 61 62 63 64 65 66 67 68 69                               uvwabcdefghi

ER 0-digiwr11 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
75 1B                            ID:             29979
00 00                            Frag Offset:   0
                                Congestion:       Normal
                                                May Fragment
                                                Last Fragment
7F                               TTL:            127
01                               Proto:         ICMP
39 8C                            Checksum:    14732
C0 A8 0A 64                      Src IP:     192.168.10.100
C0 A8 01 65                      Dst IP:     192.168.1.101
ICMP:
08                               Type:        ECHO REQ
00                               Code:         0
0E 46                            Checksum:    17934
-----
----- 24-3-2017 08:28:10.110 -----
45 00 00 78 00 1B 00 00 FA 32 20 58 25 51 3C 80   E..x.....2 X%Q<.
25 55 18 BB 86 65 7E 91 00 00 00 1B 24 B3 D5 85   %U...e~.....$.
C2 5B 0B 82 9C 49 AD AE C9 E9 A4 23 0E 46 7C F1   .[...I.....#.F|.
90 73 AB 4C 9B DA FF 7D 59 7C AE 8D AA 7B 90 BF   .s.L...}Y|...{..
33 3C 10 04 AC 7C 51 59 0F 54 CA A9 DA 80 5B 5F   3<...|QY.T....[_
82 DD 5A 44 71 47 70 FA AC D0 22 F4 E9 CA 8E 27   ..ZDqGp..."....'
2C 45 43 CB 93 4C C9 50 9E 09 CB DF D7 BC 63 25   ,EC..L.P.....c%
E0 23 EB 04 CB 54 CE 90                               .#...T..

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 78                            Length:          120
00 1B                            ID:             27
00 00                            Frag Offset:   0
                                Congestion:       Normal
                                                May Fragment
                                                Last Fragment
FA                               TTL:            250
32                               Proto:         ESP
20 58                            Checksum:    8280
25 51 3C 80                      Src IP:     37.81.60.128
25 55 18 BB                      Dst IP:     37.85.24.187
-----
----- 24-3-2017 08:28:11.040 -----
45 00 00 78 00 15 00 00 F4 32 26 5E 25 55 18 BB   E..x.....2&^%U..
25 51 3C 80 AB 00 EC B3 00 00 00 15 22 15 C5 15   %Q<....."....
54 A9 77 EB 5E 0D 21 65 A0 CC 27 42 88 D3 2B 88   T.w.^!.e..'B..+.
22 C3 DB 74 E0 9E 7E 2C A3 F0 C0 7E 1C 5A 3B 41   "...t...~,...~.Z;A
1C C6 40 73 51 93 1A F7 A7 EB 8D 54 2E 55 E8 5B   ..@sQ.....T.U.[
B8 DE 62 7C 3B 6B 0E AE 93 40 99 2A 44 E2 51 B3   ..b|;k...@.*D.Q.
8E 14 44 EE C6 26 68 A7 14 69 12 C4 CD 25 86 F1   ..D..&h..i...%..
C8 10 37 E1 F9 F5 49 B6                               ..7...I.

```

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

```

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 15                      ID:        21
00 00                      Frag Offset: 0
                             Congestion:  Normal
                             May Fragment
                             Last Fragment

F4                          TTL:       244
32                          Proto:    ESP
26 5E                      Checksum: 9822
25 55 18 BB                Src IP:   37.85.24.187
25 51 3C 80                Dst IP:  37.81.60.128
-----
----- 24-3-2017 08:28:11.040 -----
45 00 00 3C 54 14 00 00 7F 01 5A 93 C0 A8 01 65      E..<T.....Z....e
C0 A8 0A 64 00 00 16 46 00 01 3F 15 61 62 63 64      ...d...F...?.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                  uvwabcdefghijklhi

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
54 14                      ID:      21524
00 00                      Frag Offset: 0
                             Congestion:  Normal
                             May Fragment
                             Last Fragment

7F                          TTL:      127
01                          Proto:    ICMP
5A 93                      Checksum: 23187
C0 A8 01 65                Src IP:   192.168.1.101
C0 A8 0A 64                Dst IP:  192.168.10.100
ICMP:
00                          Type:    ECHO REPLY
00                          Code:    0
16 46                      Checksum: 17942
-----
----- 24-3-2017 08:28:11.040 -----
45 00 00 3C 54 14 00 00 7E 01 5B 93 C0 A8 01 65      E..<T...~.[.....e
C0 A8 0A 64 00 00 16 46 00 01 3F 15 61 62 63 64      ...d...F...?.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                  uvwabcdefghijklhi

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

```

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

```
54 14          ID:          21524
00 00          Frag Offset: 0
                Congestion: Normal
                May Fragment
                Last Fragment
7E            TTL:          126
01            Proto:        ICMP
5B 93          Checksum:    23443
C0 A8 01 65    Src IP:         192.168.1.101
C0 A8 0A 64    Dst IP:         192.168.10.100
ICMP:
00            Type:         ECHO REPLY
00            Code:         0
16 46          Checksum:    17942
-----
```

CONFIGURATION FILES

This is the config.da0 file used for the purpose of this Application Note on the Responder side:

```
Command: config c show
Command result

eth 0 IPAddr "192.168.1.1"
eth 0 ipanon ON
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
ip 0 cidr ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 descr "IKEv2 with Certs"
eroute 0 peerid "digiwr21"
eroute 0 ourid "digiwr11"
eroute 0 locip "192.168.1.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "192.168.10.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 authmeth "RSA"
eroute 0 ikever 2
eroute 0 dhgroup 2
eroute 0 enckeybits 256
eroute 0 privkey "privh.pem"
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
sntp 0 server "time.devicecloud.com"
dyndns 0 ifent "default"
ppp 0 timeout 300
ppp 1 name "W-WAN (HSPA 3G)"
ppp 1 phonenum "*98*1#"
ppp 1 IPAddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 ipsec 1
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 ipanon ON
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
ftpcli 0 hostname "ftp1.digi.com"
ftpcli 0 directory "support/firmware/transport/radio_module_firmware/he910d"
ike2 0 rencalgs "AES"
ike2 0 renckeybits 256
ike2 0 rauthalgs "SHA1"
```

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

```
ike2 0 rprfalgs "SHA1"
ike2 0 rdhmaxgroup 2
ike2 0 privrsakey "privh.pem"
modemcc 0 info_asy_add 3
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "Internet.t-d1.de"
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
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 anon ON
ana 0 l2on OFF
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 tremto 1200
cmd 0 rcihttp ON
user 0 access 0
user 1 name "username"
user 1 epassword "KD51SVJDVg="
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
sslcli 0 verify 10
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
cloud 0 ssl ON

Power Up Profile: 0
OK
```

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

This is the config.da0 file used for the purpose of this Application Note on the Initiator side:

```
Command: config c show
Command result

eth 0 IPaddr "192.168.10.1"
eth 0 ipanon ON
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
ip 0 cidr ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 descr "IKEv2 with Certs"
eroute 0 peerip "37.85.24.187"
eroute 0 peerid "digiwr11"
eroute 0 ourid "digiwr21"
eroute 0 locip "192.168.10.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "192.168.1.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 authmeth "RSA"
eroute 0 nosa "TRY"
eroute 0 autosa 2
eroute 0 ikever 2
eroute 0 dhgroup 2
eroute 0 enckeybits 256
eroute 0 privkey "privcl.pem"
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
sntp 0 server "time.devicecloud.com"
dyndns 0 ifent "default"
ppp 0 timeout 300
ppp 1 name "W-WAN"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 ipsec 1
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 ipanon ON
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
ike2 0 iencalg "AES"
ike2 0 ienckeybits 256
ike2 0 idhgroup 2
ike2 0 privrsakey "privcl.pem"
modemcc 0 asy_add 4
modemcc 0 info_asy_add 2
```

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

```
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "Internet.t-d1.de"
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
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 anon ON
ana 0 l2on OFF
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
cmd 0 rcihttp ON
user 0 access 0
user 1 name "username"
user 1 epassword "KD51SVJDVg="
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
sslcli 0 verify 10
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
creq 0 digest "MD5"
scep 0 cafile "cadc.pem"
scep 0 keybits 1024
templog 0 mo_autooff ON
cloud 0 ssl ON

Power Up Profile: 0
OK
```