

Quick Note 63

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

Contents

1 Intr	roduction	3
1.1	Outline	3
1.2	Assumptions	3
1.3	Corrections	3
1.4	Version	3
2 Ger	nerate 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	i Routers Configuration	22
3.1	Responder configuration	22
3.1.	.1 Upload Certficates and Keys	22
3.1.	.2 VPN Configuration	27
3.2	Initiator configuration	31
3.2.	.1 Upload Certficates and Keys	31
3.2.	.2 VPN Configuration	36
4 Tes	ting	40
4.1	Check the IPsec tunnel is UP	40
4.2	Check the Traffic passes through the IPsec tunnel	42
Configur	ration 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 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: <u>tech.support@digi.com</u>.

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 ca be used. The first step is to download and install the latest release of XCA which can be found at: <u>http://sourceforge.net/projects/xca/</u>.

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:**

Op Re Set Clo	ven DataBase cent DataBases t as default Data <mark>B</mark> ase	Ctrl+O	Ceruncates	Templates	Revocation lists	
Re Set Clo	cent DataBases t as default DataBase	*				
Clo	t as default Database					New Certificate
Op	ose DataBase	Ctrl+F4				Export
	itions					Import
La	nguage	•				Show Details
Exi	t					Delete
						Import PKCS#12
						Import PKCS#7
						Plain View
					J	Zaumineeta Diviskooo ⁶ 9 Zina
					(scal)	

Chose a name for the Database and click "**Save**":

12 Internet					
Irganize 👻 New fol	der				== • (
Common 🔨	Name	Date modified	Туре	Size	
E Desktop	🕞 database4	3/16/2017 4:03 PM	XCA database	10 KB	
🗄 Documents 🗸	🕞 database3	3/16/2017 2:51 PM	XCA database	6 KB	
File name: den	nodatabase				
Save as type: XCA	Databases (*.xdb)				

Chose a password for the Database and click "**OK**":

vate Keys	Certificate signing requests Certificates Templates Revocation lists
	View Certificate
	Password
	Please enter a password, that will be used to encrypt your private keys in the database file: C:/Users/amingo/Documents/demodatabase.xdb #12
	# 7
	Password ••••••
	Repeat Password •••••••
	Exit OK Cancel
	3 Dinhores Jim

Under the "Certificates" tab, click on "New Certficate":

die keys – Ceru	icate signing requests	Cerunca	iempi	ates Revocation I	SIS
Internal name	commonName	CA	Serial	Expiry date	New Certificate
					Export
					Import
					Show Details
					Delete
					Import PKCS#12
					Import PKCS#7
					Plain View
				>	Zerminate Dingwas 7 Zine
			1	>	

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"

ource Cubiect Extensions Keyyungen	Notecno Advanced	
Subject Extensions Key usage	Neiscape Advanced	
Signing request		
Sign this Certificate signing request		Ψ.
Copy extensions from the request	Show request	
Modify subject of the request		
Signing		
Oreate a self signed certificate with the serial	1	
Use this Certificate for signing		7
	5 <u></u>	
ignature algorithm	SHA 1	•
Template for the new certificate		
[default] CA		*
	Apply extensions Apply si	biect Apply all
	(the second seco	select select

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

	Extensions	Key usage Ne	tscape	Advanced		
istinguished name	24				24	
nternal name	democa			organizationName	Digi	
ountryName	DE somestate		organizationalUnitName commonName	Support DigiCA		
tateOrProvinceName						
ocalityName	Munich			emailAddress	support@digi.com	
						Delete
						Delete

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@digi.com	Enter your organization general email address.

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

ew ke	у			
ase give a ey proper	a name to the ties	new key and select th	ne desired keysize	
lame	democa			
Keytype	RSA			•
Keysize	1024 bit			~

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

ii ce	Subject	Extensions	ney usage	Netscape	Advanced			
nterna ountry tateOr ocality!	l name Name ProvinceName Name	democ DE somes	X Certificate a	nd Key mana sfully created	gement the RSA private	× key 'democa' OK	t :@digi.com	
	Туј	pe			Conter	nt	E	Add
								Delete

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:

vate Keys Certificate s	ning requests Certificates Templates Revoca	tion lists
1-1	X Certificate and Key management	×
democa Digi	TA Successfully created the certificate 'de	emoca' New Certificate
		Export
	O	K Import
		Show Details
		Delete
		Import PKCS#12
		Import PKCS#7
		Diain Minus

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.

Private Keys	Certifi	cate <mark>sign</mark> ing requests	Certificate	s Templates	Revocation lists	
Internal	name democa	commonName DigiCA	CA 🖌 Yes	Serial Ex	xpiry date	New Certificate
		10				Export
						Import
						Show Details
						Delete
						Import PKCS#12
						Import PKCS#7
						Plain View
						Zoumineeta, Divistence Jim

2.2 Create a CA-Signed Host Certificate (Responder)

Under the "**Certificates**" tab, click again on "**New Certficate**" 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":

ource Subject Extensions Key usage	Netscape Advanced
Signing request	
Sign this Certificate signing request	Ť
Copy extensions from the request	Show request
Modify subject of the request	
Signing O Create a self signed certificate with the serial O Use this Certificate for signing	1 democa 👻
Signing O Create a self signed certificate with the serial O Use this Certificate for signing	1 democa 🔹
Signing Create a self signed certificate with the serial Use this Certificate for signing	1 democa 🗸
Signing O Create a self signed certificate with the serial Use this Certificate for signing gnature algorithm	1 democa 🔹
Signing Create a self signed certificate with the serial Use this Certificate for signing Ignature algorithm	1 democa 🔹
Signing O Create a self signed certificate with the serial Use this Certificate for signing ignature algorithm Template for the new certificate	1 democa 🔹
Signing Create a self signed certificate with the serial Use this Certificate for signing ignature algorithm Template for the new certificate [default] HTTPS_server	1 democa 🔹
Signing O Create a self signed certificate with the serial O Use this Certificate for signing ignature algorithm Template for the new certificate [default] HTTPS_server	1 democa SHA 1 Apply extensions Apply subject Apply all
Signing Create a self signed certificate with the serial Use this Certificate for signing ignature algorithm Template for the new certificate [default] HTTPS_server	1 SHA 1 Apply extensions Apply subject Apply all
Signing Create a self signed certificate with the serial Use this Certificate for signing ignature algorithm Template for the new certificate [default] HTTPS_server	1 democa SHA 1 Apply extensions Apply subject Apply all

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

	Extensions Key usa	ge Netscape	Advanced		
istinguished name	L]	Di-1	
	nostcert			Digi	
tateOrProvinceName	DE compostato			digiour 11	
calityName	Munich			digiwr11	
					Delete

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 <u>digiwr11</u> 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.

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

and the second se
8.
23

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

urce	Subject	Extensions	Key usage	Netscape	Advanced				
Distingui	shed name								
Internal	name	hostce	X Certificate a	nd Key mana	gement	×	(1
countryf	Name	DE	Succes	efully created	the RSA privat	e key 'hostcert	t2		ī.
stateOrF	ProvinceNan	ne somes	D	siany created	the tox privat	e key nostcen	1		1
ocalityN	lame 🖌	Munich				OK	:2@digi.com	n	1
ocancyra		the second se				and the second sec			
Cantyry									

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:

vate Keys Certificate signing requests Certificates Temolates Revocation lists Internal name comm Memoca DigiCA Successfully created the certificate 'hostcert' OK	New Certificate Export Import Show Details Delete Import PKCS#12 Import PKCS#7
---	--

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.

rivate Keys Cer	rtificate signing requests	Certificates	Templates	Revocation lists		
Internal na	me common	Name CA	Serial	Exp	New Certificate	
A he	ostcert digiwr11	No		02 2018-	Export	
					Import	
					Show Details	
					Delete	
					Import PKCS#12	
					Import PKCS#7	
					Plain View	
					Jarmineeta Diuskaado Jine)

2.3 Create a CA-Signed Client Certificate (Initiator)

Under the "**Certificates**" tab, click again on "**New Certficate**" 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":

eate x509 Certificate				1	-	1
urce Subject Extensions Key usage I	Netscape Advanced					
gning request						
] Sign this Certificate signing request						7 .
Copy extensions from the request			Show request			
Modify subject of the request						
ning) Create a self signed certificate with the serial 1) Use this Certificate for signing	democa				22	•
gning) Create a self signed certificate with the serial 1) Use this Certificate for signing ature algorithm	democa					
gning) Create a gelf signed certificate with the serial 1) Use this Certificate for signing ature algorithm	democa SHA 1					•
gning) Create a self signed certificate with the serial 1) Use this Certificate for signing ature algorithm molate for the new certificate	democa SHA 1					
gning) Create a self signed certificate with the serial 1) Use this Certificate for signing ature algorithm mplate for the new certificate default] HTTPS_client	democa SHA 1				,	
gning) Create a self signed certificate with the serial 1) Use this Certificate for signing ature algorithm mplate for the new certificate default] HTTPS_client	democa SHA 1	Apply ext	tensions Apply s	ubject	, Apply all	
gning) Create a self signed certificate with the serial 1) Use this Certificate for signing ature algorithm mplate for the new certificate default] HTTPS_client	democa SHA 1	Apply ext	tensions Apply s	ubject	Apply all	•
gning) Create a self signed certificate with the serial 1 Use this Certificate for signing nature algorithm emplate for the new certificate default] HTTPS_dient	democa SHA 1	Apply ext	tensions Apply s	ubject	Apply all	

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

urce Subject	Extensions Key usage Ne	letscape Advanced		
istinguished name	dientcert	organizationName	Digi	
countryName	DE	organizationalUnitName	support3	
tateOrProvinceName	somestate	commonName	digiwr21	
ocalityName	Munich	emailAddress	support3@digi.com	
Tvi		C		
21	pe	Content		Add
	JE	Content		Delete
	DE	Content		Delete

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 <u>digiwr21</u> will be used. This will be used as the router Identity for the IPSec tunnel settings on the initiator
Email Address	Support3@digi.com	Enter your organization general email address.

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

(Second
~

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

stina	uished name	Extensions	Rey usage	Netscape	Advanceu				
nterna ountry	al name yName	cliente d'	X Certificate ar	nd Key manag fully created	jement the RSA private	× key 'clientcert'	3		
cality	Name	Munic				- OK	3@digi.con	n	
	Тур	e			Conte	nt		Add	
								Delete	

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:

ivate Keys	Certificate sign	ina requests	Certificates	Templates	Revocation lists		
120000	<u>.</u>	– 🥜 X Certif	ficate and Key n	nanagement	× –		- 1
A A	democa	I 🝙 🗄	Successfully cre	ated the certi	icate 'clientcert'	New Certificate	
A	e clientce					Export	
八章	hostcert	c			ОК	Import	
		-				Show Details	
						Delete	

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.

vate Keys	Certificate sig	ning requests Certi	ficates Te	mplates	Revocation lists	
Intern	al name	commonName	CA	Serial	Exp	
ALL .	democa	DigiCA	🖌 Yes	01	2027-	New Certificate
A	clientce.	digiwr21	No	03	2018-	Export
A	hostcert	digiwr11	No	02	2018-	Import
						Show Details
						Delete
						Import PKCS#12
						Import PKCS#7
						Diain View

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":

rivate Keys	Certificate sign	ning requests	Certificates	Te	emplates	Revocatio	n lists		
Inter	nal name	common	Name (CA .	Serial	Exp			
~ A:	democa	DigiCA	~	Yes	01	L 2027-	-	New Certificate	
R	elientce	digiwr21	No		03	3 2018-		Export	
A	hostcert	digiwr11	No		02	2018-		Import	
								Show Details	
								Delete	
								Import PKCS#12	
								Import PKCS#7	
								Diain View	

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

vate Keys	Certificate si	gning requests	Certificates	Templates	Revocation lis	ts		
Inte	mal name	commonN	ame CA	Serial	Exp	New	Certificate	1
Nº G	X Certificate an	d Key managem	ent	/	11 2002	107501	?	×
C	ertificate e	export				-	a) Contractory 70	
Nar	me democa							
F	ilename C:/Prog	ram Eiles (v86)/vc	/IKEv2Test/cac	ert nem			1	
		ann neo (nooy) nei		er open	14			
P	EM Text format w	ith headers						
						Export Format		
					L	PEM (".crt)		-
					L L	ОК	Cancel	
						e a	Nurdeno6 7	tina)
					>			

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

100000000	s Certificate sig	ning requests Certifi	icates	Templates	Revocation list	ts					
Int	ernal name	commonName	CA	Serial	Exp	Nev	v Certificate				
1	X Certificate and	I Key management	- V-	- '	1 2022 11 1		? ×	F			
	2 72							-			
C	Certificate e	xport						F			
N	Name hostcert										
	Filename C:/Program Files (x86)/xca/IKEv2Test certh.pem										
	PEM Text format wi	th headers									
						Export Format					
						OK	Cancel				
					11			-			
						A C	Dividence & Jim				

	Certificate si	igning requests	Certifica	ates Te	mplates	Revocation	lists			
Inte	rnal name	common	Name	CA	Serial	Exp	N	ew Certificate		
10	X Certificate an	nd Key manager	ment			2023		? >	<	
								-		
C	ertificate e	export						A		
Na	me clientcert							-	1 =	
								T.	7 📃	
Ľ	Filename C:/Program Files (x86)/xca/IKEv2Test certcl.pem									
F	PEM Text format v	vith headers								
							Export Form	at		
							PEM (*.crt)	•		
							ОК	Cancel		
						11	3)	miler	-)	
							12	anno 1 fi	ina	

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:

	ite signing requi	ests	Certif	icates	100	Templates	Revocatio	on lists			
Internal name	Туре	Siz		Use		Password			New Kev		
clientcert	RSA	1024	bit		1 0	Common	_		inch incy	_	_
democa	RSA	1024	bit		1 0	Common			Export		
hostcert	RSA	1024	bit		1 (Common			Import		
								Im	port PFX (PKCS#)	12)	
									Show Details		
									Delete		T

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":

	eys Certificat	e signing requ	iests Cei	tificates	Templates	Revocation lists		
Int	ernal name	Туре	Size	Use	Password		New Key	
5 m	💣 X Certificate	and Key ma	nagement				? ×	
21	Eventer	ivete ker						
	Export pr	ivate key	(RSA					
	Name hostcert							
	Filename C:/F	Program Files (x86)/xca/IKE	v2Tes <mark>i</mark> /pri	vh.pem			
	Unencrypted p	rivate key in t	ext format			Export PEM pi	Format ivate (*.pem)	
							OK Cancel	

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:

- **cacert.pem** : CA root certificate
- certh.pem : Responder certificate
- certcl.pem : Initiator certificate
- privh.pem : Responder private key
- privcl.pem : Initator 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 Certficates 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:

🔁 username@192.168.1.1 - FileZilla							-		×
File Edit View Transfer Server	Bookmarks Help	New version available!							
#- *** 01	8 🛛 🛼 🏷 🗏	F 🔍 🧿 🧥							
Host: 192.168.1.1	e: username	Pass <u>w</u> ord:	Port:	Quickconnect -					
Status: Connecting to 192.168.1. Status: Connection established, i Status: Insecure server, it does no Status: Server does not support r Status: Logged in Status: Retrieving directory listin	1:21 waiting for welcome m ot support FTP over TL non-ASCII characters. g	nessage S.							^
Status: Directory listing of "/" su	ccessful								v
Local site: C:\Program Files (x86)\xca	a\IKEv2Test\		~	Remote site: /					~
BSourceGear BSyntellect BTeamViewer BTeamViewer			^	B /					
Filename	Filesize	Filetype	Last modified	Filename	Filesize	Filetype	Last modified	Per	rmi ^
anith nem	997	Privacy Enhanced Mail	3/23/2017 4:00			File folder	2/1/2017 2:01:00 AM	dre	-vr-
/ privel.pem	887	Privacy Enhanced Mail	3/23/2017 4:09	privov.zin	61 489	Archivio W	6/23/2017 4:07:00 PM	-1-1	×r->
d certh.pem		Enhanced Mail	3/23/2017 4:07	python.zip	1.736.922	Archivio W	6/23/2017 12:34:00 PM	-ги	VXEV
d certcl.pem	1,086	Privacy Enhanced Mail	3/23/2017 4:07		389,063	Archivio W	6/23/2017 12:34:00 PM	-пл	VXIV
d cacert.pem	1,086	Privacy Enhanced Mail	3/23/2017 4:06	debug.bak	34,049	BAK File	2/2/2017 3:21:00 PM	-ги	vxrv
		2		templog.c1	131,072	C1 File	6/23/2017 3:37:00 PM	-r-)	xr->
1				C 10	15 105	D 4 0 51	C /22 /2017 10 CC 00 +14		· ·
Selected 3 files. Total size: 3,059 bytes				51 files and 1 directory. To	tal size: 23,866,991 bytes				
Server/Local file Dire	ection Remote file		Size Priority Sta	tus					_
Queued files Failed transfers S	uccessful transfers								
							🔕 🕜 Queue: empty		•

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

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:**

Certificate Authorities (CAs)	Choose File to Upload				×
A certificate authority (CA) is a trusted third party which issues digital certificates for use b Digital certificates issued by the CA contain a public key. The certificate also contains inforr about the individual or organization to which the public key belongs.	← → ~ ↑ □	xca → IKEv2Test	ٽ ~	Search IKEv2Test	٩
A CA verifies digital certificate applicants' credentials. The CA certificate allows verification of digital certificates, and the information contained therein, issued by that CA.	Organize 🔻 🛛 New fo	older			
Installed Certificate Authority Certificates	📙 builds 🖌	^ Name	^	Date modified	Туре
Subject Issuer Expiration Filename	Common	🧭 cacert		3/23/2017 4:06 PM	Privacy Enha
Digi International Digi International May 13 16:32:25 2111 GMT cadc.pem	E Desktop	C certcl		3/23/2017 4:07 PM	Privacy Enha
Server CA Server CA	Documents	🖉 certh		3/23/2017 4:07 PM	Privacy Enha
Upload CA Certificates	Downloads	d privel		3/23/2017 4:09 PM	Privacy Enha
Upload certificate authorit y (CA) certificates. Files may be in ASN.1 DER or PEM Base64 enc	b Music	S privh		3/23/2017 4:09 PM	Privacy Enha
Upload File: Browse	Pictures				
Upload	Videos				
Obtain CA certificates from a SCEP Server	Windows (C)				
SCEP Server IP address: Port: 0	and mindows (ci)	~ <			,
Path:edit 🗸	File	e name: cacert	~	All Files (*.*)	~
Application: pkiclient.exe				Open	Cancel
CA identifier					

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

	es (CAs)				
A certificate authority Digital certificates issu- bout the individual of A CA verifies digital ce of digital certificates, a	(CA) is a trusted thir ued by the CA contain r organization to whice ertificate applicants' or and the information of	d party which issues digital cer a public key. The certificate al ch the public key belongs. redentials. The CA certificate al contained therein, issued by tha	tificates for use so contains info llows verification It CA.	by other par rmation 1	ties.
nstalled Certificate	Authority Certifica	tes			
Subject	Issuer	Expiration	Filename	12 1/2	200
DigiCA	DigiCA	Mar 23 14:44:00 2027 GMT	cacert.pem	View	Delete
Digi International Server CA	Digi International Server CA	May 13 16:32:25 2111 GMT	cadc.pem	View	Delete
pload CA Certificat	es				
pload CA Certificat pload certificate auth Uplo Upload File received	es ority (CA) certificates oad File: C:\Program d.	s. Files may be in ASN.1 DER or Files (x86)\xca\IKEv2Test\cace	r PEM Base64 er Browse	ncoded form	ats.
pload CA Certificat pload certificate auth Uplo Upload File receive obtain CA certificate	es oority (CA) certificate: oad File: C:\Program d. es from a SCEP Ser	s. Files may be in ASN.1 DER or Files (x86)\xca\IKEv2Test\cace ver	PEM Base64 er	ncoded forma	ats.

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**":

ertificate Authorities (CAs) Deer /SSH / HTTPS Certificates	Choose File to Upload		×
nstalled Certificates	← → → ↑ 📙 « xca → IKEv2Test	✓ Ö Search IKEv2Test	م
Subject Issuer Expiration Key Size	Organize 👻 New folder		• •
Mar 22 15:36:06 2025 GMT 2048	builds ^ Name ^	Date modified	Туре
pload Certificate or Private Keys	Common di cacert	3/23/2017 4:06 PM	Privacy Enha
pload RSA keys and certificates. Certificate and key files may be in ASN.1 DER or PEM Bas	Desktop	3/23/2017 4:07 PM	Privacy Enha
Upload File: Browse	Documents descent	3/23/2017 4:07 PM	Privacy Enha
Upload	Downloads Priver	3/23/2017 4:09 PM	Privacy Enha
nronment	Music Ø privh	3/23/2017 4:09 PM	Privacy Enha
Automatically re-enrol aging certificates	E Pictures		
SCEP Server IP address: Port: 0	Videos		
Path:edit 💙	Mindaux (C)		
Application: pkiclient.exe	windows (C:) V K		>
CA identifier:	File name certh	 All Files (*.*) 	~
CA certificate: DigiCA (cacert.pem)		Open	ancel
CA encryption certificate:		Open	lancer
CA signature certificate:			
RSA Private Key: OUse Existing Key			
Generate new key with size 1024 V bits			

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

ertificate Authoriti	es (CAs)					
sec/SSH/HTTPS C	Certificates					
stalled Certificate	5					
Subject	Теснов	Evpiration	Key Size	Filename	_	_
Subject	Issuer	Mar 22 15:36:06 2025 GMT	2048	cert01.pem	View	Delete
digiwr11	DigiCA	Mar 23 14:54:00 2018 GMT	1024	certh.pem	View	Delete
nland Cartificate o	- Drivata Kaus					
pload DEA kove and	cortificator, Cortifi	cate and key files may be in ASN 1	DEP or DEM R-	sof 4 anodad for	mate	
pioau KSA keys allu	ceruncates, cerun	cate and key mes may be in ASN.1	DEK OF PEM Da	iseo4 encoded for	nats.	
Uple	oad File: C:\Progra	am Files (x86)\xca\IKEv2Test\certh	Browse			

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**"

Certificate Authorities (CAs)		🦉 Choose File to Upload				×
Neer files Upload Private Key		← → · ↑	xca > IKEv2Test	ٽ ~	Search IKEv2Test	Q
Upload RSA key. Key files may be in PEM Base64 encoded format.		Organize 🔻 New fo	lder			• •
Upload File:	Browse	builds	Name	^	Date modified	Type
Filename:		Common	1.00		2/22/2017 A 05 PM	D F. h.
Passphrase:		Deskton	C cacert		3/23/2017 4:00 PIVI	Privacy Enna
Confirm Passphrase:		Decuments	erth		2/22/2017 4:07 PM	Privacy Enha
Upload		Developeda	an privel		3/23/2017 4:07 PM	Privacy Enha
		Downloads	el privh		3/23/2017 4:09 PM	Privacy Enha
Key Ceneration		J Music				
Key deneration		Pictures				
		Videos				
		Windows (C:)	, c			>
		File	name: privh	~	All Files (*.*)	~
		75.735			Open	Cancel
						.H.

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:

Certificate Authorities (CAs)	
IPsec/SSH/HTTPS Certificates	
r Key files	
Upload Private Key	
Upload RSA key. Key files may be in PEM Base64 encoded format.	
Upload File: pgram Files (x86)\xca\IKEv2Test\privh.pem	Browse
Filename: privh.pem	
Passphrase:	
Confirm Passphrase:	
Upload Key file saved.	

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

Use backup APN Retry the main APN after 0 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	
SIM PIN:(Optional) Confirm SIM PIN:(Optional) Username:(Optional) Password:(Optional) Confirm Password:(Optional) Confirm Password:(Optional) Mobile Connection Settings	minutes
Confirm SIM PIN:	
Username: (Optional) Password: (Optional) Confirm Password: (Optional) Mobile Connection Settings Re-establish connection when no data is received for a period of time Mobile Network Settings	
Password: (Optional) Confirm Password: Mobile Connection Settings Re-establish connection when no data is received for a period of time Mobile Network Settings	
Confirm Password:	
Mobile Connection Settings Re-establish connection when no data is received for a period of time Mobile Network Settings	
Mobile Connection Settings Re-establish connection when no data is received for a period of time Mobile Network Settings	
Re-establish connection when no data is received for a period of time Mobile Network Settings	
Mobile Network Settings	
Mobile Network Settings	
☑ Enable NAT on this interface	
● IP address ○ IP address and Port	

Parameter	Setting	Description		
Service	internet	Enter the APN of your mobile		
Plan/APN	internet	provider		
Enable IPSec		Enable IDSec on DDD 1		
on this	\checkmark	interface		
interface		interface		

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

Psec 0	
Description: IKEv2 with Certs	
The IP address or hostname of the remote unit	
Use	as a backup unit
Local LAN	Remote LAN
Ose these settings for the local LAN	Use these settings for the remote LAN
IP Address: 192.168.1.0	IP Address: 192.168.10.0
Mask: 255.255.255.0	Mask: 255.255.255.0
○ Use interface PPP 💙 0	O Remote Subnet ID:
Off OPreshared Keys OXAUTH Init Pre RSA Key File: privh.pem V Our ID: digiwr11 Our ID type ® IKE ID OFC Remote ID: digiwr21 Use AES (256 bit keys) V encryption on this tunnel Use SHA1 V euthentication on this tunnel Use Diffie Hellman group 2 V	shared Keys RSA Signatures OXAUTH Init RSA
Use IKE $v2 \vee$ to negotiate this tunnel Use IKE configuration: $0 \vee$	
Bring this tunnel up All the time Whenever a route to the destination is av On demand If the tunnel is down and a packet is ready to b	railable
Bring this tupped down if it is idle for 0	
Renew the tunnel after	

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	digiwr11	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	digiwr21	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

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

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

TKEv2
> IKEv2 0
▶ IKEv2 1
▶ IKEv2 2
FIKEv2 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
RSA private key file: privh.pem
Apply
1.564.1

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:

🔁 username@192	168.10.1 - FileZilla							- 0	×
File Edit View	Transfer Server Bookmarks Help New	version available!							
	T 🗱 🖸 比 🛛 🐛 🗊 🔳 🏛	i 🧧 🦓							
Host: 192.168.10.1	Username: Username Pa	ssword:	ort:	Quickconnect 👻					
itatus: Conne	cting to 192.168.10.1:21		22 2						-
tatus: Conne	ction established, waiting for welcome messa	ge							
tatus: insecul tatus: Server	does not support non-ASCII characters.								
tatus: Logged	lin								
itatus: Retriev	ing directory listing								
status: Directo	ry listing of 7 successful								4
Local site: C:\Prog	ram Files (x86)\xca\IKEv2Test\		~	Remote site: /					
	Windows Sidebar		^						
	WindowsPowerShell								
ė-	хса								
	IKEv2Test		~						
Filename	Filesize Filetype	Last modified		Filename	Filesize	Filetype	Last modified	Permissions	On ^
/ privh.pem	887 Privacy Enhanced Mail	3/23/2017 4:09:57		user		File folder	2/1/2017 2:01:0	dr-xr-xr-x	ftp
grīvcl.pem	887 Privacy Enhanced Mail	3/23/2017 4:09:31		activate.sb	32,636	SB File	3/14/2017 12:3	-rwxrwxrwx	ftp
🖉 certh.pem	1,086 Privacy Enhanced Mail	3/23/2017 4:07:59		EN	1,000,000	TXT File	3/23/2017 4:10:	-r-xr-xr-x	ftp
💕 certcl.pem	1,086 Privacy Enhanced Mail	3/23/2017 4:07:27		🔚 anaeth.cap	1,000,000	Wireshark	3/23/2017 4:10:	-r-xr-xr-x	ftp
💕 cacert.pem	1,086 Privacy Enhanced Mail	3/23/2017 4:06:33		🛅 anaip.cap	1,000,000	Wireshark	3/23/2017 4:10:	-r-xr-xr-x	ftp
				📑 anappp.cap	1,000,000	Wireshark	3/23/2017 4:10:	-r-xr-xr-x	ftp
				CAcert cer	1 371	Security Ce	3/14/2017 12-3	- 04/204/204/2	ftn
Selected 3 files. Total	size: 3,059 bytes			51 files and 1 directory. Total	size: 19,632,232 bytes				
Server/Local file	Direction Remote file	Size Pri	ority Sta	tus					
		and here							
Queued files Fa	iled transfers Successful transfers								

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

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:**

A certificate authority (CA) is a trusted thi Digital certificates issued by the CA contai about the individual or organization to whi C Q verifics digital certificate annicants!	rd party which issues digital cert n a public key. The certificate als ch the public key belongs. credentials. The CA certificate all	ificates for use so contains info lows verification	by other parties. mation				
of digital certificates, and the information	contained therein, issued by that	t CA.	😂 Choose File to Upload				×
Installed Certificate Authority Certifica	ites		← → • ↑ 🛄 « xe	ca → IKEv2Test	ٽ v	Search IKEv2Test	P
Subject Issuer	Expiration	Filename	Organize 👻 New fold	er			
Digi International Digi International Server CA Server CA	May 13 16:32:25 2111 GMT	cadc.pem	🔛 Windows (C:) \land	Name		Date modified	Туре
			Intel	🧭 cacert		3/23/2017 4:06 PM	Privacy Enha
Upload CA Certificates			iperf-3.1.3-win	€″ certcl		3/23/2017 4:07 PM	Privacy Enha
opioad certificate authority (CA) certificate	s. Files may be in ASN.1 DER or	PEM Base64 en	ManageEngine	d certh		3/23/2017 4:07 PM	Privacy Enha
Upload File:		Browse	MININT	🕜 privcl		3/23/2017 4:09 PM	Privacy Enha
nateral			PerfLogs	🦪 privh		3/23/2017 4:09 PM	Privacy Enha
opioad			Program Files				
obtain CA certificates from a SCEP Ser	ver	1	Program Files (
SCEP Server IP address:		Port: 0	source	1			
Path:edit	<u> </u>	<u>·</u>					
Application: pkiclient.ex	e		File r	iame: cacert	~	All Files (*.*)	~
CA identifier:						Open	Cancel

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

ertificate Authoritie	es (CAs)				
igital certificates iss bout the individual o CA verifies digital co	ued by the CA contain or organization to whice ertificate applicants' c	a public key. The certificate als the public key belongs. the public key belongs. tredentials. The CA certificate al	so contains infor	mation	es.
f digital certificates, Installed Certificate	and the information of Authority Certifica	contained therein, issued by that tes	t CA.		
digital certificates, stalled Certificate Subject	and the information of Authority Certifica	Expiration	t CA. Filename		
digital certificates, stalled Certificate Subject Digi International Server CA	and the information of Authority Certifica Issuer Digi International Server CA	Expiration May 13 16:32:25 2111 GMT	Filename cadc.pem	View	Delete

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**":

Certificate Authorities (CAs)									
IPsec/SSH/HTTPS Certifica	tes									
Installed Certificates					20.001					
Subject	(cenor	Expiration	Koy Sizo	Eile 🤮 C	noose File to Uplo	ad	_			×
Subject	M	ar 22 15:36:06 2025 GMT	2048	cert(-> · · 🕇 📙	< xca → IKEv2T	est	v Č Se	arch IKEv2Test	م
				Org	anize 👻 New	/ folder				. 0
Upload Certificate or Privat	e Keys	nd key files may be in ASN	1 DER or PEM Base	64 en	builds	↑ Name	^		Date modified	Туре
Upload Filos	les. certificate a	na key mes may be m Asia.	Browno	or en	Common	el cace	rt		3/23/2017 4:06 PM	Privacy Enha
opidad File.			Browse		Desktop	- Certo	1		3/23/2017 4:07 PM	Privacy Enha
Upload					Documents	C certi			3/23/2017 4:07 PM	Privacy Enha
Enrollment					Downloads	d prive	i		3/23/2017 4:09 PM	Privacy Enha
Automatically re-enrol ag	ing certificates				Music	S privi			3/23/2017 4:09 PM	Privacy Enha
SCEP Server IP address:			Port: 0		Pictures					
Path:	edit		~		Videos					
Application:	pkiclient.exe				Windows (C:)	× <				>
CA identifier:						Charles and a second	1		II () (* *)	
CA certificate:	Digi Internation	al Server CA (cadc.pem) 🗸	1		3	certo		A	in thes (,)	~
CA encryption certificate:		~	-						Open	Cancel
CA sizestus settificator		7 54	5							

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

cate Authoritie	s (CAs)					
SSH/HTTPS Co	ertificates					
ed Certificate	5					
Subject	Issuer	Expiration	Key Size	Filename		
		M 00 15-06-0005 CMT	2040		1/1	Delate

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**"

Certificate Authorities (CAs)	← → · · ↑ • « xca → IKEv2Test	y ♂ Search IKEv2Test Q
IPsec/SSH/HTTPS Certificates		
Key files	Organize 👻 New folder	8== 👻 🛄 🕝
Upload Private Key	builds ^ Name	Date modified Type
Upload RSA key. Key files may be in PEM Base64 encoded format.	Common	2/22/2017 4:05 PM
Upload File: Browse	Desktop d catch	3/23/2017 4:00 PM Privacy Enha
Filename:	Documents Certch	3/23/2017 4:07 PM Privacy Enha
Decembrace	L Downloads	3/23/2017 4:09 PM Privacy Enha
	Muric Orivh	3/23/2017 4:09 PM Privacy Enha
Confirm Passphrase:	- Distance	
Upload	Pictures	
	Videos	
	Windows (C:) V	• • • • • • • • • • • • • • • • • • •
• Key Generation	File name: privcl	✓ All Files (*.*) ✓
		Open Cancel

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:

Certificate Authorities (CAs)		
IPsec/SSH/HTTPS Certificat	tes	
Key files		
Upload Private Key		
Upload RSA key. Key files may	be in PEM Base64 encoded format.	
Upload File:	gram Files (x86)\xca\IKEv2Test\privcl.pem	Browse
Filename	privcl.pem	
Passphrase:		
Confirm Passphrase:		
Upload Key file saved.		

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

	Service Plan / APN: Internet.t-d1.de
	Use backup APN Retry the main APN after 0 minute:
	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
Ena	IB address OIR address and Bot
-	

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

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

The IP address or hostname of the remote u	nit 37.85.24.187
Use	as a backup unit
Local LAN	Remote LAN
Output Use these settings for the local LAN	 Use these settings for the remote LAN
IP Address: 192.168.10.0	IP Address: 192.168.1.0
Mask: 255.255.255.0	Mask: 255.255.255.0
○ Use interface PPP 🗸 0	O Remote Subnet ID:
RSA Key File: privcl.pem Our ID: digiwr21 Our ID type IKE ID Remote ID: digiwr11 Use <u>AES (256 bit keys)</u> encryption on this Use <u>SHA1</u> authentication on this tunne Use Diffie Hellman group 2	FQDN OUser FQDN OIPv4 Address
Bring this tunnel up	available
If the tunnel is down and a packet is ready t	o be sent bring the tunnel up
Bring this tunnel down if it is idle for 0	nrs 0 mins 0 secs

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

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

•1	IKEVZ U
	Use the following settings for negotiation
	Encryption: ONONE ODES O3DES OAES (128 bit) OAES (192 bit) OAES (256 b
	Authentication: ONone OMD5 @SHA1 OSHA256
	PRF Algorithm: ONone OMD5 @SHA1 OSHA256
	MODP Group for Phase 1: 2 (1024) V
	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
-	

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

I				
	08:10:14,	24 Mar	2017, (2) IKEv2 Negotiation completed pe, Initiator	
I	08:10:14,	24 Mar	2017, Eroute 0 VPN up peer: digiwr11	
I	08:10:14,	24 Mar	2017, New IPSec SA created by digiwr11	
I	08:10:14,	24 Mar	2017, (2) IKE Notification: AUTH LIFETIME, RX	
I	08:10:13,	24 Mar	2017, (2) IKE Keys Negotiated. Peer:	
I	08:10:13,	24 Mar	2017, (2) IKE Notification: Initial Contact, RX	
I	08:10:13,	24 Mar	2017, (2) IKE Notification: NATD dest. IP,RX	
I	08:10:13,	24 Mar	2017, (2) IKE Notification: NATD source IP,RX	
I	08:10:10,	24 Mar	2017, (2) New IKEv2 Negotiation peer 37.85.24.187, Initiator (Ini	it)
	08:10:10,	24 Mar	2017, IKE Request Received From Eroute 0	

Responder:

Managem	nent - Ev	vent 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)

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:

utbound V1 SAs													
o Tunnels													
bound V1 SAs													
Tunnels													
utbound 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	
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													
bound V2 SAs													
F 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	
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
emove All Refree	h	,					0		-0	<u></u>			

Responder:

atbound V1 SAs													
Tunnels													
nbound V1 SAs													
to 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	
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													
nbound 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	
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
		-				~							

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

Initiator:



Responder:

KEv1 SAs Io SAs									
IKEv2 SAs									
Peer ID	Peer IP	Our IP	Session ID	Rekeys	Auth Alg	Enc Alg	Time Left (secs)	Internal ID	
digiwr21 37	7.81.60.128 3	7.85.24.187	0x1	0	SHA1	AES (256)	28675	1	Remove
Refresh	Remove All	V2 SAs							÷.

In case of issues in the negotiation, take an IKE/IPsec trace following this guide: <u>http://ftp1.digi.com/support/documentation/QN_045_How_To_setup_analyser_To_Get_IKE_IPsec_trac_e.pdf</u>.

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 initator router (but the same can be done on the responder) must be configured as follows:

MANAGEMENT - ANALYSER > SETTINGS

lanagement - Analyser > Settings
▼ Settings
☑ Enable Analyser
Maximum packet capture size: 1500 bytes
Log size: 180 Kbytes
Protocol layers Layer 1 (Physical) Layer 2 (Link) Layer 3 (Network) XOT
Enable IKE debug
Enable QMI trace
LAPB Links
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
Clear all Serial Interfaces
Ethernet Interfaces
□ ETH 0 □ ETH 1 □ ETH 2 □ ETH 3 □ ETH 4
□ ETH 5 □ ETH 6 □ ETH 7 □ ETH 8 □ ETH 9
Clear all Ethernet Interfaces
PPP Interfaces
TD Courses
V ETH 0 C ETH 1 ETH 2 ETH 3 ETH 4
OVPN 0 OVPN 1 OVPN 2
□ PPP 0
□ PPP 5 □ PPP 6 □ PPP 7
Clear all IP Sources

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



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

MANAGEMENT - ANALYSER > TRACE

		2	24-3	3-20)17	08	3:28	3:10).11	LO							
	45 C0 65 75	00 A8 66 76	00 01 67 77	3C 65 68 61	75 08 69 62	1B 00 6A 63	00 0E 6B 64	00 46 6C 65	80 00 6D 66	01 01 6E 67	38 3F 6F 68	8C 15 70 69	C0 61 71	A8 62 72	0A 63 73	64 64 74	E <u8d eF?.abcd efghijklmnopqrst uvwabcdefghi</u8d
	IP 45	(Ir	1) H	ron	n RI	EM T IP Hdi	TO I Vei C Le	LOC			IF# 4 20	ACE	: E1	TH (C		
	00					TOS Del Thi Rel	S: Lay: roug Liak	; ghpu oili	it:	:	Rou Noi Noi Noi	utin cmai cmai cmai	ne l l l				
	00	3С 1в				Ler	ngtł	1:			60	379					
	00	00				Fra Cor	ag (nges)ffs stic	set: on:	:	0 Noi May Las	cmai y F:	l ragi Frac	nent	t nt.		
	80 01 38 C0 C0	8C A8 A8	0A 01	64 65		TTI Pro Che Sro Dst	bto: ecks c IH c IH	: sum: ?: ?:	:		128 ICN 144 192 192	3 4P 476 2.1 2.1	68.1 68.1	10.1	100		
	08 00 0E	46 				Typ Coc Che	be: de: ecks	sum:	:		ECH 0 179	10 1 934	REQ				
45 C0 65	00 A8 66	2 00 01 67	24-3 3C 65 68	3-20 75 08 69)17 1B 00 6A	08 00 0E 6B	3:28 00 46 6C	3:10 7F 00 6D	0.12 01 01 6E	LO 39 3F 6F	8C 15 70	C0 61 71	A8 62 72	0A 63 73	64 64 74		E <u9d eF?.abcd efghijklmnopqrst</u9d

					••••			- • • •								
75	76	77	61	62	63	64 6	5 66	67	68	69						uvwabcdefghi
ER 45 00	0-0	dig:	iwr:	11 1	From IP Hdr TOS Del Thr Rel	Ver: Ler : ay: ough iabi	TO TO n: nput: lity	REM	IFA 4 20 Rou Non Non	ACE: utir rmal rmal rmal	: Pi ne l l	PP :	1			
75 00	1B 00				ID: Fra Con	.g Of .gest	fset	:	299 0 Noi May	979 rmal y Fi	l ragi	nen [.]	t			
7F 01 39 C0 C0 ICN	8C A8 A8 4P:	0A 01	64 65		TTL Pro Che Src Dst	to: cksu IP: IP:	ım:		12 ICN 14 192 192	7 MP 732 2.10 2.10	68.1 68.1	10.1	100 01			
08 00 0E	46				Typ Cod Che	e: e: cksı	ım:		ECH 0 179	HO F 934	REQ					
45 25 C2 90 33 82 2C E0	00 55 5B 73 3C DD 45 23	2 00 18 0B 10 5A 43 EB	24-3 78 82 4C 04 44 CB 04	3-20 00 86 9C 9B AC 71 93 CB	017 1B 65 49 DA 7C 47 4C 54	08: 00 (7E 9 AD <i>F</i> 51 5 70 E C9 5 CE 9	28:1 0 FA 0 C9 7D 59 7D 59 59 0F 7A AC 50 9E	0.1 32 00 E9 7C 54 D0 09	10 20 00 A4 AE CA 22 CB	58 1B 23 8D A9 F4 DF	25 24 0E AA DA E9 D7	51 B3 46 7B 80 CA BC	3C D5 7C 90 5B 8E 63	80 85 F1 8F 5F 27 25		Ex2 X%Q<. %Ue~\$.[I#.F . .s.L}Y {. 3< QY.T[_ ZDqGp"' ,ECL.Pc% .#T.
IP 45 00	(F:	inai	1) 1	Fror	n LO IP Hdr TOS Del Thr	Ver: Ver: Ler ay: ough) REM	I ,.	IFA 4 20 Rou Nos	ACE: utir rmal rmal	: Pi ne L	PP :	1			
	78 1B 00				Len ID: Fra Con	.gth: .g Of	fset	:	120 27 0 Noi May	rmal y Fi	l Tagi	nen [.]	t			
FA 32 20 25 25	58 51 55	3C 18	80 BB		TTL Pro Che Src Dst	to: cksu IP: IP:	ım:		250 ESI 828 37 37	30 30 .81.	. 60 . 24	.12; .18	8			
	 45	0.0	00	24-3 78	3-20 00	17 15 (08:2	8:1 F4	1.04	40 26	 5E	25	 55	18	BB	Ex2%^%U
	25 54 22 1C B8 8E C8	51 A9 C3 C6 DE 14 10	3C 77 DB 40 62 44 37	80 EB 74 73 7C EE E1	AB 5E E0 51 3B C6 F9	00 E 0D 2 9E 7 93 1 6B 0 26 6 F5 4	EC B3 21 65 7E 2C .A F7 DE AE 58 A7	00 A0 A3 A7 93 14	00 CC F0 EB 40 69	00 27 C0 8D 99 12	15 42 7E 54 2A C4	22 88 1C 2E 44 CD	15 D3 5A 55 E2 25	C5 2B 3B E8 51 86	15 88 41 5B B3 F1	<pre>%Q<" T.w.^.!e'B+. "t~Z;A @sQT.U.[b ;k@.*D.Q. D&hi% 7I.</pre>

	IP (In) From P 45 00 00 00 78 00 15 00 00	REM TO LOC IP Ver: Hdr Len: TOS: Delay: Throughput: Reliability: Length: ID: Frag Offset: Congestion:	IFACE: PPP 1 4 20 Routine Normal Normal 120 21 0 Normal May Fragment	
	F4 32 26 5E 25 55 18 BB 25 51 3C 80	TTL: Proto: Checksum: Src IP: Dst IP:	Last Fragment 244 ESP 9822 37.85.24.187 37.81.60.128	
	24-3-2 45 00 00 3C 54 C0 A8 0A 64 00 65 66 67 68 69 75 76 77 61 62	2017 08:28:11.0 4 14 00 00 7F 01 0 00 16 46 00 01 9 6A 6B 6C 6D 6F 2 63 64 65 66 67	040 L 5A 93 CO A8 01 65 L 3F 15 61 62 63 64 E 6F 70 71 72 73 74 7 68 69	E <tze dF?.abcd efghijklmnopqrst uvwabcdefghi</tze
	IP (Cont) From 45	n REM TO LOC IP Ver:	IFACE: PPP 1 4	
	00 00 3C 54 14 00 00	Hdr Len: TOS: Delay: Throughput: Reliability: Length: ID: Frag Offset: Congestion:	20 Routine Normal Normal 60 21524 0 Normal May Fragment	
	7F 01 5A 93 C0 A8 01 65 C0 A8 0A 64 ICMP: 00	TTL: Proto: Checksum: Src IP: Dst IP: Type:	Last Fragment 127 ICMP 23187 192.168.1.101 192.168.10.100 ECHO REPLY	
	00 16 46 	Code: Checksum:	0 17942	
45 C0 65 75	24-3-201 00 00 3C 54 14 A8 0A 64 00 00 66 67 68 69 62 76 77 61 62 63	7 08:28:11.040 4 00 00 7E 01 5H 0 16 46 00 01 3H A 6B 6C 6D 6E 6H 3 64 65 66 67 68	3 93 CO A8 01 65 7 15 61 62 63 64 7 70 71 72 73 74 3 69	E <t~.[e dF?.abcd efghijklmnopqrst uvwabcdefghi</t~.[e
IP 45 00	(Final) From I II Ho TO De Th	LOC TO REM IN P Ver: 4 dr Len: 20 DS: Ro elay: No proughput: No	FACE: ETH 0 Dutine Dormal Dormal	
00	Re 3C Le	eliability: No	ormal	

54	14		ID:	21524
00	00		Frag Offset:	0
			Congestion:	Normal
			2	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
ICM	P:			
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"

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 12on 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 "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 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

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 11_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 Ø 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

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 12on 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 "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 Ø 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 ОК