

TheGreenBow IPSec VPN Client

User Guide

Using Certificates

WebSite:

http://www.thegreenbow.com

Contact:

support@thegreenbow.com

Certificates User Guide

THEGR	EÉ	RB	8111181

Doc.Ref	tgbvpn_certificates_en
Doc.version	2.0 – Nov 2006
VPN version	4.00

Table of contents

1	Introduction	. 3
2	Managing certificates 2.1 Features 2.2 Using certificates 2.3 Importing PKCS#12 certificate 2.4 Importing PEM files 2.5 Reading smart cards 2.6 Configuration options	. 4 . 3 . 4 . 6 . 8 10 12
3	Using Microsoft Certificates Server	14 14 16 19 20
4	Using OpenSSL 4.1 Generating Certificates 4.1.1 Generating a self-signed Certificate 4.1.2 Generating a User Certificate 4.2 Additional TgbSmallPKI tools 4.2.1 Displaying Certificate information	22 22 22 23 25 25
5	Troubleshootings	27
6	Contacts	28

THEGR	DB	

Doc.Ref	tgbvpn_certificates_en
Doc.version	2.0 – Nov 2006
VPN version	4.00

1 Introduction

1.1 Goal of the document

This document explains how to use certificates with TheGreenBow IPSec VPN Client. Theses certificates can be stored on a smart card or imported from a PKCS#12 file.

This document explains also how to use a third party Certification Authority in order to be able to generate X509 Certificates and to open a VPN tunnel securely. There are many options to generate Certificates like using Microsoft Certificates server (i.e. Microsoft Certificate Service) available under Windows 2000/2003 Server, OpenSSL or some VPN Router themselves.

1.2 Features

Two kinds of certificates can be imported to TheGreenBow VPN Client:

- PKCS#12
- PEM certificates.

Certificates can be stored in a smart card whose access is protected by a PIN code. TheGreenBow VPN Client uses them dynamically while establishing a tunnel.

A certificate has three parts:

- certificate authority public key
- user certificate public key
- user certificate private key

Once imported, these keys are stored in the configuration file. One certificate is bound to one tunnel. All configuration elements can be easily exported to another computer.

In the case of smart card, the configuration file contains no one of the three keys.

Doc.Ref	tgbvpn_certificates_en
Doc.version	2.0 – Nov 2006
VPN version	4.00

2 Managing certificates

2.1 Using certificates

X509 certificates and smart cards are managed in phase 1 settings. A phase 1 must be created.

e <u>V</u> PN Configuration Vie <u>v</u>	<u>v T</u> ools <u>?</u>
HEGREENBOL	IPSec VPN Clien
🔑 Console	Phase 1 (Authentication)
🚱 Parameters	Name Phase_1
S Connections	Interface Any
E <u>↓ Phase 1</u> Phase_2 Phase_2	Preshared Key Confirm Certificate Certificates Import
	IKE Encryption AES 128 P1 Advanced P1 Advanced.
	<u>S</u> ave & Apply

Click on "Certificate" and then on "Certificates Import..."

Doc.Ref	tgbvpn_certificates_en
Doc.version	2.0 – Nov 2006
VPN version	4.00

In the Certificates import window, the user can import certificates files in the VPN configuration or read them from a smart card.

E
Root Certificate
User Certificate
User Private Key
Choose below the Certificate location and type:
Certificate from a PKCS#12 file Certificate from a PKCS#12 file Certificate from a PEM file
Certificate from a SmartCard Import Certificates from a PKCS12 file Import
Ok Cancel

TheGreenBow VPN client supports the following certificates format file:

- PKCS#12 files
- PEM files
- CRT files

Doc.Ref	tgbvpn_certificates_en
Doc.version	2.0 – Nov 2006
VPN version	4.00

2.2 Importing PKCS#12 certificate

From the drop-down list, select "Certificate from a PKCS#12 file".

E
Root Certificate
User Certificate
User Private Key
Choose below the Certificate location and type:
Certificate from a PKCS#12 file
Import Certificates from a PKCS12 file Import
Cancel

And click on "Import..."

Open	? 🔀
Look jn: [Desktop 💌 🗲 🛅 📸 🖬 🕇
My Docum My Compu My Netwoi Cigb1.p12	ents ter ½ Places
File <u>n</u> ame:	tgb1.p12
Files of <u>type</u> :	Certificates P12 (*.p12) Cancel
	C Open as read-only

Select the PKCS#12 file and click on "Open".



PKCS12 file password	
	5
Please enter the file pass	word below:
OK	Cancel

The file can be protected by a password. If not, the edit box can be let empty.

Click on "OK" for importing the file.

E		
Root Certificate /C=FR/L=Paris/0=TheGreenBow/CN=TheGreenBow CA/emailA		
User Certificate /C=FR/0=TheGreenBow/CN=tgb1		
🙀 User Private Key		
Choose below the Certificate location and type:		
Certificate from a PKCS#12 file		
Import Certificates from a PKCS12 file		
Ok Cancel		

If the password is correct and the file not corrupted, the subject of the certificate and the subject of the issuer of the certificates are displayed.

The key icons indicate that the data is now stored in TheGreenBow VPN Client configuration file.

Doc.Ref	tgbvpn_certificates_en
Doc.version	2.0 – Nov 2006
VPN version	4.00

2.3 Importing PEM files

In the certificate management window, select "Certificate from a PEM file" in the drop-down list.

	Ð
Root Certificate	
User Certificate	
User Private Key	
Choose below the Certificate location	and type:
Certificate from a PEM fil	≥
	[test
Import a PEM Hoot Certificate	Import
Import a PEM User Lertificate	
Import a Private Key	Import
[Ok Cancel

Click on each button "Import..." for importing the Certificate Authority (CA) public key, the user public key and the user private key.



Select the file and click on "Open"

THEGREERBOUNIN	Doc.Ref	tgbvpn_certificates_en
	Doc.version	2.0 – Nov 2006
	VPN version	4.00

	×
	63)
Root Certificate /C=FR/L=Paris/O=TheGreenBow/CN=	-TheGreenBow CA/emailA
User Certificate /C=FR/0=TheGreenBow/CN=tgb1	
<table-of-contents> User Private Key</table-of-contents>	
Choose below the Certificate location and I	type:
Certificate from a PEM file	
Import a PEM Root Certificate	Import
Import a PEM User Certificate	Import
Import a Private Key	Import
	Ok Cancel

Once the files are imported, the subjects of the user certificate and its issuer are displayed.

	Doc.Ref	tgbvpn_certificates_en
	Doc.version	2.0 – Nov 2006
	VPN version	4.00

2.4 Reading smart cards

In the certificate management window, select "Certificate from a smart card".

E
Root Certificate
User Certificate
User Private Key
Choose below the Certificate location and type:
Certificate from a SmartCard
Select a Smart Card Reader:
Ok Cancel

Select in the smart card list the smart card reader



Enter the smart card PIN code

THEGREEDBOUND	Doc.Ref	tgbvpn_certificates_en
	Doc.version	2.0 – Nov 2006
	VPN version	4.00

E
Root Certificate /C=FR/L=Paris/0=TheGreenBow/CN=TheGreenBow CA/emailA
User Certificate /C=FR/0=TheGreenBow/CN=tgb1
User Private Key
Choose below the Certificate location and type:
Certificate from a SmartCard
Select a Smart Card Reader: OMNIKEY CardMan 3x21 0 ATR = 38:78:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00 Using IDOne Lite PKCS#11 middleware found
Ok Cancel

If the PIN is correct, the subject of the certificate is displayed in the window.

	Doc.Ref	tgbvpn_certificates_en
	Doc.version	2.0 – Nov 2006
	VPN version	4.00

If the smart card is not supported, ar	n error message is displayed:
--	-------------------------------

E
Root Certificate
User Certificate
User Private Key
Choose below the Certificate location and type:
Select a Smart Card Reader: OMNIKEY CardMan 3x21 0 ATR = 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00 Unknown ATR: this smart card may not be supported No PKCS11 middleware for this smart card was found. You can set PKCS#11 middleware with the command line : vpnconf.exe /addmiddleware:path_to_the_dll
(Ok Cancel

Read next section for details about making your smart card supported.

2.5 Configuration options

Several smart card options are available for IT managers. It is possible to force use of a specific PKCS#11 middleware, for example. Administrative rights are required for using these options.

/addmiddleware:[path_to_middleware.dll]

Set manually the path to the PKCS#11 DLL that must be used by the client

/checkkeyusage:[yes|no]

By default, TheGreenBow VPN client does not check X509 key usage extensions.

If "yes" is used, the VPN client will only look for certificates that have digital signature (DIGITAL_SIGNATURE) key usage.

This parameter is only used for certificates read from smart cards.

Doc.F	tgbvpn_certificates_en
Doc.v	ersion 2.0 – Nov 2006
VPN	version 4.00

Doc.Ref	tgbvpn_certificates_en
Doc.version	2.0 – Nov 2006
VPN version	4.00

3 Using Microsoft Certificates Server

In the section, we provide full steps to generate an user certificate, sign a Certificate Request and export Certificates using **Microsoft Certificate Server**.

3.1 Installing Microsoft Certificate Server

Microsoft Certificate server comes as a part of the Windows NT/2000/2003 server option packs. The Certificate server needs Microsoft Internet Information server (IIS) and Microsoft Internet explorer (IE) before it can be used.

The enrollment Web pages provided by Certificate Services allow you to connect to the service with a Web browser, and to do common tasks such as requesting the certification authority, processing a Certificate Request file, or processing a Smart Card enrollment file. The Web pages will be located on http://ServerName/CertSrv where ServerName is the name of the CA-issuing machine.

For information on configuring Microsoft Certificate Services on Windows 2000 server, see the following URLs:

- On Setting up a Certificate Authority: <u>http://www.microsoft.com/windows2000/techinfo/planning/security/casetupsteps.asp</u>
- On Microsoft Certificate Services Web Pages: <u>http://www.microsoft.com/windows2000/techinfo/planning/security/cawebsteps.asp</u>
- On Administering Microsoft Certificate Services: <u>http://www.microsoft.com/windows2000/techinfo/planning/security/adminca.asp</u>

Below we provide required steps to install Internet Information Server (IIS 6.0) and Microsoft Certificate Server (MCS) with a stand-alone root CA on Windows 2003 Server.

Microsoft Internet Information Server installation steps :

- Click Start, point to Control Panel and click Add or Remove Programs .
- Click the Add/Remove Windows Components button in the Add or Remove Programs window.
- On the Windows Components window, click on the Application Server entry and click the Details button.
- On the Application Server page, click on the Internet Information Services (IIS) entry and click the Details button.
- In the Internet Information Service (IIS) dialog box, put a checkmark in the World Wide Web Service checkbox and click OK.
- Click **OK** on the **Application Server** dialog box.
- Click Next on the Windows Components dialog box.
- Click Finish on the Completing the Windows Components Wizard page.

Microsoft Certificate Server with a stand-alone root CA installation steps :

- Click Start, point to Control Panel and click Add/Remove Programs.
- In the Add or Remove Programs window, click the Add/Remove Windows Components button.
- In the Windows Components dialog box, click on the Certificate Services entry and click the Details button.
- In the Certificate Services dialog box, put a checkmark in the Certificate Services CA checkbox.

	Doc.Ref	tgbvpn_certificates_en
	Doc.version	2.0 – Nov 2006
	VPN version	4.00

- Both the Certificate Services CA and Certificate Services Web Enrollment Support checkboxes are checked. Click OK in the Certificate Services dialog box.
- Click **Next** in the **Windows Components** dialog box.
- Update the CA Type page as shown below. Click Next.

C.4.	Turne
LA	Select the type of CA you want to set up.
1	C Externing root CA
	C Externing subscripts D/
	Chephse substance cs. Stand along test CA
	C Shand alone subardinate CA
	 sjand-alone subordinate CA
	Description of CA type The most trusted CA in a CA hierarchy
	To install an enterprise LA, Active Directory is required; you must also be a member of the Enterprise Admins group.
	Use custom settings to generate the key pair and CA certificate

Update/customize the **Public and Private Key Pair** page as shown below. Click **Next**.

<u>C</u> SP:	P. F. M. THURSDOOM, SPACE WAS ADDRESS.	Hash algorithm:	
Microsoft Base DSS Crypt Microsoft Ephanced Crypt	ographic Provider	MD4 MD5	
Microsoft Strong Cryptogr	aphic Provider	SHAT	
Schlumberger Cryptograpi	ric service Provider	Key length:	
Allow this Coll to intere	ici min nie gesktop	1024	
n mac an Existing Key.		I <u>m</u> port	
		View Certificate	
		Tiew cermicare	

Doc.Ref	tgbvpn_certificates_en
Doc.version	2.0 – Nov 2006
VPN version	4.00

Department of the CA Identifying Information page as shown below. Click Next.

common name for this CA:	
ГgbCA	
istinguished name suffix:	
DC=TheGreenBow,DC=fr	
Preview of distinguished na	ame:
CN=TgbCA,DC=TheGreen	ıBow,DC=fr
alidity period:	Expiration date:
	20 10 1 1001 5 1 1 10

- On the Certificate Database Settings page, use the default locations for the Certificate Database and Certificate Database Log. You do not need to specify a shared folder to store configuration information because this information will be stored in the Active Directory. Click Next.
- Click Yes on the Microsoft Certificate Services dialog box that informs you that Internet Information Services must be stopped temporarily.
- Click Yes on the Microsoft Certificate Services dialog box that informs you that Active Server Pages must be enabled on IIS if you wish to use the Certificate Services Web enrollment site.
- Click Finish on the Completing the Windows Components Wizard page.
- Close the Add or Remove Programs window.

3.2 Generating Certificates

In the section, we provide full steps to generate an user certificate and sign a Certificate Request.

3.2.1 Generating an user certificate

This section describes the generation of User certificate for TheGreenBow VPN IPSec Client. This section applies to any other VPN IPSec end point, like a VPN router.

To generate generated an user certificate do:

- Connect to your Certificate Server (http://ServerName/CertSrv where ServerName is the name of the CAissuing machine)
- Click **Request a Certificate** on the **Welcome** page.

	Doc.Ref	tgbvpn_certificates_en
	Doc.version	2.0 – Nov 2006
	VPN version	4.00

- Click Advanced Certificate Request on the Request a Certificate page.
- Click Create and submit a request to this CA on the Advanced Certificate Request page.
- Fill the Advanced Certificate Request page (a sample is shown below). You must check Mark keys as exportable as TheGreenBow VPN IPSec Client needs the Certificate private key to establish a tunnel. Click Submit.

<i>ficrosoft</i> Certific	cate Services TgbCA	Ho
dvanced Ce	rtificate Request	
entifying Infor	mation:	
Name:	TheGreenBow VPN Client	
E-Mail:	TgbClient@thegreenbow.fr	
Company:	TheGreenBow	
Department:	VPN	
City:	Paris	
State:	France	
Country/Region:	FR	
me of Certifica	te Needed	
L'a et setuned	Client Authentication Certificate	
ey Options:		
	Create new key set OUse existing key set	
CSP:	Microsoft Enhanced Cryptographic Provider v1.0	
Key Usage:	C Exchange Signature Both	
Key Size:	1024 (common key sizes: <u>512 1024 2048 4096 8192 16384</u>)	
	Automatic key container name	
	Mark keys as exportable	
	Export keys to file	
	Enable strong private key protection	
	Store certificate in the local computer certificate store Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.	
Additional Op	ntions:	
Request Form	at:	
Hash Algorith	m: SHA-1 👻	
	Only used to sign request.	
	Save request to a file	
Attribute	es:	
Friendly Nan	ne; TgbClient	
-	Qubmit >	

After processing, the **Certificate Pending** page appears. You have to wait until your request is accepted and validated by your Microsoft Certificate Server administrator.

	Doc.Ref	tgbvpn_certificates_en
	Doc.version	2.0 – Nov 2006
	VPN version	4.00

Eile Action View Help						
⇔ → 🖻 🖪 🕼 🔮						
🔁 Certification Authority (Local)	Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective
Control Certificates Certificates Sudd Certificates Pending Requests Failed Requests	12	2003SERVER\IU	BEGIN CERTIFICATE MILEBDCCA2		152c458c000	21/04/2005 16:33
	4					×

- To retrieve your Certificate, return back to Microsoft Certificate Server's home page and click View the status of a pending Certificate Request.
- In the View the Status of a Pending Certificate Request page, select the request you want to view.
- The Certificate Issued page appears as shown below:

<i>Microsoft</i> Certificate Services TgbCA	Home
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	

To add the current Certificate to your local Certificates Store click the Install this Certificate.

Microsoft Certificate Services TgbC	As .	<u>Home</u>
Certificate Issued		
The certificate you requested was	issued to you.	
Install this certificate		
Root Ce	rtificate Store 🔀	
	Do you want to ADD the following certificate to the Root Store? Subject : TgbCA, TheGreenBow, fr Issuer : Self Issued Time Validity : Wednesday, April 20, 2005 through Monday, April 20, 2015 Serial Number : 7AAF234C 526E4484 471E4185 F0049521 Thumbprint (sha1) : D8ADC900 7C7A1292 E0837DF0 EE18B26D D5D97F21 Thumbprint (md5) : E418FC22 A0082FFF 19F8FBF5 71A97FF8 Yes No	

After processing the **Certificate Installed** page appears confirming the Certificate successful installation in Internet Explorer Certificate store.



Doc.Ref	tgbvpn_certificates_en
Doc.version	2.0 – Nov 2006
VPN version	4.00

Home

ne

Microsoft Certificate Services -- TgbCA

Certificate Installed

Your new certificate has been successfully installed.

To export a Certificate from Internet Explorer Certificate store, check 3.3 section.

3.2.2 Signing a Certificate Request

To sign the Certificate Request using Microsoft Certificate Server do:

- Connect to your Certificate Server (http://ServerName/CertSrv where ServerName is the name of the CAissuing machine)
- Click Request a Certificate on the Welcome page.
- Click Advanced Certificate Request on the Request a Certificate page.
- Click Submit a Certificate Request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
- Click Browse for a file to insert and browse to the certificate request file then Read! Button. The Submit a Certificate Request or Renewal Request page looks like:

ate Services TgbCA	H
ficate Request or Renewal Request	
ed request to the CA, paste a base-64-encoded CMC or PF S #7 renewal request generated by an external source (such box.	<cs #10="" certificate<br="">as a Web server) in th</cs>
The set of the s	
Browse for a file to insert.	
<	
	Ale Services - 1gbCA ficate Request or Renewal Request ed request to the CA, paste a base-64-encoded CMC or Pk S #7 renewal request generated by an external source (such box. BEGIN CERTIFICATE REQUEST MIIBpDCCAQ0CAQAwIjEgMB4GA1UEAwwXen14ZWwx g28wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM7c 44igK119ZW3Y+CVm9uiyD1IX33v8yyWq9yvCqDpT y8mfEw0KvPNWkBktSKHpbulyD/ligWHsiJTbi3Lr XXCYAR0WtdecFmwDAgMBAAGgQjBABgkqhkiG9w0B Browse for a file to insert. ttes:

Click Submit.

After processing, the **Certificate Pending** page appears. You have to wait until your request is accepted and validated by your Microsoft Certificate Server administrator.

- To retrieve your Certificate, return back to Microsoft Certificate Server's home page and click View the status of a pending Certificate Request.
- In the View the Status of a Pending Certificate Request page, select the request you want to view.
- The **Certificate Issued** page appears as shown below:



Click Download Certificate. A file download would pop out, press Save button (The default file name is certnew.cer).

3.3 Certificate Export

Installed Certificates in Internet Explorer Certificate store can be exported using the PKCS12 file format.

To export Certificates from Internet Explorer Certificate store do:

- Run Internet Explorer.
- Open Internet Options... in Tools menu.
- Select **Content** tab then click **Certificates** button.
- In the Certificates dialog box, open Personal tab. Select the Certificate to export as shown below:

ourie				
Issued 10	Bow VPN	TgbCA	4/21/2006	TgbClient
nport	Export	. Remove		Advar

- Click Export....
- In the Certificate Export Wizard click Next.
- In the Export Private Key select Yes, export private key as need by TheGreenBow VPN IPSec Client.

Doc.Ref	tgbvpn_certificates_en
Doc.version	2.0 – Nov 2006
VPN version	4.00

Certificate Export Wizard
Export Private Key You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
• Yes, export the private key
🚫 No, do not export the private key
< Back Next > Cancel

In the Export File Format page select Include all Certificates in the certification path if possible. The Root CA is also exported as needed by TheGreenBow VPN IPSec Client.

с	rt File Format ertificates can be exported in a variety of file formats.
S	elect the format you want to use:
	O DER encoded binary X.509 (CER)
	G Base-64 encoded X.509 (.CER)
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
	Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
	Delete the private key if the export is successful

- Click Next.
- In the **Password** page, type and confirm your password then click **Next**.
- In the **File to Export** page specify destination file path then click **Next**.
- In the Completing the Certificate Export Wizard Click Finish.

4 Using OpenSSL

OpenSSL is a free non-commercial toolkit that provides a wide range of cryptographic operations. It also includes utilities for Certificate management. More details about building and using OpenSSL can be found at http://www.openssl.org.

Since the openssl program is a command line tool we have written several batch scripts for Certificate generation and management. Unzip **TgbSmallPKI.zip** into **C:\TgbSmallPKI** for instance (in the following sections, we will assume that this path is our working folder). The working folder contains:

- RootCA.bat: It generates a self-signed root Certificate.
- UserCA.bat: It generates an user certificate signed by the root Certificate.
- Pkcs12.bat: It Converts a P12 file into PEM files.
- **CAinfo.bat**: It displays a PEM Certificate information.
- CAsign.bat: It signs a Certificate Request.
- The \Bin forlder contains:
 - openssl.cnf: A large part of what goes into a Certificate depends on the contents of this configuration file. It is divided into sections, which helps to make the configuration more modular. You can customize this file depending on your needs (see OpenSSL documentation for more details).
 - o openssl.exe, libeay32.dll and ssleay32.dll are the toolkit core for Windows platforms.
- **ReadME.txt**: A documentation file.

4.1 Generating Certificates

In the following section we will show how to generate a self-signed root Certificate, an User Certificate and sign a Certificate Request using OpenSSL for Windows.

4.1.1 Generating a self-signed Certificate

A self-signed Certificate is a Certificate that is not signed by a recognized Certificate Authority. A self-signed Certificate can be used to act as a Certificate authority issuing, renewing and revoking Certificates.

To create a self-signed Certificate, run RootCA. Below a sample output:

```
*
! Creating Root CA folders
*
Root CA folder set to .\RootCA
Root CA key length is 1024 bits
Root CA validity is 3650 days
The system cannot find the file specified.
*
! Creating CA private key (1024 bits, 3650 days)
*
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
......++++++
```



Doc.Ref	tgbvpn_certificates_en
Doc.version	2.0 – Nov 2006
VPN version	4.00

e is 65537 (0x10001)

! CA autosigning (1024 bits, 3650 days)

Using configuration from .\Bin\openssl.cnf You are about to be asked to enter information that will be incorporated into your Certificate Request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. -----Country Name (2 letter code) [FR]:FR State or Province Name (full name) [France]:France Locality Name (eg, city) []:Paris

Organization Name (eg, company) [TheGreenBow]:TheGreenBow Organizational Unit Name (eg, section) []:Authority Certificate Common Name (eg, YOUR name) []:TheGreenBow CA Email Address []:TgbCA@thegreenbow.fr

Please enter the following 'extra' attributes to be sent with your Certificate Request A challenge password []:capassword An optional company name []:TheGreenBow Loading 'screen' into random state - done Signature ok subject=/C=FR/ST=France/L=Paris/O=TheGreenBow/OU=Authority Certificate/CN=TheGreenBow CA/Email=TgbCA @thegreenbow.fr Getting Private key

"_____"

Root Certificate at .\RootCA\RootCA.pem Root Private Key at .\RootCA\CAKey.key

The root Certificate RootCA.pem and its private key CAKey.key are located in RootCA folder.

4.1.2 Generating an user certificate

When X.509 Certificate authentication is chosen within IKE, a User certificate is used to identify a VPN IPSec end point and to perform signatures/verification operations.

The **UserCA** script generates an user Certificate, its private key and a PKCS12 file. It requires an intermediate folder as a parameter. It can be used to generate Certificates for all VPN IPSec end points.

To generate all required files for TheGreenBow VPN IPSec Client, run UserCA TgbClient:

! Creating User CA folder

Creating User Certificate folder at .\TgbClient User CA key length is 1024 bits User CA validity is 3650 days

Do	oc.Ref	tgbvpn_certificate
Do	oc.version	2.0 – Nov 2006
VF	PN version	4.00

*

! Creating User CA private key (1024 bits)

Loading 'screen' into random state - done Generating RSA private key, 1024 bit long modulus

e is 65537 (0x10001)

! Signing User CA

Using configuration from .\Bin\openssl.cnf You are about to be asked to enter information that will be incorporated into your Certificate Request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. -----Country Name (2 letter code) [FR]:FR

State or Province Name (full name) [France]:France Locality Name (eg, city) []:Paris Organization Name (eg, company) [TheGreenBow]:TheGreenBow Organizational Unit Name (eg, section) []:VPN Common Name (eg, YOUR name) []:TheGreenBow VPN Client Email Address []:TgbClient@thegreenbow.fr

Please enter the following 'extra' attributes to be sent with your Certificate Request A challenge password []:tgbcapwd An optional company name []:TheGreenBow Loading 'screen' into random state - done Signature ok subject=/C=FR/ST=France/L=Paris/O=TheGreenBow/OU=VPN/CN=TheGreenBow VPN Client/Email=TgbClient@thegreenbow.fr Getting CA Private Key

! User CA in P12 Format

Loading 'screen' into random state - done Enter Export Password: Verifying password - Enter Export Password: TgbClient.p12 created in .\TgbClient.p12

"_____" "_____"

User Certificate at .\TgbClient\TgbClient.pem User Private Key at .\TgbClient\local.key User Certificate Subject is: subject= /C=FR/ST=France/L=Paris/O=TheGreenBow/OU=VPN/CN=TheGreenBow VPN Client/Email=TgbClient@thegreenbow.fr

The most relevant files in the **TgbClient** folder are:

s_en

Doc.Ref	tgbvpn_certificates_en
Doc.version	2.0 – Nov 2006
VPN version	4.00

- TgbClient.pem: The User Certificate.
- Local.key: the User Certificate private key.
- Subject.txt: the User Certificate subject.
- TgbClient.p12: a PKCS12 file format containing user and root Certificates and the user certificare private key.

4.2 Additional TgbSmallPKI tools

In the following section we will show how to display Certificate information and how to extract Certificates and private keys from a PKCS12 format file.

- Pkcs12.bat: It Converts a P12 file into PEM files.
- **CAinfo.bat**: It displays a PEM Certificate information.

4.2.1 Displaying Certificate information

Displaying Certificate information can be useful to retrieve several fields such as the Issuer, the Validity date and the Subject.

The CAinfo script displays a User Certificate information. It requires Certificate file as a parameter.

To display more information about TgbClient.pem (TheGreenBow User Certificate generated in section **4.1.2**), run **CAinfo TgbClient\TgbClient.pem**:

```
! Certificate TgbClient\TgbClient.pem information
Certificate:
  Data:
     Version: 1 (0x0)
     Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
     Issuer: C=FR, ST=France, L=Paris, O=TheGreenBow, OU=Authority Certificate, CN=TheGreenBow CA
/Email=TgbCA@thegreenbow.fr
    Validity
       Not Before: Apr 19 12:44:03 2005 GMT
       Not After: Apr 17 12:44:03 2015 GMT
     Subject: C=FR, ST=France, L=Paris, O=TheGreenBow, OU=VPN, CN=TheGreenBow VPN Client/Email=Tg
bClient@thegreenbow.fr
    Subject Public Key Info:
       Public Key Algorithm: rsaEncryption
       RSA Public Key: (1024 bit)
         Modulus (1024 bit):
           00:ac:00:2c:1b:82:6d:32:2e:17:09:9f:13:8d:b9:
           9f:9b:db:d7:3f:f7:45:9b:f2:73:6d:8b:3d:9b:b1:
           14:99:25:22:fb:a8:56:30:9d:68:43:e9:14:84:6f:
           4c:24:fa:e2:36:84:56:2d:b2:5c:11:fd:be:b9:9e:
           ed:49:c8:c1:08:29:d0:17:ca:b8:12:41:41:55:4d:
           48:01:57:bc:22:9a:c9:48:ca:e2:c2:59:2c:78:8d:
           6d:cc:89:09:3a:97:f5:f4:b7:96:ea:da:82:0e:8c:
           87:49:a7:45:a4:74:45:31:8e:ac:be:9a:a2:8c:a1:
            16:be:f7:46:4a:94:78:31:73
         Exponent: 65537 (0x10001)
```

Doc.Ref	tgbvpn_certificates_en
Doc.versior	2.0 – Nov 2006
VPN versio	n 4.00

Signature Algorithm: md5WithRSAEncryption b2:ba:7c:92:9c:eb:59:c2:7e:d9:95:af:71:8b:06:2f:b8:44: b3:b5:2a:b7:98:0b:1e:08:97:85:c7:bc:21:1c:cf:df:15:97: d9:4f:e5:ec:31:14:6f:9e:b1:8a:47:37:ad:6b:4b:c8:15:bf: cd:8a:1b:ed:a5:f7:3e:ac:72:73:b9:bc:f6:22:b3:05:f5:26: 40:dd:f8:4c:83:3f:25:da:68:32:8b:bd:1b:68:24:e8:df:31: 83:5b:74:91:10:1f:6a:d0:b9:3c:f3:04:50:4c:6e:ce:c9:de: 3a:38:fe:2d:ad:6c:6b:e6:74:38:51:0c:5b:c5:bb:6b:05:25: 44:d9

THEGREEDBOU	Doc.Ref	tgbvpn_certificates_en
	Doc.version	2.0 – Nov 2006
	VPN versior	4.00

5 Troubleshootings

You will be able to find all troubleshooting issues, listed in a TroubleShooting Document (pdf) on our website. The document is available at: <u>www.thegreenbow.com/vpn_doc.html</u>

THEGR	EÉ	R B B M 8811981

Doc.Ref	tgbvpn_certificates_en
Doc.version	2.0 – Nov 2006
VPN version	4.00

6 Contacts

Information and update are available at: <u>http://www.thegreenbow.com</u> Technical support by email at: <u>support@thegreenbow.com</u> Sales at +33 1 43 12 39 37 or by email at: <u>sales@thegreenbow.com</u>