THEGREENBOW

TheGreenBow
VPN Client

Management of PKI, certificates, tokens and smart cards

Table of Contents

1 Introduction

1.1 PKI options

This document describes all the possibilities offered by the TheGreenBow VPN Client software for its integration into any PKI. It is intended for use by the security administrator.

TheGreenBow VPN Client implements a set of functions, options and parameters that enable it to merge into any existing PKI, be it large infrastructures or small configurations.

PKI functions make it possible to:

- Characterise the certificate that the VPN Client needs to use to open a VPN tunnel
- Define the token or smart card reader to be used on the user's workstation
- Configure a set of rules for checking the certificate (validity, CRL, key usage etc.)

PKI parameters can be configured:

- Through the software's user interface
- Through a software setup preconfiguration (vpnsetup.ini paired with the software setup)
- Through a set of command-line options
- Through an initialisation file for the running software (vpnconf.ini)

This document describes all possibilities for the configuration of PKI options during software deployment. Therefore, the intended audience is the safety administrator and not so much the end user.

This document is an extension of the "Deployment Guide for TheGreenBow VPN Client".

1.2 Reference documents

The following documents are referenced throughout the present document. They are available for download on the TheGreenBow website: http://www.thegreenbow.com/vpn_doc.html.

Reference	Title	Document name
[Deployment Guide]	Deployment Guide for TheGreenBow VPN Client	tgbvpn_ug_deployment_fr
[User Guide]	User Guide for TheGreenBow VPN Client	tgbvpn_ug_fr

1.3 Terminology

CSP mode

CSP stands for "Cryptographic Service Provider". This access mode by token and smart card is provided by Microsoft. No additional configuration in TheGreenBow VPN Client is necessary.
Note: not all tokens/smart cards are compatible with this mode.

PKCS#11 mode

PKCS#11 is a token or smart card access API (standardised by RSA Labs).

Tokens are usually compatible with PKCS#11.
This mode requires a DLL provided by the token's manufacturer in a middleware installation package.
This package must be installed on the computer before using TheGreenBow VPN Client.

Some DLL are now identified and automatically recognised by TheGreenBow VPN Client. Some DLL, however, are not, and must therefore be configured (see Section "vpnconf.ini").

ATR

ATR stands for "Answer To Reset". It is an identifier that the token or smart card will provide when asked to reset.
This identifier depends on the manufacturer and model of the token or smart card.

TheGreenBow VPN Client already knows a certain number of ATRs and the associated DLL to be used. In this case, no DLL configuration is necessary as it is automatically identified.
Conversely, if the VPN Client does not already know the ATR, the token must be configured in the VPN Client. This configuration is carried out in an initialisation file, "vpnconf.ini" (see Section "vpnconf.ini").

2 PKI options

2.1 Token and smart card reader characterisation

TheGreenBow VPN Client is natively compatible with a wide array of tokens and smart cards.
A list of certified compatible tokens and smart cards is available on the TheGreenBow website, at the following address: http://www.thegreenbow.com/vpn_token.html. The configuration guide is also provided for several of the items on the list.

It is possible to configure the VPN Client in such a way that the required token or smart card is selected in one of three different ways:

- The smart card reader is specified in the VPN security policy (VPN configuration file)
  Note: A VPN security policy can be associated with the setup so that it is automatically taken into account during the installation.
- The smart card reader can be specified in the software initialisation file "vpnconf.ini".
- The smart card reader is the first one found on the user's workstation, which also contains a smart card.

TheGreenBow VPN Client accesses the tokens or smart card readers using the CSP (Cryptographic Service Provider) or PKCS#11 modes. In order to access the middleware, the VPN Client uses the CSP mode by default. It is, however, possible to force the VPN Client to use the PKCS#11 mode for accessing the middleware.

Note: TheGreenBow VPN Client uses the CSP mode to access the Windows Certificate Store.

2.2 Criteria for choosing a certificate

TheGreenBow VPN Client characterises the certificate required for opening a VPN tunnel by combining the following criteria:

- The subject of the certificate is configured in the VPN security policy (VPN configuration file)
- The type of the certificate to be used is "Authentication" (i.e. its "key usage" contains the attribute "Digital signature")
- The subject of the certificate is not taken into account; the certificate used is the first one found on the token or smart card.

2.3 Certificate management

The VPN Client and the VPN Gateway might use certificates issued by separate certification authorities (i.e. Client and Gateway certificates might be issued by separate intermediate certification authorities, both attached to the same root certification authority). TheGreenBow VPN Client can manage such a certificate configuration.

2.4 VPN gateway certificate

It is possible to force TheGreenBow VPN Client to check the certificate chain for the certificate received from the VPN gateway.

To do this, the root certificate and all the certificates from the certificate chain (the root and intermediate certification authorities) must be imported into the Windows Certificate Store.

The VPN Client will also use the CRL (Certificate Revocation List) from the various certification authorities.
Should these CRLs be missing from the certificate store, or unavailable for download when the VPN tunnel is opened, the VPN Client will not be able to confirm the gateway certificate.

Checking every link of the chain means:

- checking the expiration date of the certificate
- checking the starting date of the certificate's validity
- checking the signatures of all the certificates from the certificate chain (including the root, intermediate and server certificates)
- updating the CRLs of all certificate issuers in the certificate chain
- checking that no certificate revocation is present in the corresponding CRL lists

In the "VPN Certified" version, the gateway authentication must be carried out. For more information on this topic, see the recommended configuration in Section 3.2.

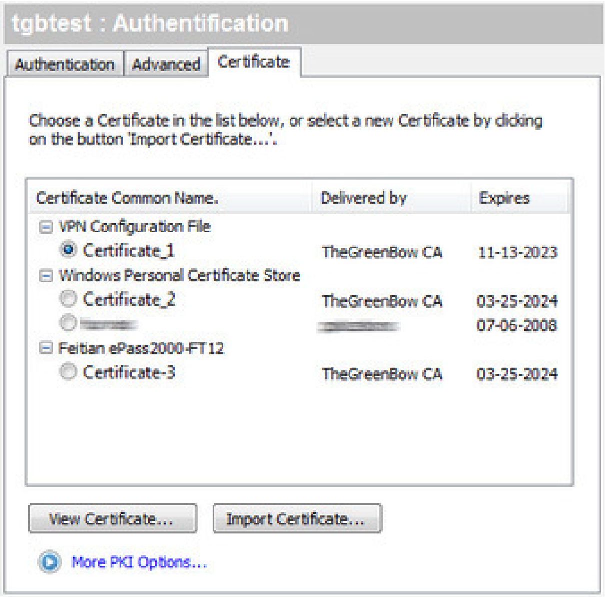
3 Configuration interface

TheGreenBow VPN Client's main interface allows the user to configure the way tokens, smart cards and certificates are managed.

3.1 Certificate tab

The "Certificate" tab automatically displays the list of all certificates found on the token or smart card, provided:

- The token or smart card is CSP or PKCS#11 compatible
- The token's or smart card's middleware is properly installed on the computer
- The smart card is, if need be, correctly inserted in the relevant reader.



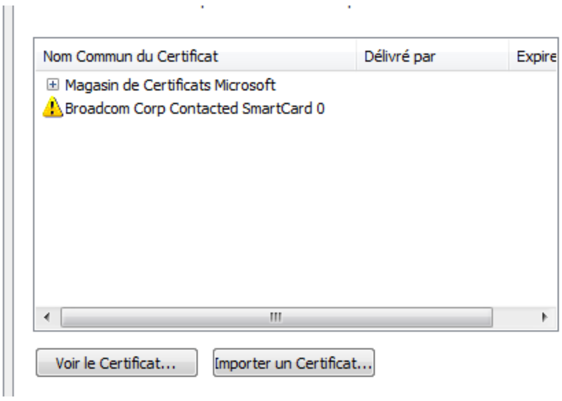
tgbtest : Authentification

Choose a Certificate in the list below, or select a new Certificate by clicking on the button 'Import Certificate...'.

Certificate Common Name.	Delivered by	Expires
⊟ VPN Configuration File		
● Certificate_1	TheGreenBow CA	11-13-2023
⊟ Windows Personal Certificate Store		
○ Certificate_2	TheGreenBow CA	03-25-2024
○ [redacted]	[redacted]	07-06-2008
⊟ Feitian ePass2000-FT12		
○ Certificate-3	TheGreenBow CA	03-25-2024

The Client will display all non-expired certificates on the card.

Note: When using a smart card reader, an alert icon is displayed next to the reader on the list if the smart card is not inserted.

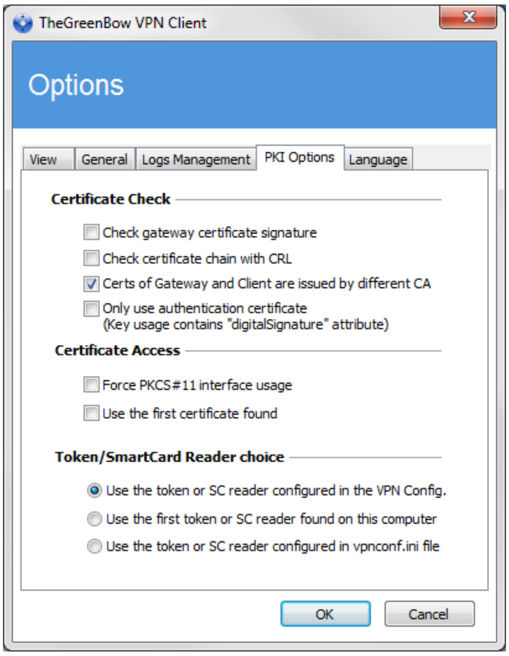


Nom Commun du Certificat	Délivré par	Expire
⊞ Magasin de Certificats Microsoft		
⚠ Broadcom Corp Contacted SmartCard 0		

3.2 PKI options

The "PKI options" menu allows the user to further configure the way tokens and smart cards are managed. It also allows for further configuration of the access to certificates. The "PKI options" menu can be accessed through the "Tools > Options" menu.

Note: The "PKI options" menu is available both in the "PREMIUM" and "CERTIFIED" versions of TheGreenBow VPN Client.



Certificate Check

□ Check gateway certificate signature
□ Check certificate chain with CRL
☑ Certs of Gateway and Client are issued by different CA
□ Only use authentication certificate (Key usage contains "digitalSignature" attribute)

Certificate Access

□ Force PKCS#11 interface usage
□ Use the first certificate found

Token/SmartCard Reader choice

● Use the token or SC reader configured in the VPN Config.
○ Use the first token or SC reader found on this computer
○ Use the token or SC reader configured in vpnconf.ini file

Checking certificates

Check the gateway certificate's signature ⚠	Selecting this option will check the following properties of the VPN gateway certificate: validity date, certificate chain, signature of each certificate in the certificate chain. Security advisory: when this option is set, it is recommended to fill the Remote ID of the relevant VPN tunnel with the subject of the VPN Gateway certificate, in order to avoid any exploit of the vulnerability 2018_7293.
Check the certificate chain using CRL	Selecting this option will check the following properties of the VPN gateway certificate: validity date, certificate chain, signature and CRL of each certificate in the certificate chain.
VPN Gateway and Client certificates issued by different CAs	This box must be ticked if the VPN Client and VPN Gateway use certificates issued by separate certification authorities.
Only use "Authentication"-type certificates.	If this box is ticked, only "Authentication" type certificates (i.e. those for which "Key Usage" is set to "Digital signature") will be taken into account by the VPN Client. (2)

(1) The complete VPN Gateway certificate's certificate chain is checked. It is therefore strongly recommended to import the root and intermediate certificates into the Windows Certificate Store. Similarly, the CRLs relevant to the Gateway certificate will be checked as well. Therefore, these must be accessible either through the Windows Certificate Store or through download.

(2) This function can notably characterise a specific certificate among several others, when, for example, several certificates with the same subject are stored on the same token or smart card.

In the "VPN Certified" version, the gateway authentication must be carried out. This means that the three options ("Check the gateway certificate's signature", "Check the certificate chain using CRL" and "VPN Gateway and Client certificates issued by different CAs") must be selected.

Access to certificates

Force PKCS#11 use	VPN Client can manage both PKCS#11 and CSP readers. If this box is ticked, VPN Client will only take PKCS#11 readers and tokens into account.
Use the first certificate found	If this box is ticked, VPN Client will use the first certificate found on the specified smart card or token, regardless of the certificate's subject that might have been configured in the Local ID field of the "Advanced" tab of the relevant phase 1.

Selection of token/smart card reader

Use the token/smart card reader specified in the VPN Config.	The smart card readers or tokens used are memorised in the VPN Configuration. VPN Client will prioritise the readers or tokens specified in the VPN Configuration file.
Use the first token/smart card reader found	VPN Client will use the first token or smart card reader found on the workstation to obtain a certificate.
Use the token/smart card reader specified in vpnconf.ini	VPN Client will prioritise the vpnconf.ini file in order to determine which smart card readers or tokens to use. See Section 4

Warning: The vpnconf.ini file can only be used with the PKCS#11 interface. For example, a PKCS#11 middleware has to be specified in the file. See Section 4. Therefore, the option: "Use the token/smart card reader specified in vpnconf.ini" requires that the option "Force PKCS#11 use" is selected.

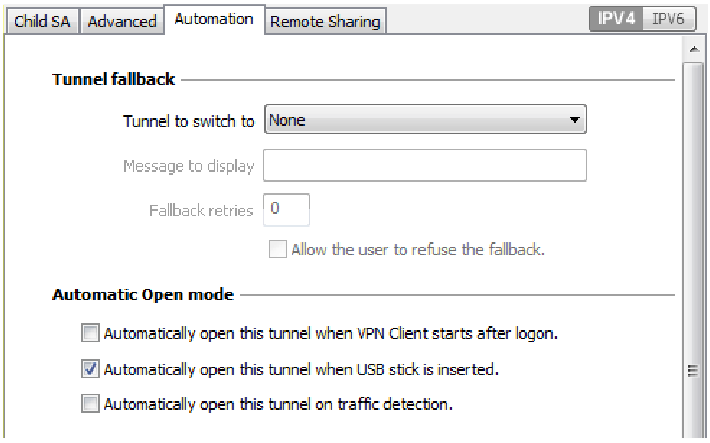
3.3 Automatic operations

Subject X509

For IKEv1 and IKEv2, the selected certificate's subject is automatically used as a connection login. It automatically appears in the "Local ID" field "Subject X509" of the "Advanced" tab.

Automatic opening and closing of the VPN tunnel

If the box "Open this tunnel automatically when a USB key is inserted" in the "Automatic operations" tab is ticked, the tunnel will automatically be opened when the user inserts a smart card and will close automatically as soon as the user removes the card.



Tunnel fallback

Tunnel to switch to: None

Message to display:

Fallback retries: 0

□ Allow the user to refuse the fallback.

Automatic Open mode

□ Automatically open this tunnel when VPN Client starts after logon.

☑ Automatically open this tunnel when USB stick is inserted.

□ Automatically open this tunnel on traffic detection.

4 VPN Client initialisation (vpnconf.ini)

TheGreenBow VPN Client recognises the smart cards or tokens issued by major manufacturers (Gemalto, Oberthur, Schlumberger, Aladdin, Safenet, Feitian etc.). A list of VPN Client-certified compatible tokens and smart cards is available on the TheGreenBow website, at the following address: http://www.thegreenbow.fr/vpn_token.html.

For the tokens or smart cards that would not be readily recognised by TheGreenBow VPN Client, it is possible to use the software to specify their characteristics in a "vpnconf.ini" file so that these might be automatically taken into account.

The vpnconf.ini file must be located in the installation folder of VPN Client (usually C:\Program Files\TheGreenBow\TheGreenBow VPN) and is editable with any regular text editor (e.g. notepad).

The parameters defined in the vpnconf.ini file are divided in two categories:

- [ATR]: This category defines the attributes of the tokens/smart cards that should be used
- [ROAMING]: This category defines the tokens or smart cards that should be used

4.1 [ATR] category

Use and limitations

- The "vpnconf.ini" file is made of a series of "ATR" blocks.
- Each ATR block defines the criteria for accessing a token or family of tokens.

- The information pertaining to the ATRs and ATR masks are provided by the smart cards manufacturers. However, should the need arise, a mask containing only FF can be configured. The lengths of the ATR and the ATR mask must be identical. The mask line can, for instance, look like this:
  +mask=FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF
- At least one of the two parameters "registry" or "dllpath" must be defined.

Parameters

Parameters	Meaning
`[ATR#]`	ATR of the token to be added
`mask`	Mask to be used with this ATR
`scname`	Name of the token (descriptive field only)
`manufacturer`	Name of the manufacturer (descriptive field only)
`pkcs11dllname`	Name of the PKCS#11 DLL
`registry`	Name of the key in the registry that indicates the path to the middleware
`dllpath`	Access path to the PKCS#11 DLL The path is the complete path. It should also contain the DLL name (see example below)

Example

```
[3B:0 F:52:4E:42:4 F:24:00:23:00:00:00:00:00:00:00:01]
mask="FF:FF:FF:FF:FF:FF:FF:00:FF:00:00:FF:FF:00:00:00:FF"
scname="Card Name"
manufacturer="Company Name"
pkcs11dllname="mdlw.dll"
dllpath="C:\Program Files (x86)\MyCompany\Model\mdlw.dll"
```

4.2 [ROAMING] category

Use and limitations

- The [ROAMING] category is used to characterise the token or smart card when the "Use the token/smart card reader specified in vpnconf.ini" option is selected (see Section 3.2), or when the software has been installed with the "smartcardroaming" option equal to 2 or 3 (see Section 5.2).

- Parameters defined in the [ROAMING] category of the vpnconf.ini file are prioritised against possible similar parameters defined in the VPN security policy (VPN configuration file).
- At least one of the two parameters, "SmartCardMiddlewareRegistry" or "SmartCardMiddlewarePath", must be defined.
- The registry access parameters must use the following syntax:
  PRIMARY_KEY:path\\to\\the\\specific\\key:value
  Example: HKEY_LOCAL_MACHINE:SOFTWARE\\Axalto\\Access\\CK:PKCS#11DLL
- "PKCS#11" is the only possible value for the parameter "SmartCardMiddlewareType".

Parameters

Parameters	Meaning
SmartCardReader	Name of the reader used for accessing the token
SmartCardMiddleware	Dll file used for communicating with the token
SmartCardMiddlewareType	PKCS#11
SmartCardMiddlewarePath	Path to the middleware including the middleware’s name
SmartCardMiddlewareRegistry	Name of the key in the registry that indicates the path to the middleware

Example

```
[ROAMING]
SmartCardReader="Axalto reader"
SmartCardMiddleware="middleware.dll"
SmartCardMiddlewareType="PKCS#11"
SmartCardMiddelwarePath="c:\path\to\middleware\mdlw.dll"
SmartCardMiddlewareRegistry="HKEY_LOCAL_MACHINE:SOFTWARE\\Axalto\\Access\\CK:PKCS#11DLL"
```

5 VPN Client setup

5.1 Software customisation

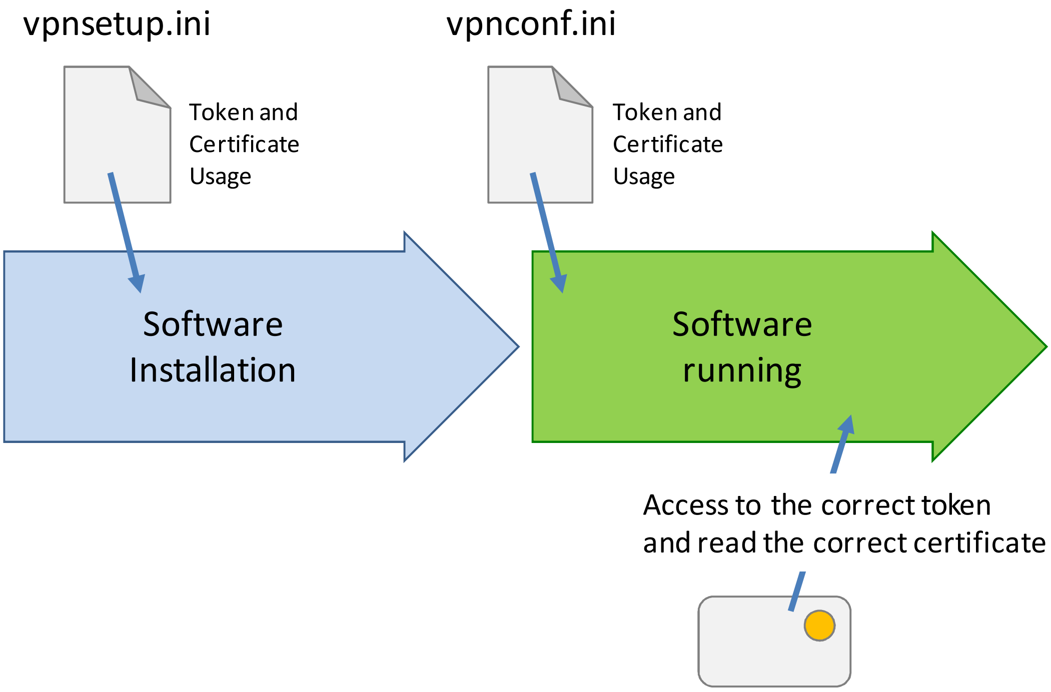
TheGreenBow VPN Client can be customised during its installation and first use using either one of the following three methods:

- Through a software installation PKI options definition file: vpnsetup.ini
- Through a set of installation command-line options
- Through a PKCS#11 parameters definition file: vpnconf.ini

The installation files must be located in the following folders:

- vpnsetup.ini must be located in the same folder as the one from which the VPN Client installation file is executed: TheGreenBow_VPN_Client.exe
- vpnconf.ini must be located in the same folder as the one in which is installed and from which the TheGreenBow VPN Client software is executed (see Section 4)

The way the PKI options parameters are taken into account is illustrated below:


vpnsetup.ini
vpnconf.ini
Token and Certificate Usage
Token and Certificate Usage
Software Installation
Software running
Access to the correct token and read the correct certificate

These different methods for configuring the software during installation are particularly relevant when deploying the VPN Client on heterogeneous platforms using different smart card readers which must use certificates that have the same characteristics (e.g. all certificates to be used are "authentication" types).

Other example: The VPN Client can be deployed on platforms equipped with unknown tokens. The configuration file enables VPN Client to recognise those tokens.

5.2 Setup configuration file: vpnsetup.ini

The vpnsetup.ini file allows the user to customise the installation of TheGreenBow VPN Client.
It must be located in the same folder as the executable installation file: TheGreenBow_VPN_Client.exe.
The vpnsetup.ini file can be edited with any standard text editor (e.g. notepad).

5.2.1 Syntax

The vpnsetup.ini file is arranged in several sections, keys and optional values.
The "PKI options" parameters are defined in the "[PKIOptions]" section.

Parameter	Section	Value	Meaning
Smartcardroaming	3.1 / 3.2	Undefined	Smart card reader configured in the VPN Configuration
			Certificate subject in the VPN Configuration
		"01"	Smart card reader configured in the VPN Configuration
			Certificate subject in the VPN Configuration is not taken into account
		"02"	Smart card reader configured in the vpnconf.ini file
			Certificate subject in the VPN Configuration
		"03"	Smart card reader configured in the vpnconf.ini file
			Certificate subject in the VPN Configuration is not taken into account
		"04"	First plugged-in reader containing a smart card
			Subject of the certificate in the VPN Configuration
		"05"	First plugged-in reader containing a smart card
			Certificate subject in the VPN Configuration is not taken into account
PKCS11Only	3.1	Undefined	The CSP mode is used by default
		"01"	Forces VPN Client to use PKCS#11 mode
KeyUsage	3.2	Undefined	Certificate type unchecked
		"01"	"Authentication"-type certificate
NoCACertReq	3.3	Undefined	
		"01"	Separate Client/Gateway certification authorities
PkiCheck	3.4	"00" or Undefined	VPN gateway certificate unchecked
		"01"	The following properties of the VPN gateway certificate are checked: validity date, certificate chain, signature and CRL of each certificate in the certificate chain
		"02"	The following properties of the VPN gateway certificate are checked: validity date, certificate chain, signature of each certificate in the certificate chain (not the CRLs)
		"03"	Identical to "01"

5.2.2 Example

```
[PKIOptions]
PkiCheck=01
SmartCardRoaming=01
NoCACertReq=01
KeyUsage=01
```

```
PKCS11Only=01
```

5.3 Installation command-line options

Two "PKI options" parameters can be specified using installation command-lines:

- pkicheck: value and meaning are identical to those described in Section 5.2
- smartcardroaming: value and meaning are identical to those described in Section 5.2

Important: The "PKI options" parameters specified in the vpnsetup.ini file take precedence over the parameters defined with command lines.

5.3.1 Syntax and use

--pkicheck

Syntax:	--pkicheck=1
Use:	this option is either undefined or assigned the value 0, 1, 2 or 3 (see Section 5.2.1)
Example:	TheGreenBow_VPN_Client.exe --pkicheck=1

--smartcardroaming

Syntax:	--smartcardroaming=1
Use:	this option is either undefined or assigned the value 1, 2, 3, 4 or 5 (see Section 5.2.1)
Example:	TheGreenBow_VPN_Client.exe --smartcardroaming=1

6 Contact

6.1 Information

All the information on TheGreenBow products is available on: www.thegreenbow.fr

6.2 Sales

Phone: +33.1.43.12.39.30
Email: sales@thegreenbow.com

6.3 Support

Several links related to support activities are available on the TheGreenBow website:

Support

http://www.thegreenbow.fr/support.html

Online help

http://www.thegreenbow.com/support_flow.html?product=vpn&lang=fr

FAQ

http://www.thegreenbow.fr/vpn_faq.html

Contact

The Technical Support department can be contacted using the forms available online or at the following address:
support@thegreenbow.com

Secure, Strong, Simple

TheGreenBow Security Software