THEGREENBOW

TheGreenBow VPN Client

Token, Smartcard Certificate and PKI Management

Table of Contents

1 Introduction

1.1 VPN Client PKI Options

This document describes the PKI facilities of TheGreenBow VPN Client. It is intended to IT managers.

TheGreenBow VPN Client implements a set of functions, options and settings that enable seamless and easy integration of the software within existing PKI, in small or large Information Systems.

These new functions enable to:

- Define the certificate to be used by the VPN Client to open a VPN tunnel
- Define the smartcard reader or the token to be used on the target computer
- Define the certificate checking rules (validity, CRL, subject, key usage, etc.)

The PKI parameters, called "PKI options", can be configured:

- Via the software interface
- Via a pre-configuration of the software setup (vpnsetup.ini file used together with the setup)
- Through a set of command line options
- Via a software initialization file, which is used when the software starts (vpnconf.ini)

This document describes the different ways to configure the PKI options.

1.2 References

The following documents are referenced in this document. They can be downloaded freely on TheGreenBow website at: http://www.thegreenbow.com/vpn_doc.html

Reference	Title	Document name
[Deployment Guide]	TheGreenBow VPN Client Deployment Guide	tgbvpn_ug_deployment_en
[User Guide]	TheGreenBow VPN Client User Guide	tgbvpn_ug_en

2 PKI Options

2.1 Token and smartcard reader characterization

TheGreenBow VPN Client is natively interoperable with a large range of tokens and smartcards.

The list of qualified tokens and smartcard – which often comes together with its configuration guide - is available on TheGreenBow website at: http://www.thegreenbow.com/vpn_token.html.

It is possible to configure the VPN Client in order to select the smartcard or the token to be used with one of the three following methods:

- The smartcard reader to be used is specified in the VPN Security Policy (VPN Configuration file).
  Note: The VPN Security Policy may be joined to the setup in order to be automatically taken into account during installation
- The smartcard reader to be used is specified in the initialization file of the software ("vpnconf.ini")
- The smartcard reader to be used is the first smartcard reader found on the computer, connected and owning a smartcard.

TheGreenBow VPN Client can access to smartcard or token middleware in CSP mode (Cryptographic Service Provider) or in PKCS#11 mode. By default, TheGreenBow VPN Client uses the CSP mode to access the middleware. However it is possible to force the VPN Client to use PKCS#11 mode.

Note: TheGreenBow VPN Client always accesses the Windows Certificate Store in CSP mode.

2.2 Certificate selection criteria

TheGreenBow VPN Client enables to characterize the certificate to be used to open a VPN Tunnel through a combination of the following criteria:

- The subject of the certificate to be used may be 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 doesn't matter: the first certificate found on the token or smartcard is used by the VPN Client

2.3 Certificate usage

A VPN Client and a VPN Gateway may use certificates issued from different certification authorities (i-e: the Client and Gateway certificates are issued from different intermediate certification authorities, which are all issued from the same certification root). TheGreenBow VPN Client is able to manage such a certificate configuration.

2.4 Certificate of the VPN Gateway

TheGreenBow VPN Client can be configured to check the certification chain of the certificate received from the VPN gateway. This feature requires importing the root certificate and all the certificates of the certification chain in the Windows Certificate Store.

TheGreenBow VPN will also use the CRL (Certification Revocation List) of each intermediate certification authority. These CRL must be accessible, either in the Windows Certificate Store or downloadable. If not, the VPN Client won't be able to check the validity of the certificate.

TheGreenBow VPN Client checks the following elements of the certification chain:

- Expiration date of the certificate
- Validity beginning date of the certificate
- Signature of each certificate of the certification chain (included the root certificate, the intermediate certificates and the server certificate)
- The update of each CRL
- Lack of certificates revocation in the relevant CRL

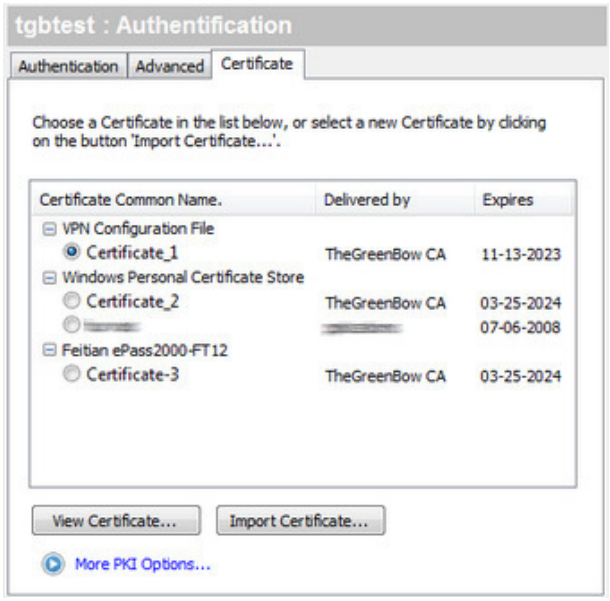
3 User interface

TheGreenBow VPN Client enables to configure the token, smartcard and certificate management from its user interface.

3.1 Certificate tab

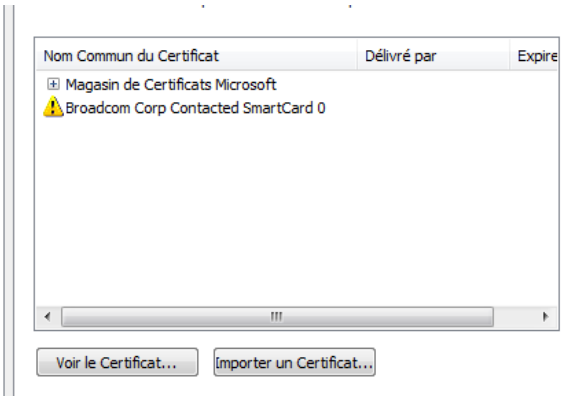
The "Certificate" tab automatically displays the list of all certificates found on a token or on a smartcard, as soon as:

- The token or smartcard is compatible with CSP or PKCS#11 mode
- The middleware of the token or smartcard is correctly installed on the computer
- If required, the smartcard is correctly inserted in the smartcard reader.



TheGreenBow VPN Client displays all certificates found on the token, which are not expired.

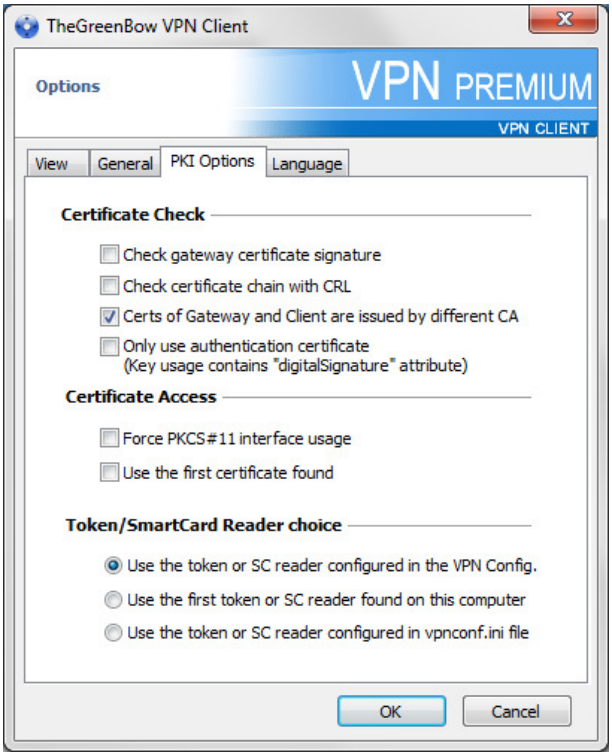
Note: When the smartcard is not inserted in the smartcard reader, the reader is displayed with a warning icon.



3.2 PKI Options

The "PKI Options" menu enables to tune the token and smartcard management.
It also enables to specify the way the certificates are taken into account.
The "PKI Options" menu can be open from the menu "Tools > Options".

Note: The "PKI Options" menu is proposed in the "PREMIUM" version of TheGreenBow VPN Client.



Certificate Check

Check gateway certificate signature	This option enables the VPN Client to check the following characteristics of the VPN gateway certificate: expiration date, certification chain, and the signature of each certificate of the certification chain (1)
Check certificate chain with CRL	This option enables the VPN Client to check the following characteristics of the VPN gateway certificate: expiration date, certification chain, and the signature and CRL (Certification Revocation List) of each certificate of the certification chain. (1)
Certs of GW and Client issued by different CA	Must be selected if the VPN Client and Gateway use certificates from a different CA.
Only use authentication certificate	When this option is checked, only the "Authentication" type Certificate (i.e. "Key Usage" is "Digital signature") is used by the VPN Client. (2)

(1) The certification chain of the VPN Gateway certificate is checked. It is therefore strongly recommended to import the root certificate and the intermediate certificates in the Windows Certificate Store.
Similarly, the CRL for the certificate of the gateway is checked. It must be downloadable or available in the Windows Certificate Store.

(2) This feature allows defining a particular certificate among multiple ones, when several certificates with the same subject, for example, are stored on the same smartcard or token.

Certificate Access

Force PKCS#11 interface usage	The VPN Client can manage PKCS#11 and CSP readers. When this option is checked, the software takes into account only PKCS#11 readers and Token.
Use the 1st certificate found	When this option is checked, the VPN Client uses the first certificate found on the specified smart card or token, regardless of the subject of the certificate that may be configured in the Local ID field of the Phase1/IKE Auth/TLS "Advanced" tab involved.

Token/Smartcard Reader choice

Use the token or SC reader configured in the VPN Configuration file	Smartcard readers or Tokens used are stored in the VPN Configuration. The VPN Client favors readers or Token specified in the VPN Configuration File.
Use the 1st token or SC reader found on this computer	The VPN Client uses the first Smart Card reader or Token found on the computer to search for a certificate
Use the token or SC reader configured in the vpnconf.ini file (1)	The VPN Client favors the configuration file vpnconf.ini to consider smart card readers or tokens to be used. See chapter 4 for the vpnconf.ini file management.

(1) The vpnconf.ini file is only used for a PKCS#11 interface. For example, the definition of the PKCS#11 middleware is required, Cf. chapter 4). Thus, the option: "Use the token or SC reader configured in the vpnconf.ini file" requires the option "Force PKCS#11 interface usage" to be checked.

3.3 Automations

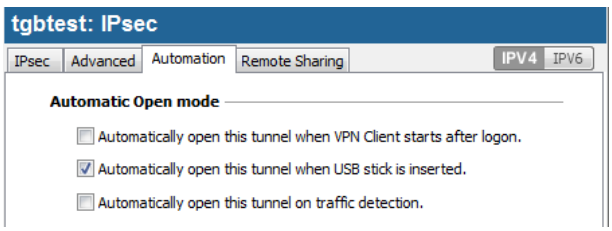
X509 subject

For IKEv1 and IKEv2 tunnels, the subject of the certificate is automatically used as a connection identifier. It automatically appears in the "Local ID" field of the tunnel ("Advanced" tab).

Tunnel automatic opening and closing

It is possible to configure the VPN Client to automatically open the VPN tunnel when the token or the smartcard is inserted, and to automatically close the VPN tunnel as soon as the token or the smartcard is removed from the computer.

This feature is configured in the "Automation" tab of the VPN tunnel, when the option "Automatically open this tunnel when USB stick is inserted" is checked.



4 VPN Client initialisation file (vpnconf.ini)

TheGreenBow VPN Client recognizes the smartcards or USB tokens from leading manufacturers (Gemalto, Oberthur, Aladdin, SafeNet, Feitian, etc.). The list of qualified tokens or smartcards is available on TheGreenBow website at: http://www.thegreenbow.com/vpn_token.html.

However, administrators have the ability to specify their own tokens or smartcards and the paths to custom middleware in an initialization file called "vpnconf.ini".

The vpnconf.ini file is automatically taken into account by the software when it starts. It must be located under the software installation directory (e.g.:"C:\Program Files\TheGreenBow\TheGreenBow VPN"). It can be edited with a text editor (e.g.: notepad.exe).

The PKI Options parameters defined in the vpnconf.ini file are divided in two sections:

- [ATR]: This section enables to define a smartcard or token attributes
- [ROAMING]: This section specifies the smartcard or token to be used

4.1 ATR Section

Usage and limitations

- An ATR section describes the parameters required by the VPN Client to access a token or a family of tokens.
- Several ATR sections can be defined in the vpnconf.ini file.
- An ATR is provided by the smartcard / token manufacturer.

- ATR and ATR mask information are provided by the manufacturer. However, in case of problem, it is possible to set a mask with only "FF" values.
- The length of the ATR and of the ATR mask must be identical. The difference between ATR and ATR mask lengths is a common error.
- The ATR mask can be as follows: "`mask=FF:FF:FF:FF:FF:...FF:FF:FF`"
- It is mandatory one of the two parameters "registry" or "DllPath" is defined.

Parameters

Parameters	Meaning
`[ATR#]`	Section name = Token Id
`mask`	ATR mask
`scname`	Token name
`manufacturer`	Vendor's name
`pkcs11DllName`	PKCS#11 DLL name
`registry`	Name of the registry key which references the path to the middleware
`DllPath`	Path to the PKCS#11 DLL files. The path must be the full path of the dll, including the name of the dll file.

Example

```
[3B:0F:52:4E:42:4F:24:00:23:00:00:00:00:00:00:01]
mask="FF:FF:FF:FF:FF:FF:00:FF:00:00:FF:FF:00:00:00:FF"
scname="Access"
manufacturer="Axalto"
pkcs11DllName="mdlw.dll"
registry="KEY_LOCAL_MACHINE:SOFTWARE\\Axalto\\Access\\CK:PKCS#11DLL"
```

4.2 [ROAMING] Section

Usage and limitations

- The [ROAMING] section is used to characterize a token or a smartcard when the option "Use the token or SC reader configured in the vpnconf.ini file" is set in the PKI Options menu (see chapter 3.2), or when the installation of the software comes with the option "smartcardroaming" set to 2 or 3 (see chapter 5).

- The parameters defined in the section [ROAMING] in the VpnConf.ini have priority over the parameters defined in the VPN Security Policy (VPN Configuration file)
- It is mandatory one of the parameters "SmartCardMiddlewareRegistry" or "SmartCardMiddlewarePath" is defined.
- "PKCS#11" is the only possible value for the parameter "SmartCardMiddlewareType".

Parameters

Parameters	Meaning
SmartCardReader	Name of the smartcard reader to be used to access the smartcard/token
SmartCardMiddleware	DLL file used to communicate with the token/smartcard
SmartCardMiddlewareType	PKCS#11
SmartCardMiddelwarePath	Path to the middleware, including the middleware name
SmartCardMiddlewareRegistry	Name of the registry key which owns the path to access 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 Customization

5.1 Software customization

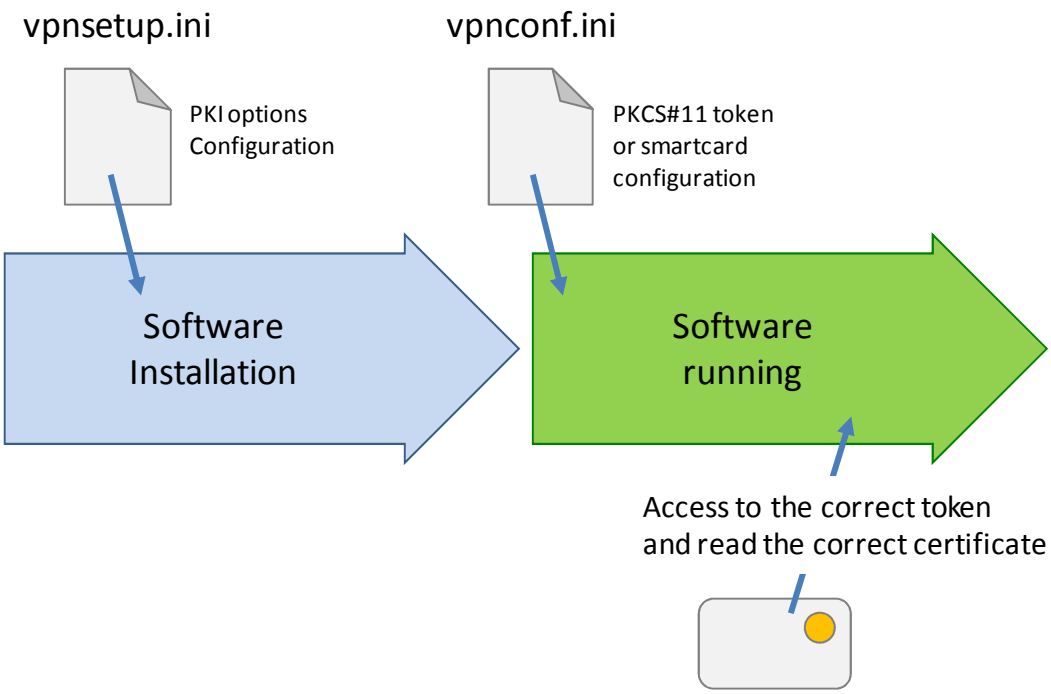
TheGreenBow VPN Client can be customized during its installation and for its first utilization via the three following ways:

- A PKI options configuration file coming together with the software setup : vpnsetup.ini
- A set of command line options available with the setup
- A PKCS#11 configuration file coming together the VPN Client software : vpnconf.ini

The initialization file must be located in the following directories:

- vpnsetup.ini must be located in the same directory as the software setup TheGreenBow_VPN_Client.exe
- vpnconf.ini must be located in the installation directory of the VPN Client (see chapter 4)

The way the various PKI options are taken into account during the software installation is as follows:



Example: The deployment facilities enable to prepare a software deployment over computers equipped with various smartcard readers, from which a certificate with a specific subject has to be used to open VPN tunnels.

5.2 Setup configuration file: VpnSetup.ini

The "VpnSetup.ini" file enables to configure the installation of TheGreenBow VPN Client.
It must be located in the directory where the setup is ran: TheGreenBow_VPN_Client.exe.
The "VpnSetup.ini" file can be edited with a text editor (e.g.: notepad.exe)

5.2.1 Syntax

In the VpnSetup.ini file, the PKI Options parameters are defined in the section: [PKIOptions]

Parameter	Chapter	Value	Meaning
Smartcardroaming	3.1 / 3.2	Undefined	The smartcard reader is defined in the VPN Configuration file
			The certificate subject is defined in the VPN Configuration file
		"01"	The smartcard reader is defined in the VPN Configuration file
			The certificate subject from the configuration file is ignored
		"02"	The smartcard reader is defined in the VpnConf.ini file
			The certificate subject is defined in the VPN Configuration file
		"03"	The smartcard reader is defined in the VpnConf.ini file
			The certificate subject from the configuration file is ignored
		"04"	First smartcard reader that owns a smartcard
			The certificate subject is defined in the VPN Configuration file
		"05"	First smartcard reader that owns a smartcard
			The certificate subject from the configuration file is ignored
PKCS11Only	3.1	Undefined	The CSP mode is used (default)
		"01"	Force the VPN Client to use the PKCS#11 mode
KeyUsage	3.2	Undefined	The certificate type isn't checked
		"01"	The certificate must be with a type: "Authentication"
NoCACertReq	3.3	Undefined	The VPN Client doesn't handle certificates issued from different CA
		"01"	The VPN Client handles certificates issued from different CA
PkiCheck	3.4	"00" or Undefined	The gateway certificate isn't checked
		"01"	This option enables the VPN Client to check the following characteristics of the VPN gateway certificate: expiration date, certification chain, and the signature and CRL (Certification Revocation List) of each certificate of the certification chain
		"02"	This option enables the VPN Client to check the following characteristics of the VPN gateway certificate: expiration date, certification chain, and the signature of each certificate of the certification chain (no CRL is checked)
		"03"	Identical to "01"

5.2.2 Example

```
[PKIOptions]
PkiCheck=01
SmartCardRoaming=01
NoCACertReq=01
KeyUsage=01
PKCS11Only=01
```

5.3 Setup command line options

The PKI options parameters which can be specified in the Setup Command Line are:

- pkicheck: same value and meaning as defined in chapter 5.2
- smartcardroaming: same value and meaning as defined in chapter 5.2

Important: the PKI options parameters specified in the VpnSetup.ini file have priority over parameters from the command line.

5.3.1 Syntax and usage

--pkicheck

Syntax: --pkicheck=1
Usage: This option is either undefined or defined with value 0 to 3
Example: TheGreenBow_VPN_Client.exe --pkicheck=1

--smartcardroaming

Syntax: --smartcardroaming=1
Usage: This option is either undefined or defined with value 1 to 5
Example: TheGreenBow_VPN_Client.exe --smartcardroaming=1

6 Contact

6.1 Information

All TheGreenBow products information is available on: www.thegreenbow.com

6.2 Sales

Phone: +33.1.43.12.39.30
Email: sales@thegreenbow.com

6.3 Support

Different pages concerning the support are available on TheGreenBow website:

Support

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

Online help

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

FAQ

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

Contact

Technical support is available through the inline forms or directly at: support@thegreenbow.com

THEGREENBOW

Secure, Strong, Simple

TheGreenBow Security Software