THEGREENBOW

TheGreenBow
VPN Certified

Gestion des PKI certificats, tokens et cartes à puce

Table des Matières

1 Introduction

1.1 Options PKI

Ce document décrit les facilités proposées par le logiciel TheGreenBow VPN Client pour son intégration dans toute PKI. Il est destine à l'administrateur sécurité.

Le Client VPN TheGreenBow implémente un ensemble de fonctions, options et paramètres qui lui permettent de s'intégrer dans toute PKI existante, que ce soit dans de larges infrastructures ou sur de petites configurations.

Les fonctions PKI permettent :
- De caractériser le certificat que le Client VPN doit utiliser pour ouvrir un tunnel VPN
- De définir le token ou le lecteur de carte à puce à utiliser sur le poste utilisateur
- De configurer un ensemble de règles pour la vérification du certificat (validité, CRL, key usage, etc.)

Les paramètres PKI peuvent être configurés :
- Via l'interface utilisateur du logiciel
- Via une pré-configuration de l'installeur du logiciel (vpnsetup.ini associé au setup du logiciel)
- Grâce à un ensemble d'options de ligne de commande
- Via un fichier d'initialisation du logiciel en cours d'exécution (vpnconf.ini)

Ce document s'attache à décrire toutes les possibilités de configuration des options PKI au cours du déploiement du logiciel. En ce sens, il s'adresse à l'administrateur, plutôt qu'à l'utilisateur.

Ce document est une extension du "Guide de Déploiement du Client VPN TheGreenBow'".

1.2 Références

Les documents suivants sont référencés dans la suite de ce document. Ils sont disponibles en téléchargement sur le site TheGreenBow: http://www.thegreenbow.fr/vpn_doc.html.

Référence	Titre	Nom du document
[Guide de déploiement]	Guide de déploiement du Client VPN TheGreenBow	tgbvpn_ug_deployment_fr
[Guide Utilisateur]	Guide Utilisateur du Client VPN TheGreenBow	tgbvpn_ug_fr

1.3 Terminologie

Mode CSP

Le mode CSP signifie "Cryptographic Service Provider". Ce mode d'accès aux tokens et aux cartes à puce est fourni par Microsoft. Il ne requiert pas de configuration supplémentaire dans le Client VPN TheGreenBow.
A noter : ce mode n'est pas supporté par tous les tokens/cartes à puces.

Mode PKCS#11

PKCS#11 est une API d'accès aux tokens ou aux cartes à puce (standardisée par RSA Labs).

Les tokens sont généralement compatibles PKCS#11.
Ce mode requiert une DLL fournie par le fabricant du token dans un package d'installation du middleware.
Ce package doit être installé sur l'ordinateur avant d'utiliser le Client VPN TheGreenBow.

Certaines DLL sont aujourd'hui identifiées et reconnues automatiquement par le Client VPN TheGreenBow. Certaines DLL ne le sont pas et doivent être configurées (Cf. chapitre "vpnconf.ini").

ATR

ATR signifie "Answer To Reset". C'est un identifiant retourné par le token ou la carte à puce sur commande reset.
Cet identifiant est lié au fabricant et au modèle de token ou de carte à puce.

Le Client VPN TheGreenBow connait un certain nombre d'ATR, associé à la DLL à utiliser. Dans ce cas, il n'est pas nécessaire de configurer la DLL : elle est identifiée automatiquement.
Dans le cas contraire (Le Client VPN ne connait pas l'ATR), il est nécessaire de configurer le token dans le Client VPN. Cette configuration s'effectue dans un fichier d'initialisation "vpnconf.ini" (Cf chapitre "vpnconf.ini").

2 Options PKI

2.1 Caractérisation des Tokens et Lecteurs de carte à puce

Le Client VPN TheGreenBow est nativement interopérable avec une grande variété de tokens et de cartes à puce.
La liste des tokens et cartes à puce qualifiés, dont plusieurs accompagnés de leur guide de configuration, est disponible sur le site TheGreenBow sur la page: http://www.thegreenbow.fr/vpn_token.html

Il est possible de configurer le Client VPN pour qu'il sélectionne le token ou la carte à puce à utiliser de trois façons différentes :

- Le lecteur de carte à utiliser est spécifié dans la politique de sécurité VPN (fichier de configuration VPN)
  Note : Une politique de sécurité VPN peut être jointe au setup de façon à ce qu'elle soit automatiquement prise en compte au moment de l'installation.
- Le lecteur de carte à utiliser peut être spécifié dans le fichier d'initialisation du logiciel "vpnconf.ini"
- Le lecteur de carte à utiliser est le premier trouvé sur le poste utilisateur, qui contient une carte à puce.

Le Client VPN TheGreenBow accède aux tokens ou aux lecteurs de cartes à puce en mode CSP (Cryptographic Service Provider) ou en mode PKCS#11. Par défaut, le Client VPN utilise le mode CSP pour accéder au middleware. Il est toutefois possible de forcer le Client VPN à accéder au middleware en mode PKCS#11.

Note : Le Client VPN TheGreenBow accède au magasin de certificat Windows en mode CSP.

2.2 Critères de sélection du certificat

Le Client VPN TheGreenBow permet de caractériser le certificat à utiliser pour ouvrir un tunnel VPN grâce à la combinaison des critères suivants :

- Le sujet du certificat à utiliser est configuré dans la politique de sécurité VPN (fichier de configuration VPN)
- Le type de certificat à utiliser est "Authentification" (i.e. : son "key usage" contient l'attribut "Digital signature")
- Le sujet du certificat n'est pas pris en compte : c'est le premier certificat trouvé sur le token ou la carte à puce qui est utilisé.

2.3 Exploitation des certificats

Un Client VPN et une Gateway VPN peuvent utiliser des certificats issus d'autorités de certification différentes (i.e. : Les certificats du Client et de la Gateway sont issus d'autorités de certification intermédiaires différentes, placées sous une même autorité de certification racine). Le Client VPN TheGreenBow permet de gérer cette configuration des certificats.

2.4 Certificat de la passerelle VPN

Il est possible de forcer le Client VPN TheGreenBow à vérifier la chaîne de certification du certificat reçu de la passerelle VPN.

Cela nécessite d'importer le certificat racine et tous les certificats de la chaîne de certification (l'autorité de certification racine et les autorités de certification intermédiaires) dans le magasin de certificats Windows.

Le Client VPN utilisera aussi la CRL (Certificate Revocation List) des différentes autorités de certification.
Si ces CRL sont absentes du magasin de certificats, ou si ces CRL ne sont pas téléchargeables à l'ouverture du tunnel VPN, le Client VPN ne sera pas en mesure de valider le certificat de la passerelle.

La vérification de chaque élément de la chaîne implique :

- la vérification de la date d'expiration du certificat
- la vérification de la date de début de validité du certificat
- la vérification des signatures de tous les certificats de la chaîne de certificats (y compris le certificat racine, certificats intermédiaires et le certificat du serveur)
- la mise à jour des CRL de tous les émetteurs de certificats de la chaîne de certification
- la vérification de l'absence de révocation de certificats dans les listes de CRL correspondantes

Dans la version "VPN Certified", l'authentification de la passerelle doit être mise en œuvre. Voir à ce titre la recommandation de configuration au chapitre 3.2.

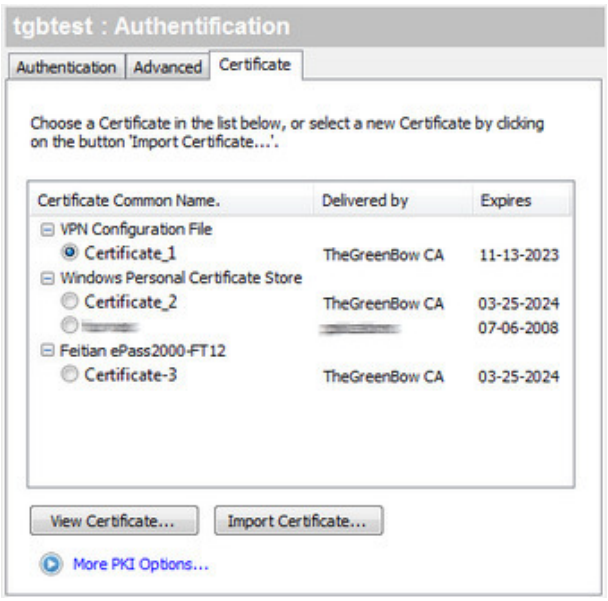
3 Interface de configuration

Le Client VPN TheGreenBow permet de configurer la gestion les tokens, cartes à puce et certificats depuis son interface principale.

3.1 Onglet certificat

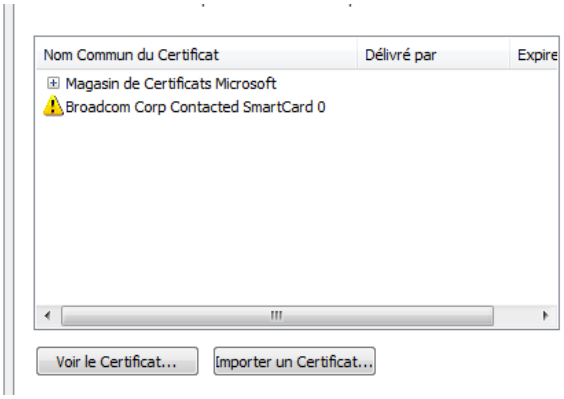
L'onglet "Certificats" affiche automatiquement la liste de tous les certificats trouvés sur le token ou la carte à puce, dès lors que :

- Le token ou la carte à puce est compatible CSP ou PKCS#11
- Le middleware du token ou de la carte à puce est correctement installé sur l'ordinateur
- Le cas échéant, la carte à puce est correctement insérée dans le lecteur associé.



Le client affiche les certificats présents sur la carte qui ne sont pas périmés.

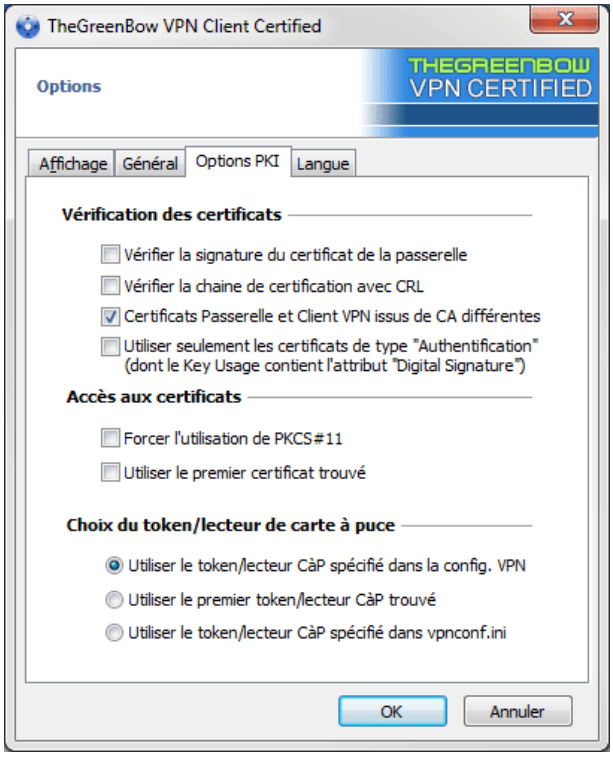
Note : Dans le cas d'un lecteur de carte à puce, le lecteur est affiché précédé d'une icône d'alerte si la carte à puce n'est pas insérée.



3.2 Options PKI

Le menu "Options PKI" permet d'affiner la gestion des tokens et cartes à puce. Il permet aussi de caractériser plus finement l'accès aux certificats. Le menu "Options PKI" est accessible par le menu "Outils > Options ".

Note : Le menu "Options PKI" est proposé dans la version "PREMIUM" et "CERTIFIED" du Client VPN TheGreenBow.



Vérification des certificats

Vérifier la signature du certificat de la passerelle	Lorsque cette option est sélectionnée, les caractéristiques suivantes du certificat de la passerelle VPN sont vérifiées : date de validité, chaîne de certification, signature de chaque certificat de la chaîne de certification.
Vérifier la chaîne de certification avec CRL	Lorsque cette option est sélectionnée, les caractéristiques suivantes du certificat de la passerelle VPN sont vérifiées : date de validité, chaîne de certification, signature et CRL de chaque certificat de la chaîne de certification.
Certificats Passerelle et Client VPN issus de CA différentes	Si le Client VPN et la Passerelle VPN utilisent des certificats issus d'une autorité de certification différente, cette case doit être cochée.
Utiliser seulement les certificats de type "Authentification"	Lorsque cette option est cochée, seuls les Certificats de type "Authentification" (c'est-à-dire dont le "Key Usage" est à "Digital signature") sont pris en compte par le Client VPN. (2)

(1) La chaîne de certification complète du certificat de la Passerelle VPN est vérifiée. Il est donc vivement conseillé d'importer le certificat racine et les certificats intermédiaires dans le Magasin de Certificats Windows. De même, les CRL concernant le certificat de la Passerelle sont vérifiées. Elles doivent donc être accessibles (soit dans le Magasin de Certificat Windows, soit téléchargeables)

(2) Cette fonction permet en particulier de caractériser un Certificat parmi N, lorsque plusieurs certificats ayant par exemple le même sujet, sont stockés sur la même Carte à puce ou le même Token.

Dans la version "VPN Certified", l'authentification de la passerelle doit être mise en œuvre. A ce titre, les trois options "Vérifier la signature du certificat de la passerelle", "Vérifier la chaîne de certification avec CRL" et "Certificats Passerelle et Client VPN issus de CA différentes" doivent être sélectionnées.

Accès aux certificats

Forcer l'utilisation de PKCS#11	Le Client VPN sait gérer les lecteurs PKCS11 et CSP. Lorsque cette option est cochée, le Client VPN ne prend en compte que les lecteurs et Tokens PKCS11.
Utiliser le premier certificat trouvé	Lorsque cette option est cochée, le Client VPN utilise le premier certificat trouvé sur la Carte à puce ou le Token spécifié, sans tenir compte du sujet du certificat éventuellement configuré dans le champ Local ID de l'onglet "Avancé" de la phase 1 concernée.

Choix du Token / Lecteur de carte à puce

Utiliser le token/lecteur CàP spécifié dans la Config. VPN	Les lecteurs de carte à puce ou les Tokens utilisés sont mémorisés dans la Configuration VPN. Le Client VPN privilégie les lecteurs ou Token spécifiés dans le fichier de Configuration VPN.
Utiliser le premier token/lecteur CàP trouvé	Le Client VPN utilise le premier lecteur de Carte à puce ou le premier Token trouvé sur le poste pour y chercher un certificat.
Utiliser le token/lecteur CàP spécifié dans vpnconf.ini	Le Client VPN privilégie le fichier configuration vpnconf.ini pour identifier les lecteurs de carte à puce ou les Tokens à utiliser. Voir le chapitre 4

Attention : L'utilisation du fichier vpnconf.ini ne s'applique qu'à l'interface PKCS#11. Par exemple, un middleware PKCS#11 doit y être spécifié, Cf. chapitre 4. Donc, l'option : "Utiliser le token/CàP spécifié dans vpnconf.ini" requiert que l'option "Forcer l'utilisation de PKCS#11" soit sélectionnée.

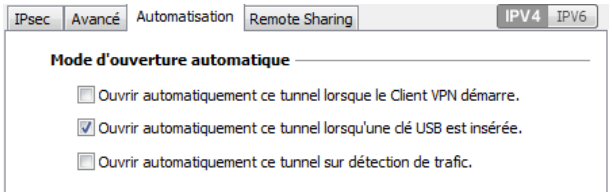
3.3 Automatismes

Sujet X509

Pour IKEv1 et IKEv2, le sujet du certificat sélectionné est automatiquement utilisé comme identifiant de connexion. Il apparaît automatiquement dans le champ "Local ID" "Sujet X509" de l'onglet "Avancé".

Ouverture et fermeture automatique du tunnel VPN

Lorsque la case "Ouvrir automatiquement ce tunnel lorsqu'une clé USB est insérée" est sélectionnée dans l'onglet "Automatisation", le tunnel s'ouvre automatiquement lorsque l'utilisateur insère sa carte à puce et il se ferme automatiquement dès que l'utilisateur extrait sa carte à puce.



4 Initialisation du Client VPN (vpnconf.ini)

Le Client VPN TheGreenBow reconnaît les cartes ou les tokens des principaux fabricants (Gemalto, Oberthur, Schlumberger, Aladdin, Safenet, Feitian, etc.). La liste des tokens et cartes à puce qualifiées avec le Client VPN est disponible sur le site TheGreenBow à l'adresse : http://www.thegreenbow.fr/vpn_token.html

Pour les tokens ou cartes à puce qui ne sont pas reconnus en standard par le Client VPN TheGreenBow, le logiciel offre la possibilité de spécifier leurs caractéristiques de façon à les prendre en compte automatiquement, dans un fichier "vpnconf.ini".

Le fichier VpnConf.ini doit être situé dans le répertoire d'installation du client VPN (généralement C:\Program Files\TheGreenBow\TheGreenBow VPN), il est éditable avec un éditeur texte classique (p.ex. notepad)

Les paramètres définis dans le fichier vpnconf.ini sont répartis en deux sections :

- [ATR]: Cette section définit les attributs des tokens / carte à puce à utiliser
- [ROAMING]: Cette section permet de définir les tokens ou carte à puce à utiliser

4.1 Section ATR

Utilisation et limitations

- Le fichier "vpnconf.ini" est constitué d'une succession de sections "ATR".
- Chaque section ATR décrit les caractéristiques nécessaires pour accéder à un token ou à une famille de tokens.

- Les informations relatives aux ATR et aux masques des ATR sont fournies par les fabricants de cartes à puce. Toutefois, en cas de problème, un masque ne contenant que FF peut être configuré. Les longueurs de l'ATR et du masque doivent être identiques. La ligne mask peut ainsi prendre la forme suivante :
  mask=FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF
- L'un au moins des deux paramètres "registry" ou "DllPath" doit obligatoirement être défini.

Paramètres

Paramètres	Signification
`[ATR#]`	ATR du token à ajouter
`mask`	Masque à utiliser avec cet ATR
`scname`	Nom du token (champ purement descriptif).
`manufacturer`	Nom du constructeur (champ purement descriptif)
`pkcs11DllName`	Nom de la dll pkcs11
`registry`	Nom de la clef en base de registre indiquant le chemin vers le middleware
`DllPath`	Chemin d'accès à la DLL PKCS#11. Le chemin est le chemin complet. Il doit contenir aussi le nom de la DLL (Cf. exemple ci-dessous)

Exemple

```
[3B:0F:52:4E:42:4F: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 Section [ROAMING]

Utilisation et limitations

- La section [ROAMING] est utilisée pour caractériser le token ou la carte à puce à utiliser lorsque l'option "Utiliser le lecteur token/CàP spécifié dans vpnconf.ini" est sélectionnée (voir chapitre 3.2) ou lorsque l'installation du logiciel a été effectuée avec l'option "smartcardroaming" égale à 2 ou 3 (voir chapitre 5.2).

- Les paramètres définis dans la section [ROAMING] du fichier vpnconf.ini sont prioritaires par rapport aux éventuels paramètres similaires définis dans la politique de sécurité VPN (fichier de configuration VPN)
- L'un au moins des deux paramètres "SmartCardMiddlewareRegistry" ou "SmartCardMiddlewarePath" doit être défini.
- Les paramètres d'accès à la base de registre doivent respecter la syntaxe suivante :
  CLEF_PRIMAIRE :chemin\\vers\\la\\clef\\specifique:valeur
  Exemple : HKEY_LOCAL_MACHINE:SOFTWARE\\Axalto\\Access\\CK:PKCS#11DLL
- "PKCS#11" est la seule valeur possible pour le paramètre "SmartCardMiddlewareType".

Paramètres

Paramètres	Signification
SmartCardReader	Nom du reader à utiliser pour accéder au token
SmartCardMiddleware	Fichier dll utilisé pour communiquer avec le token
SmartCardMiddlewareType	PKCS#11
SmartCardMiddelwarePath	Chemin vers le middleware incluant le nom du middleware
SmartCardMiddlewareRegistry	Nom de la clef en base de registre indiquant le chemin vers le middleware

Exemple

```
[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 Setup du Client VPN

5.1 Customisation du logiciel

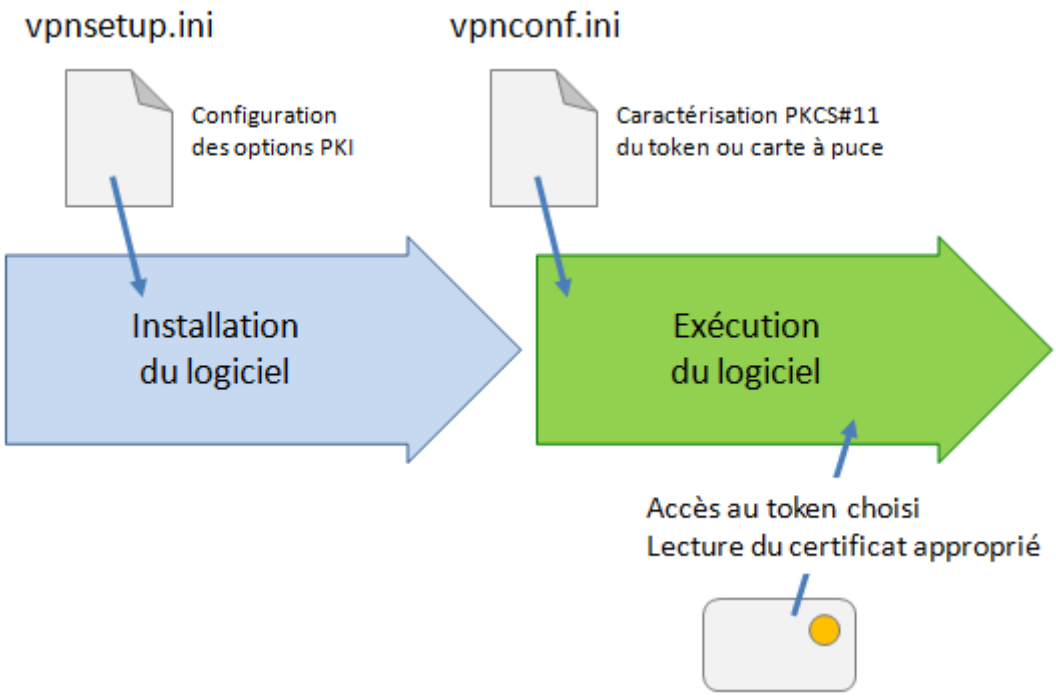
Le Client VPN TheGreenBow peut être customisé pendant son installation et lors de sa première utilisation via les trois moyens suivants :

- Dans un fichier de définition des options PKI de l'installation du logiciel : vpnsetup.ini
- Un ensemble d'options de ligne de commande de l'installation
- Dans un fichier de définition des paramètres PKCS#11 : vpnconf.ini

Les fichiers d'initialisation doivent être situés dans les répertoires suivants :

- vpnsetup.ini doit être situé dans le même répertoire que celui dans lequel est exécutée l'installation du Client VPN : TheGreenBow_VPN_Client.exe
- vpnconf.ini doit être situé dans le même répertoire que celui dans lequel est installé et s'exécute le logiciel Client VPN TheGreenBow (voir chapitre 4)

La façon dont les paramètres options PKI sont pris en compte est représentée ci-dessous :



Ces différents moyens de configuration du logiciel au cours de son installation, permettent par exemple de préparer le déploiement du Client VPN sur des plates-formes hétérogènes, équipées de lecteurs de cartes à puce différents, mais dont les certificats à exploiter présentent les mêmes caractéristiques (par exemple, les certificats à utiliser sont de type "authentification").

Autre exemple : Le Client VPN peut être déployé sur des plates-formes équipées de tokens qui lui sont inconnus. Le fichier de configuration permet au Client VPN de les reconnaître.

5.2 Fichier de configuration du setup : vpnsetup.ini

Le fichier vpnsetup.ini permet de configurer l'installation du Client VPN TheGreenBow.
Il doit être situé dans le même répertoire que l'exécutable d'installation : TheGreenBow_VPN_Client.exe.
Le fichier vpnsetup.ini peut être édité avec un éditeur de texte classique (p.ex. notepad)

5.2.1 Syntaxe

Le fichier VpnSetup.ini se compose de plusieurs sections, clés et valeurs optionnelles.
Les paramètres "Options PKI" sont définis dans la section "[PKIOptions]".

Paramètre	Chapitre	Valeur	Signification
Smartcardroaming	3.1 / 3.2	Non défini	Lecteur de Carte configuré dans la Configuration VPN
			Sujet du certificat dans la Configuration VPN
		"01"	Lecteur de Carte configuré dans la Configuration VPN
			Le sujet du certificat dans la config. VPN n'est pas pris en compte
		"02"	Lecteur de Carte configuré dans le fichier VpnConf.ini
			Sujet du certificat dans la Configuration VPN
		"03"	Lecteur de Carte configuré dans le fichier VpnConf.ini
			Le sujet du certificat dans la config. VPN n'est pas pris en compte
		"04"	1er lecteur de carte branché contenant une carte à puce
			Sujet du certificat dans la Configuration VPN
		"05"	1er lecteur de carte branché contenant une carte à puce
			Le sujet du certificat dans la config. VPN n'est pas pris en compte
PKCS11Only	3.1	Non défini	Le mode CSP est utilisé par défaut
		"01"	Force le Client VPN à utiliser le mode PKCS#11
KeyUsage	3.2	Non défini	Type du certificat non vérifié
		"01"	Certificat de type "Authentification"
NoCACertReq	3.3	Non défini	
		"01"	Autorités de certification Client / Passerelle différentes
PkiCheck	3.4	"00" ou Non défini	Certificat de la Passerelle VPN non vérifié
		"01"	Les caractéristiques suivantes du certificat de la passerelle VPN sont vérifiées : date de validité, chaîne de certification, signature et CRL de chaque certificat de la chaîne de certification.
		"02"	Les caractéristiques suivantes du certificat de la passerelle VPN sont vérifiées : date de validité, chaîne de certification, signature de chaque certificat de la chaîne de certification (pas les CRLs)
		"03"	Identique à "01"

5.2.2 Exemple

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

```
PKCS11Only=01
```

5.3 Options de ligne de commande de l'installation

Deux paramètres "Options PKI" peuvent être spécifiés en ligne de commande de l'installation :

- pkicheck : valeur et signification identiques à celles décrites au chapitre 5.2
- smartcardroaming : valeur et signification identiques à celles décrites au chapitre 5.2

Important : Les paramètres "Options PKI" spécifiés dans le fichier vpnsetup.ini ont priorité sur les paramètres passés en ligne de commande.

5.3.1 Syntaxe et utilisation

--pkicheck

Syntaxe : --pkicheck=1
Usage : Cette option est soit non définie, soit définie avec les valeurs 0, 1, 2 ou 3 (voir chapitre 5.2.1)
Exemple : TheGreenBow_VPN_Client.exe --pkicheck=1

--smartcardroaming

Syntaxe : --smartcardroaming=1
Usage : Cette option est soit non définie, soit définie avec la valeur 1, 2, 3, 4 ou 5 (voir chapitre 5.2.1)
Exemple : TheGreenBow_VPN_Client.exe --smartcardroaming=1

6 Contact

6.1 Information

Toutes les informations sur les produits TheGreenBow sont disponibles sur : www.thegreenbow.fr

6.2 Commercial

Téléphone : +33.1.43.12.39.30
Email: sales@thegreenbow.com

6.3 Support

Plusieurs liens concernant le support sont disponibles sur le site TheGreenBow :

Support

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

Aide en ligne

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

FAQ

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

Contact

Le support technique est disponible via les formulaires en ligne ou à l'adresse mail : support@thegreenbow.com

THEGREENBOW

Secure, Strong, Simple

TheGreenBow Security Software