Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2020/41

TheGreenBow VPN Client (version 6.52.006)

Paris, le 16 juin 2020

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD
[ORIGINAL SIGNÉ]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CC-2020/41**
Nom du produit **TheGreenBow VPN Client**
Référence/version du produit **version 6.52.006**
Conformité à un profil de protection **PP Application VPN Cliente** **référence PP-VPNC-CCv3.1** **version 1.3, juin 2008**
Critères d'évaluation et version **Critères Communs version 3.1 révision 4**
Niveau d'évaluation **EAL 3 augmenté** **ALC_FLR.3 et AVA_VAN.3**
Développeur : **TheGreenBow** **28 rue de Caumartin, 75009 Paris, France**
Commanditaire **TheGreenBow** **28 rue de Caumartin, 75009 Paris, France**
Centre d'évaluation **Oppida** **4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France**
Accords de reconnaissance applicables : **Aucun**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par l'Agence nationale de la sécurité de la sécurité attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est une application logicielle « TheGreenBow VPN Client », version 6.52.006, développée par la société *THEGREENBOW*.

Ce produit offre le service de client VPN (Virtual Private Network) IPSec/SSL pour des machines fixes ou nomades s'exécutant sous Windows 7 (64 bit) et Windows 10 (64 bit). Il permet d'établir un lien de communication sécurisé entre le poste de travail et une passerelle VPN placée à l'entrée d'un réseau distant sécurisé. Ce lien peut être réalisé au travers d'internet ou d'un réseau d'entreprise.

1.2. Description du produit

1.2.1. Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

La cible de sécurité a une conformité démontable au profil de protection [PP].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'établissement de connexions sécurisées via les protocoles IKEv2 et ESP en mode « tunnel » ;
- la génération d'événements d'audit (*logs*) ;
- la protection de l'accès à la politique de sécurité VPN ;
- l'import / export de la politique de sécurité VPN ;
- l'authentification par un certificat stocké soit dans « Windows certificate store », soit dans un « token » ou une carte à puce ;
- des mécanismes d'anti-rejeu s'appliquant aux données applicatives transportées dans le tunnel VPN.

Pour plus de détails, le lecteur pourra se reporter au § 1.5 « Limites de la TOE » de [ST].

1.2.3. Architecture

L'architecture logicielle du produit est constituée :

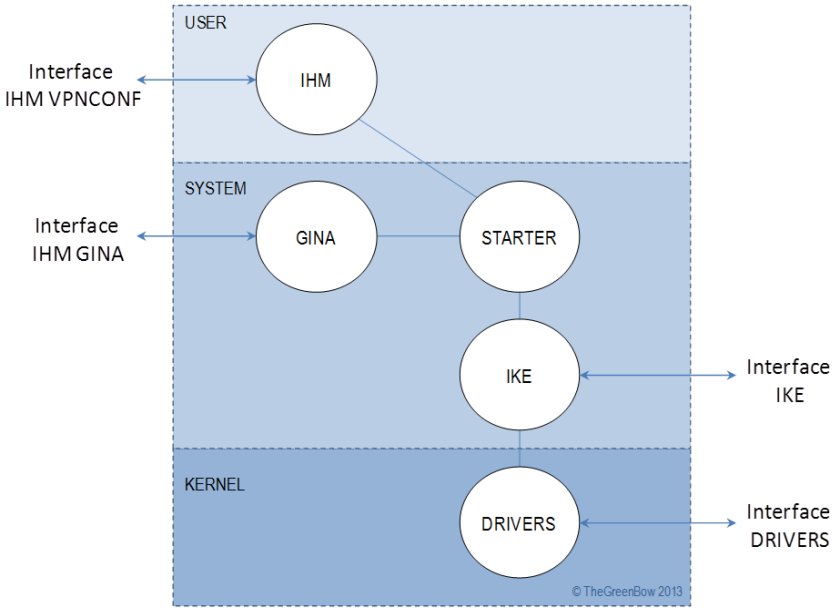


Figure 1 - Architecture du produit

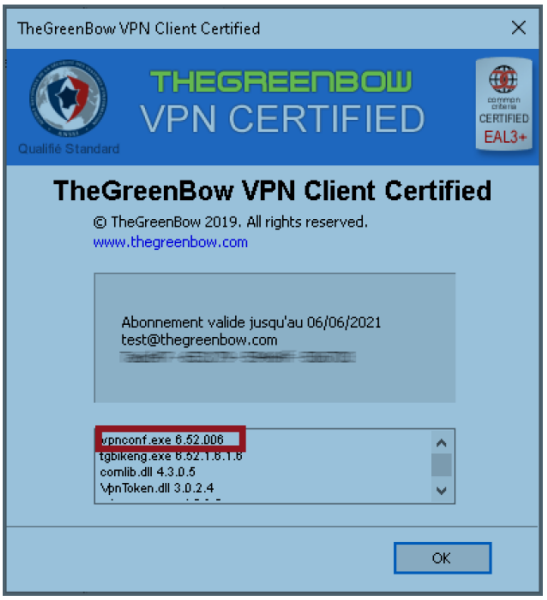
La description des sous-systèmes est la suivante :

- IHM (Interface Homme Machine) : ce sous-système a pour rôle la gestion des interactions avec l'utilisateur (préalablement authentifié par le système d'exploitation *WINDOWS*) ;
- GINA (*Graphical Identification and Authentication*) : ce sous-système a pour rôle l'ouverture et la fermeture des tunnels VPN avant l'authentification *WINDOWS* de l'utilisateur ;
- STARTER : ce sous-système a pour rôle la gestion des communications entre l'IHM / GINA et IKE et la surveillance des processus ;
- IKE (*Internet Key Exchange*) : ce sous-système de type *deamon* a pour rôle d'assurer la négociation des tunnels et des clés ;
- DRIVERS : ce sous-système a pour rôle l'interception des flux entrants et sortants pour l'application de la politique de sécurité VPN.

1.2.4. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable en se reportant au nom commercial de la TOE inscrit dans la bannière du logiciel et dans la fenêtre « A propos ».



1.2.5. Cycle de vie

Le produit a été développé sur le site suivant :

TheGreenBow

28 rue de Caumartin
75009 Paris
France

Pour l'évaluation, il a été considéré les rôles suivants :

- utilisateur : il s'agit de l'usager de la machine hébergeant la TOE qui utilise l'application VPN cliente pour accéder au réseau privé de l'organisation. Cet utilisateur peut envoyer ou recevoir des informations vers ou de ce réseau privé à travers un lien VPN établi entre l'application VPN cliente et le chiffreur IP ;
- administrateur systèmes et réseau : il s'agit de l'administrateur responsable de la machine hébergeant la TOE. Il configure les paramètres de la machine (comme les comptes utilisateurs), les paramètres réseaux de l'application VPN cliente et les paramètres systèmes qui sont liés aux contextes réseaux opérationnels, mais ne définit pas les politiques de sécurité VPN ;
- administrateur sécurité : il s'agit de l'administrateur responsable de la gestion des éléments de sécurité de la TOE. Il génère et distribue les clés dans l'application VPN cliente et importe les politiques de sécurité VPN et leurs contextes de sécurité que sont appliqués à l'application VPN cliente.

1.2.6. Configuration évaluée

La plateforme de tests *THEGREENBOW* utilisée lors de l'évaluation, est celle décrite au §7.7 de la cible de sécurité (voir [ST]).

Parmi les options possibles de configuration du produit, certaines fonctions sont en dehors du périmètre de l'évaluation. Le tableau ci-dessous présente les différentes fonctions disponibles et précise si elles sont incluses ou non dans le périmètre de cette évaluation.

	Fonctions	Périmètre de l'évaluation
Protocoles	IKEv1/IPsec	Non
	IKEv2/IPsec	Oui
	SSL/TLS	Non
Gestion de configuration VPN	Protection de l'accès à la politique de sécurité VPN	Oui
	Import/export de la politique de sécurité VPN	Oui
	Gestion centralisée des politiques de sécurité VPN, télé administration	Non
Mécanismes d'authentification	Clé partagée (PSK)	Non
	EAP	Non
	X509	Oui
	Certificat dans la configuration VPN	Non
	Certificat dans Windows Certificate Store	Oui
	Certificat sur Token/carte à puce	Oui
	Authentification passerelle	Oui
Algorithmes	Algorithmes cryptographiques	Oui
Réseau	Mode CP	Oui
	Split tunneling	Oui
Fonctions diverses	Génération de logs	Oui
	USB mode (mode nomade)	Non
	Mode « VPN point à point »	Non

Il convient d'ajouter que la TOE ne comporte pas d'interface d'administration distante (type télégestion) pour la mise à jour des politiques VPN.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC], (et) à la méthodologie d'évaluation définie dans le manuel [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 8 juin 2020, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI. Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

Dans le cadre du processus de qualification standard, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI. Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas du produit était en dehors du périmètre de l'évaluation, il n'a pas été analysé.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « TheGreenBow VPN Client, version 6.52.006 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants ALC_FLR.3 et AVA_VAN.3.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre scrupuleusement les recommandations se trouvant dans les guides fournis [GUIDES] notamment celles énoncées au §25 de [USER_GUIDE]. L'utilisateur devra également s'assurer que les recommandations ci-dessous sont correctement mises en œuvre :

- l'installation du logiciel doit être effectuée par l'administrateur de sécurité depuis un compte dédié, différent du compte de l'utilisateur final ;
- les certificats manipulés par la TOE doivent posséder des dates de validité au format « UTC Time » ;
- l'administrateur de sécurité doit changer le mot de passe par défaut pour l'accès à la configuration et doit en choisir un qui soit robuste.

3.3. Reconnaissance du certificat

Ce certificat n'entre pas dans le champ d'une reconnaissance internationale.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 3+	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	**3**	Functional specification with complete summary
	ADV_IMP				1	1	2	2		
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**2**	Architectural design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	**3**	Authorisation controls
	ALC_CMS	1	2	3	4	5	5	5	**3**	Implementation representation CM coverage
	ALC_DEL		1	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			1	1	1	2	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD			1	1	1	1	2	**1**	Developer defined life-cycle model
	ALC_TAT				1	2	3	3		
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	**2**	Analysis of coverage
	ATE_DPT			1	1	3	3	4	**1**	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	**1**	Functional testing
	ATE_IND	1	2	2	2	2	2	3	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - TheGreenBow – VPN certified, référence CDS-TGB-CC, version 1.1, 8/1/2020, *THEGREENBOW*.
[RTE]	Rapport technique d'évaluation : - Projet TGB, référence OPPIDA/CESTI/TGB/RTE, version 3.1, 5/6/2020, *OPPIDA*.
[ANA-CRY]	Expertise cryptographique – TheGreenBow VPN client, référence OPPIDTI/CESTI/TGB/CRYPTO, version 4.0, 19/2/2020, *OPPIDA*.
[CONF]	Liste de configuration du produit : - TheGreenBow VPN Client Evaluation Delivery, référence tgbvpn_eval_delivery, version 1.43, 9/1/2020, *THEGREENBOW*.
[GUIDES]	Guide d'installation du produit : - TheGreenBow – VPN certified – Guide de déploiement, référence tgbvpn_ug_deployment_fr_6.52_1.1, version 1.1, décembre 2019, *THEGREENBOW*. - TheGreenBow – VPN certified – Guide de déploiement – gestion des PKI, certificats, tokens et cartes à puce, référence tgbvpn_ug_pki_smartcard_fr_6.50_1.1a, version 1.1a, juillet 2018, *THEGREENBOW*. Guide d'utilisation du produit [USER_GUIDE] : - TheGreenBow – VPN certified – Guide utilisateur, reference tgbvpn_ug_fr_1.5, version 1.6, janvier 2020, *THEGREENBOW*.
[PP]	PP Application VPN cliente, référence PP-VPNC-CCv3.1, version 1.3, de juin 2008, ANSSI.

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; - Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; - Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.
	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), voir www.ssi.gouv.fr.