PREMIER MINISTRE

*Liberté*
*Égalité*
*Fraternité*

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

# Rapport de certification ANSSI-CC-2021/10

## TheGreenBow VPN Linux ElinOS (v6.1) version 1.5.0

Paris, le 29 mars 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

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<br>**ANSSI-CC-2021/10** |
| Nom du produit<br>**TheGreenBow VPN Linux ElinOS (v6.1)** |
| Référence/version du produit<br>**version 1.5.0** |
| Conformité à un profil de protection<br>**Aucun** |
| Critère d'évaluation et version<br>**Critères Communs version 3.1 révision 5** |
| Niveau d'évaluation<br>**EAL 3 augmenté**<br>ALC_FLR.3 et AVA_VAN.3 |
| Développeur<br>**THEGREENBOW**<br>28, rue de Caumartin, 75009 Paris, France |
| Commanditaire<br>**THEGREENBOW**<br>28, rue de Caumartin, 75009 Paris, France |
| Centre d'évaluation<br>**OPPIDA**<br>4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France |
| Accords de reconnaissance applicables<br>**CCRA**<br>Ce certificat est reconnu au niveau EAL2 augmenté de FLR.3.<br>**SOG-IS**<br>Ce certificat est reconnu au niveau EAL3 augmenté de FLR.3. |

# PREFACE

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 le directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 MATIERES

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est « TheGreenBow VPN Linux ElinOS (v6.1), version 1.5.0 » développé par THEGREENBOW.

Le produit est un logiciel « VPN IPsec IKEv2 » conçu pour fonctionner sous la distribution « Linux ELINOS 6.1 (64 bits) ». Il permet d'établir une connexion et d'assurer la communication sécurisée entre, d'une part, un équipement mobile et une station fixe, et, d'autre part, entre deux équipements mobiles.

Le produit s'appuie sur le produit *open source* « VPN StrongSwan », il implémente les protocoles IKEv1 et IKEv2, cependant, seul le protocole IKEv2 est considéré dans le cadre de la présente évaluation.

## 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 ne revendique aucune conformité à un profil de protection.

### 1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la protection en confidentialité des données applicatives ;
- la protection en intégrité des données applicatives ;
- la protection en confidentialité des données topologiques ;
- la protection en intégrité des données topologiques ;
- la protection contre le rejeu ;
- la génération de *logs*.

### 1.2.3 *Architecture*

La figure suivante présente l'architecture du produit intégré à son environnement :

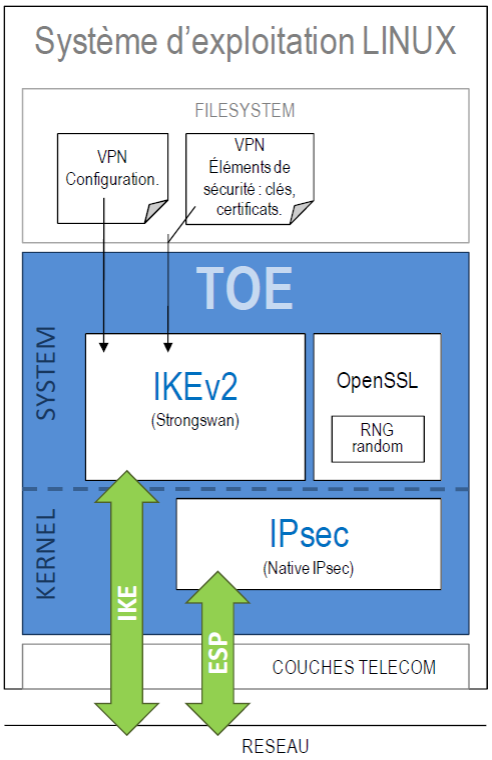


Figure 1 - Architecture du produit

La TOE est un système composé :

- du moteur IKE[1] basé sur le produit *open source* « VPN StrongSwan », version 5.8.4 assurant le service IKE V2 en s'appuyant sur la librairie « OpenSSL », version 1.1.1f ;
- et les *drivers* IPSec du noyau LINUX « ElinOS 6.1 » qui assurent le service ESP[2] (mode tunnel uniquement).

A noter que le composant IPSec a été intégré à la TOE pour qu'il soit pris en compte dans l'évaluation des fonctionnalités essentielles liées à la sécurité du produit. Cependant, il est à noter que le *package* d'installation du logiciel « TheGreenBow VPN Linux » contient les composants « IKE » et « OpenSSL », mais ne contient pas les *drivers* IPSec fournis par le noyau LINUX « ElinOS 6.1 ».

[1] *Internet Key Exchange.*

[2] *Encapsulation Security Payload.*

Eléments hors périmètre de l'évaluation :

Les éléments suivants ne font pas partie de la présente évaluation :

- infrastructure réseau entre l'équipement hébergeant la TOE et l'autre extrémité de la connexion VPN ;
- chiffreur IP (Gateway VPN) ;
- infrastructure de gestion de clés (IGC) ;
- équipements de stockage amovible de certificats (*tokens*, carte à puce).

### 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 par son numéro de version qui peut être lu à partir de la commande « cat /usr/libexec/ipsec/VERSION ».

### 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, l'évaluateur a considéré les rôles décrits au §3.2 de la cible de sécurité [ST].

### 1.2.6 *Configuration évaluée*

Le certificat porte sur les configurations identifiées comme appartenant au périmètre de cette évaluation dans le tableau suivant. Ce tableau identife également les fonctions évaluées et celles qui ne le sont pas.

| | 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 | Non |
| | Import de la politique de sécurité VPN | Oui |
| | Export de la politique de sécurité VPN | Non |
| | Gestion centralisée des politiques de sécurité VPN, télé administration | Non |
| Mécanismes d'authentification | Clé partagée (PSK) | Non |
| | EAP | Non |
| | X509 | Oui |

| | | |
|---|---|---|
| | Authentification du certificat passerelle | Oui |
| Algorithmes | Algorithmes cryptographiques | Oui |
| Réseau | Mode Configuration Payload | Oui |
| | Contrôle des flux non chiffrés | Non |
| Fonctions diverses | Génération de logs | Oui |
| | Mode « VPN point à point » | Oui |

Pour plus ample information se reporter au §1.5 de la cible de sécurité [ST].

La plateforme de test qui a été utilisée lors de l'évaluation est celle décrite au §7.7 de la cible de sécurité [ST].

# 2 L'évaluation

## 2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs version 3.1 révision 5 [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 15 février 2021, 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 [EXP-CRY]. 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 de nombres pseudo-aléatoires (PRNG) fourni par la librairie « OpenSSL », une fois le retraitement effectué, a été jugé satisfaisant par l'évaluateur.

# 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 Linux ElinOS (v6.1), version 1.5.0 » 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 les recommandations se trouvant dans les guides fournis [GUIDES]. De plus, l'utilisateur devra s'assurer que la TOE ne peut être utilisée avec une valeur de configuration *replay_windows* = 0, ce qui aurait pour effet de désactiver l'anti-rejeu.

## 3.3 Reconnaissance du certificat

### 3.3.1 *Reconnaissance européenne (SOG-IS)*

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[3], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :


### 3.3.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

[3] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[4] , des certificats Critères Communs.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[4] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

# ANNEXE A. 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 | 2 | 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 B. Références documentaires du produits évalué

| | |
|---|---|
| [ST] | Cible de sécurité de référence pour l'évaluation :<br>- TheGreenBow – VPN Linux certified, référence tgbvlx_CDS_CC, version 3.5, 5/2/2021, THEGREENBOW. |
| [RTE] | Rapport technique d'évaluation :<br>- Projet TGB VPN Linux 1.5, référence OPPIDA/CESTI/TGB VPN LINUX1.5/RTE, version 3.1, 12/2/2021, OPPIDA. |
| [ANA-CRY]<br>[EXP-CRY] | Rapport d'analyse des mécanismes cryptographiques TGB VPN Linux 1.5, référence OPPIDA/CESTI/ TGB VPN LINUX1.5 /CRYPTO, version 1.4, 3/2/2021, OPPIDA. |
| [CONF] | Liste de configuration du produit :<br>TheGreenBow VPN Client Evaluation Delivery, référence tgbvlc_eval_delivery, version 3.2, 5/2/2021, THEGREENBOW. |
| [GUIDES] | Guide d'administration du produit :<br>- Guide administrateur **-** ThegreenBow VPN Linux certified, version 3.8, décembre 2020, THEGREENBOW.<br><br>Guide d'utilisation du produit :<br>- User Guide – Strongswan documentation, référence tgbvlx_ug_strongswan, version 2.1, 17/4/2020, THEGREENBOW. |

# ANNEXE C. 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:*<br>- *Part 1: Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001;<br>- *Part 2: Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002;<br>- *Part 3: Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003. |
| [CEM] | *Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004. |
| [CC RA] | *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014. |
| [SOG-IS] | *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, 8 janvier 2010, Management Committee. |
| [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. |