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-2024/32

Trustway IP Protect (Version 6.01.17)

Paris, le 25 Novembre 2024

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

Vincent STRUBEL

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2024/32**
Nom du produit **Trustway IP Protect**
Référence/version du produit **Version 6.01.17**
Conformité à un profil de protection ***Néant***
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL4 augmenté** ALC_FLR.3
Développeur **BULL SAS** Rue Jean-Jaurès 78340 Les Clayes-sous-Bois, France
Commanditaire **BULL SAS** Rue Jean-Jaurès 78340 Les Clayes-sous-Bois, France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny-le-Bretonneux, France
Accords de reconnaissance applicables **CCRA** Ce certificat est reconnu au niveau EAL2 augmenté de ALC_FLR.3 **SOG-IS** Ce certificat est reconnu au niveau EAL4 augmenté de ALC_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.cyber.gouv.fr.

TABLE DES MATIERES

1 Le produit 6
1.1 Présentation du produit 6
1.2 Description du produit 6
1.2.1 Introduction 6
1.2.2 Services de sécurité 6
1.2.3 Architecture 7
1.2.4 Identification du produit 7
1.2.5 Cycle de vie 8
1.2.6 Configuration évaluée 8
2 L'évaluation 9
2.1 Référentiels d'évaluation 9
2.2 Travaux d'évaluation 9
2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI 9
2.4 Analyse du générateur d'aléa 9
3 La certification 10
3.1 Conclusion 10
3.2 Restrictions d'usage 10
3.3 Reconnaissance du certificat 11
3.3.1 Reconnaissance européenne (SOG-IS) 11
3.3.2 Reconnaissance internationale critères communs (CCRA) 11
ANNEXE A. Références documentaires du produit évalué 12
ANNEXE B. Références liées à la certification 13

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Trustway IP Protect, Version 6.01.17 » développé par BULL SAS.

Ce produit est un chiffreur IP, constitué du logiciel embarqué dans les équipements de chiffrement réseau Trustway IP Protect, assurant la protection des paquets IP suivant l'architecture IPSec et fournissant une plateforme pour la création de réseaux de confiance.

Les chiffreurs IP Protect représentent les points de liaison entre les réseaux sécurisés et les réseaux ouverts, effectuant le filtrage et appliquant la politique de sécurité.

Le présent certificat porte sur le logiciel embarqué dans les équipements de chiffrement Trustway IP Protect ainsi que sur le protocole sécurisé d'échange de données avec la station de configuration à distance (*Trustway Domain Manager* - TDM) ainsi que sur la protection des données de personnalisation générées par le SPC pour personnaliser les chiffreurs.

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 s'inspire du profil de protection [PP].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit, décrits au chapitre 3.2.1 « Services fournis par la TOE » de la cible de sécurité [ST], sont :

- l'application des politiques de sécurité VPN, incluant :
  - la protection en confidentialité des données applicatives ;
  - la protection en authenticité des données applicatives ;
  - la protection anti-rejeu des données applicatives ;
  - la protection en confidentialité des données topologiques des réseaux privés ;
  - la protection en authenticité des données topologiques des réseaux privés.
- le cloisonnement des flux IP.

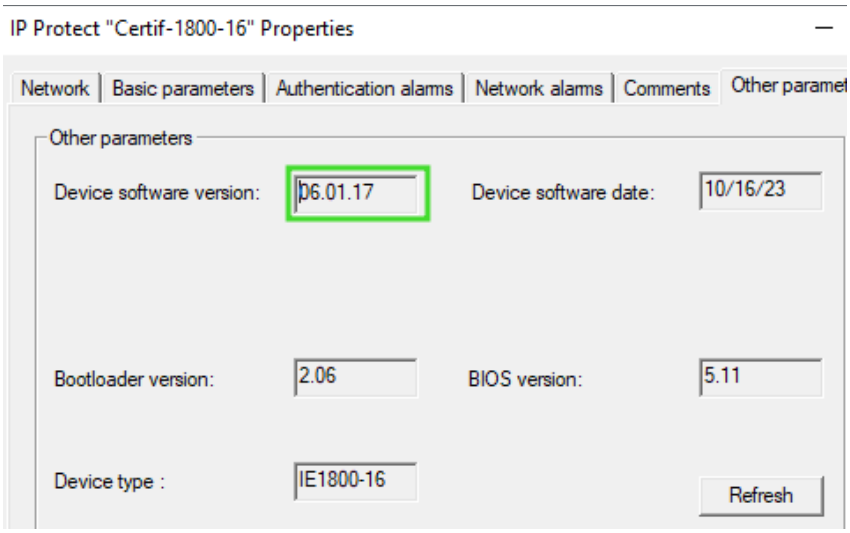
1.2.3 *Architecture*

L'architecture du produit est décrite au chapitre 3 « Description de la TOE » de la cible de sécurité [ST].

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 via l'application TDM en utilisant la commande *Get all devices versions* du menu *Devices*, qui envoie une requête sécurisée à chaque *VPN/Device* afin de connaître la version du logiciel installé, et affiche le résultat de ces requêtes.



1.2.5 *Cycle de vie*

Le cycle de vie est décrit au chapitre 3.4 de [ST].

Le produit a été développé sur les sites suivants :

Les Clayes-sous-Bois	**Angers**
Rue Jean-Jaurès, BP 68 78340 Les Clayes-sous-Bois France	30 Bis rue du Nid de Pie 49008 Angers France

Le cycle de vie comporte les six phases suivantes :

- Développement (site Les Clayes-sous-Bois) ;
- Intégration (site Les Clayes-sous-Bois) ;
- Validation (site Les Clayes-sous-Bois) ;
- Intégration matérielle et sécurisation (site Angers) ;
- Livraison au client (site Angers) ;
- Maintenance et support (site Les Clayes-sous-Bois).

1.2.6 *Configuration évaluée*

Le certificat porte sur le produit identifié dans la cible de sécurité [ST] au chapitre 2.3 « Vue d'ensemble de la cible de sécurité », dans ses configurations permises par les [GUIDES].

Au regard du cycle de vie, le certificat porte sur le produit livré à l'issue de la phase 5 (livraison au client).

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [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 jour de sa finalisation par le CESTI (voir date en bibliographie), détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises 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 d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [ANSSI Crypto], il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléa n'a pas révélé de faiblesse.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

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].

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[1], 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].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[2] , 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 :

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

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

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Trustway IP Protect – Cible de sécurité, référence TW/IPP/IP Protect_Cible de sécurité/CI, version 1.22, 9 septembre 2024. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Trustway IP Protect – Cible de sécurité, référence TW/IPP/IP Protect_Cible de sécurité - Light/PU, version 1.22 – Light.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation, référence OPPIDA/CESTI/TRUSTWAY IP PROTECT/RTE, version 3.0, 17 octobre 2024.
[ANA_CRY]	Rapport d'analyse des mécanismes cryptographiques, référence OPPIDA/CESTI/Trustway IP Protect/CRYPTO/4.0, version 4.0, 20 août 2024.
[CONF]	Liste de configuration du produit : - *Trustway IP Protec*t – Durcissement de l'OS, référence IPProtect_Durcissement_de_l_OS, version 1.8, 12 janvier 2024
[GUIDES]	Guides d'installation, d'administration et d'utilisation du produit : - *Trustway IP Protect* - Manuel de préparation usine, référence v1.18, version 1.18, novembre 2022 ; - *Trustway IP Protect* - Génération de configurations Trustway par script - Manuel d'utilisation, référence X86 F2 30ET 17, avril 2023 ; - *Trustway* - TDM - TAM - Journalisation - Description des enregistrements, ref. 86 F2 31ET 09, mai 2022 ; - *Trustway IP Protect* - Chiffreurs Trustway - Manuel d'utilisation et d'installation, référence 86 F2 23ET 31, avril 2023 ; - *Trustway IP Protect* - *Trustway Domain Manager* - Manuel d'utilisation et d'installation, référence 86 F2 26ET 44, octobre 2023 ; - *Trustway IP Protect* - Manuel de dépannage, référence 86 F2 27ET 24, version ??, avril 2023.
[PP]	Profil de protection « Chiffreur IP », référence PP-CIP-3.1, version 1.9, certifié PP-2008/08 le 22 août 2008

ANNEXE B. 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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1 : Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - *Part 2 : Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - *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.
[CCRA]	*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.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.