PREMIER MINISTRE

Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Rapport de certification ANSSI-CSPN-2026/12

WAPT Enterprise

Version 2.6.0.16859

Paris, le 17/7/2026 | 18:18 CEST

Vincent Strubel

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-CSPN-2026/12**
Nom du produit **WAPT Enterprise**
Référence/version du produit **Version 2.6.0.16859**
Catégorie de produit **Administration et supervision de la sécurité**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Tranquil I.T. Systems** 12 avenue Jules Verne, Bâtiment A 44230 Saint-Sébastien sur Loire, France
Développeur **Tranquil I.T. Systems** 12 avenue Jules Verne, Bâtiment A 44230 Saint-Sébastien sur Loire, France
Centre d'évaluation **ALMOND** 11 rue Maurice Fabre 35000 Rennes, France
Accord de reconnaissance applicable fixed time certification Ce certificat est reconnu dans le cadre du [BSZ_CSPN]
Fonctions de sécurité évaluées Communications sécurisées Identification, authentification et contrôle d'accès des utilisateurs Protection des données, en stockage ou en transit, incluant l'effacement sécurisé Fonctions cryptographiques et générateurs de nombres aléatoires Autoprotection : démarrage sécurisé, autotests, protection physique, cloisonnement et séparation de domaines Journalisation
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Non

PREFACE

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 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 CSPN sont disponibles sur le site Internet cyber.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « WAPT Enterprise, Version 2.6.0.16859 » développé par Tranquil I.T. Systems.

Ce produit permet d'automatiser l'installation, la post-configuration, la mise à jour et la suppression de logiciels sur un parc de machines Windows, Linux ou macOS.

WAPT est constitué de trois sous-ensembles :

- une composante serveur (serveur WAPT), hébergée sur une machine unique ou un jeu de machines physiques ou virtuelles, qui stocke l'inventaire du parc et les paquets (logiciels ou leurs mises à jour) et qui notifie les agents WAPT ;
- une composante client (agent WAPT) installée sur le poste client et en interaction avec le serveur WAPT ;
- une console d'administration du produit (console WAPT) installée sur le poste d'administration dédié de l'administrateur métier de la solution.

La sécurité de WAPT repose sur la signature asymétrique des paquets sur la base de certificats.

1.2 Description du produit évalué

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

1.2.1 *Catégorie du produit*

☐	1	Détection d'intrusions
☐	2	Anti-virus, protection contre les codes malveillants
☐	3	Pare-feu
☐	4	Passerelle-multiniveau
☐	5	Effacement de données
☒	**6**	**Administration et supervision de la sécurité**
☐	7	Moyen d'authentification numérique
☐	8	Système de contrôle d'accès physique
☐	9	Communication sécurisée
☐	10	Messagerie sécurisée
☐	11	Stockage sécurisé
☐	12	Environnement d'exécution sécurisé
☐	13	Matériel avec logiciel embarqué
☐	14	SCADA
☐	15	Automate programmable industriel
☐	16	Système de vidéoprotection
☐	99	Autre

1.2.2 *Identification du produit*

Produit	
Nom du produit	WAPT Enterprise
Numéro de la version évaluée	Version 2.6.0.16859

La version certifiée du produit peut être identifiée de l'une des deux manières suivantes :

- dans l'interface de la console d'administration :

- ou dans le fichier `/opt/wapt/version-full` :

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- les communications sécurisées entre les différentes composantes de la solution ;
- l'identification, l'authentification et le contrôle d'accès des utilisateurs ;
- la protection des données, en stockage et en transit, incluant l'effacement sécurisé ;
- les fonctions cryptographiques et générateurs de nombres aléatoires ;
- l'autoprotection : le démarrage sécurisé, les autotests, la protection physique, le cloisonnement et la séparation de domaines ;
- la journalisation.

1.2.4 *Configuration évaluée*

La configuration évaluée est décrite au chapitre.3.1 de la cible de sécurité [CDS].

La plateforme de test est constituée des éléments suivants :

- un serveur Active Directory sous Windows Server 2022 ;
- un serveur WAPT sous Rocky Linux 10.1 ;
- un poste d'administration sous Windows 11, contenant un agent WAPT et la console d'administration WAPT ;
- un poste utilisateur sous Windows 11, contenant un agent WAPT ;
- un poste attaquant sous Kali Linux présent sur le réseau.

La figure ci-dessous explicite la plateforme de test.

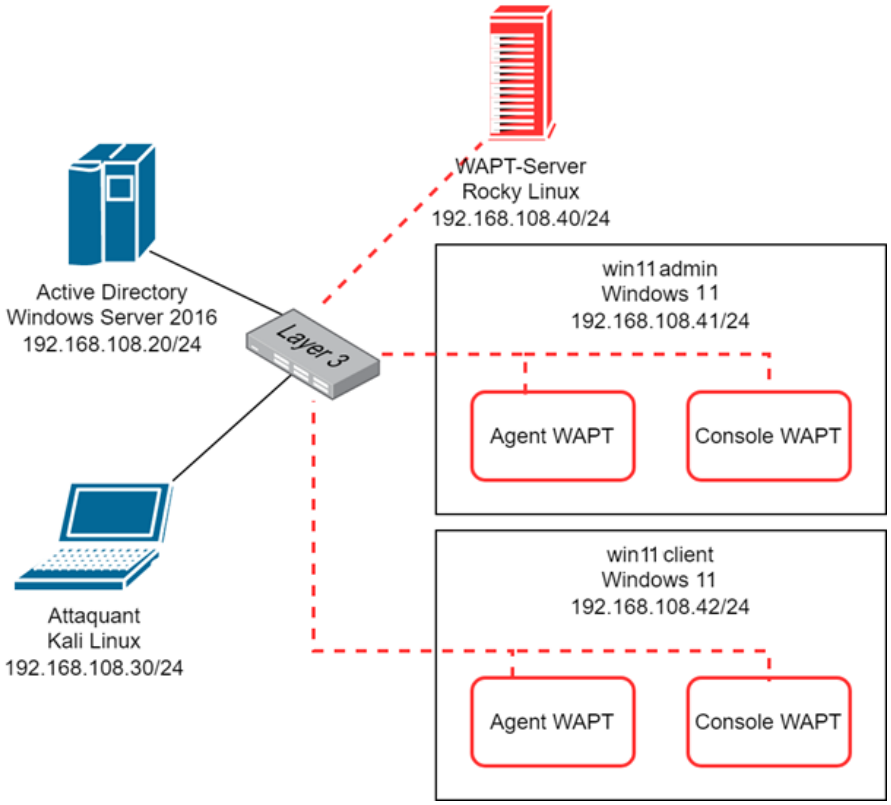

Figure 1 – Plateforme de test.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

2.2 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.2.1.2 Description de l'installation et des non-conformités éventuelles

L'évaluateur a installé la plateforme d'évaluation et le produit en suivant la documentation et les guides d'installation du produit.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'intégralité du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.2.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables dans le contexte défini par la cible de sécurité [CDS].

2.2.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.2.7.2 Avis d'expert sur la facilité d'emploi

Le produit est simple à installer. La documentation décrit clairement comment installer et utiliser le produit.

2.2.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) 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 n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. 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.

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].

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.

Ce certificat atteste que le produit « WAPT Enterprise, Version 2.6.0.16859 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2 Recommandations et 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 spécifiés dans la cible de sécurité [CDS], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3 Reconnaissance du certificat

Ce certificat est émis dans les conditions du [BSZ_CSPN].

Cet accord permet la reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ (*Beschleunigte Sicherheitszertifizierung* ou Certification de sécurité accélérée).

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité CSPN – WAPT Enterprise v2.6.0.16859, référence 2024_CSPN_WAPT_tranquil-it_TOE, version 1.16, 18 juin 2026.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN – Produit WAPT Enterprise – version 2.6.0.16859, référence CSPN-RTE-WAPT Enterprise3-4.10, version 4.10, 1er juillet 2026.
[ANA_CRY]	Rapport d'expertise cryptographique : - Expertise des mécanismes cryptographiques – Produit WAPT Enterprise – version 2.6.0.16840, référence CSPN-CRY-WAPT Enterprise3-3.00, version 3.00, 9 mars 2026.
[GUIDES]	Guides du produit : - Les guides du produit sont accessibles en ligne sur le lien suivant : https://www.wapt.fr/fr/doc-2.6/[1]

[1] Lien vérifié le 1er jullet 2026.

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.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 5.0, 12 janvier 2023. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0, 6 septembre 2018.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.2, 18 mars 2025.
[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.
[BSZ_CSPN]	*Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI,* référence *bsz_cspn_mutual_recognition_agreement*,version 3.0, mai 2026.