
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-CSPN-2018/02

# WAPT

# WAPT-Entreprise - version 1.5.0.13

*Paris, le 14 février 2018*

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

Guillaume POUPARD
[ORIGINAL SIGNE]

# 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-CSPN-2018/02** |
| *Nom du produit*<br>**WAPT** |
| *Référence/version du produit*<br>**Référence WAPT-Entreprise - version 1.5.0.13** |
| *Catégorie de produit*<br>**Administration et supervision de la sécurité** |
| *Critères d'évaluation et version*<br>**CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)** |
| *Commanditaire*<br>**Tranquil'IT Systems**<br>**12, avenue Jules Verne**<br>**44230 Saint Sébastien sur Loire** |
| *Développeur*<br>**Tranquil'IT Systems**<br>**12, avenue Jules Verne**<br>**44230 Saint Sébastien sur Loire** |
| *Centre d'évaluation*<br>**Amossys**<br>**4 bis allée du bâtiment,**<br>**35000 Rennes, France** |
| *Fonctions de sécurité évaluées*<br>**Authentification et contrôle d'accès**<br>**Protection des données**<br>**Communications sécurisées**<br>**Signature des paquets** |
| *Fonction(s) de sécurité non évaluées*<br>**Sans objet** |
| *Restriction(s) d'usage*<br>**Oui (cf. §3.2)** |

# 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 le Premier ministre 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 www.ssi.gouv.fr.

# Table des matières

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est « WAPT, version WAPT-Entreprise - version 1.5.0.13 » développé par *TRANQUIL'IT SYSTEMS*.

Ce produit est un gestionnaire de logiciels sur les plateformes Windows. Le fonctionnement de WAPT s'inspire fortement du gestionnaire de paquets *apt-get* du système GNU/Linux Debian, d'où son nom.
Les principales fonctionnalités offertes par le produit sont l'installation, la configuration, la mise à jour et la suppression de logiciels sur un parc Windows.
WAPT est constitué de trois sous-ensembles :

- un composant serveur ;
- un composant client ;
- un composant console (administration).

Le déploiement de logiciels (Firefox, MS Office, ...) s'effectue de manière centralisée avec la console graphique d'administration.

La figure ci-dessous explicite l'architecture du produit.

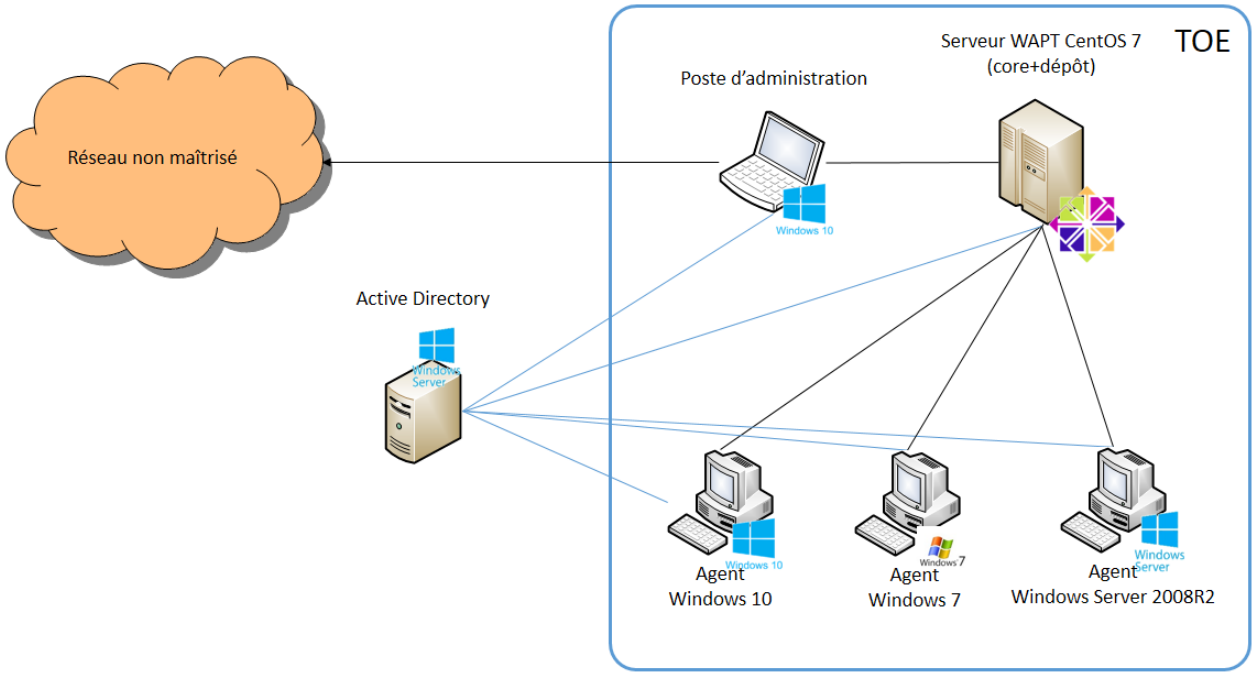


**Figure 1 - Architecture Produit**

## 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 malicieux |
| ☐ 3 – pare-feu |
| ☐ 4 – effacement de données |
| ☒ **5 – administration et supervision de la sécurité** |
| ☐ 6 – identification, authentification et contrôle d'accès |
| ☐ 7 – communication sécurisée |
| ☐ 8 – messagerie sécurisée |
| ☐ 9 – stockage sécurisé |
| ☐ 10 – environnement d'exécution sécurisé |
| ☐ 11 – terminal de réception numérique (*Set top box*, STB) |
| ☐ 12 – matériel et logiciel embarqué |
| ☐ 13 – automate programmable industriel |
| ☐ 99 – autre |

### 1.2.2. Identification du produit

| | |
|---|---|
| Nom du produit | WAPT |
| Numéro de la version évaluée | WAPT-Entreprise - version 1.5.0.13 |

La version certifiée du produit peut être identifiée de la manière suivante :
Après installation de WAPT sur la machine d'administration, l'accès à l'URL http://127.0.0.1:8088 fournit différentes informations. Il est possible, par exemple, de retrouver le statut de WAPT, avec les versions des exécutables et scripts utilisés.


**Figure 2 : Version de WAPT évaluée**

### 1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :
- l'authentification et le contrôle d'accès ;
- la protection des données ;
- les communications sécurisées ;
- la signature des paquets.

### 1.2.4. Configuration évaluée

Comme indiqué sur la *Figure 1 - Architecture Produit*, WAPT supporte les environnements suivants :
- le serveur peut être installé sous Linux CentOS, avec SELinux ;
- les agents sont disponibles sur les systèmes Windows 7, 10 et Server 2008 R2 ;
- la console d'administration est un client lourd disponible sur les systèmes Windows 7, 10 et Server 2008 R2.

La configuration évaluée est la suivante :
- le serveur est installé sous Linux CentOS 7, avec SELinux ;
- les agents sont installés sur des machines virtuelles, sur systèmes Windows 7, 10 et Server 2008 R2 ;
- la console d'administration est installée sur un système Windows 10 uniquement.

Il doit être également noté que les agents ont été déployés manuellement. La fonctionnalité de déploiement par GPO n'a donc pas été testée dans le cadre de cette évaluation.

La plateforme de test inclut enfin un serveur Windows 2008r2, mis en place avec un service DNS ainsi qu'un Active Directory (AD). L'ensemble des machines sont enrôlées dans cet AD.

# 2. L'évaluation

## 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2.

## 2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

## 2.3. 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].

### 2.3.1. **Installation du produit**

#### 2.3.1.1. **Particularités de paramétrage de l'environnement et options d'installation**

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

#### 2.3.1.2. **Description de l'installation et des non-conformités éventuelles**

Aucune non-conformité n'a été relevée.

#### 2.3.1.3. **Durée de l'installation**

L'installation de la TOE ainsi que du système hôte a duré 4 jours.

#### 2.3.1.4. **Notes et remarques diverses**

Sans objet.

### 2.3.2. **Analyse de la documentation**

La documentation est jugée claire et bien illustrée, permettant la résolution des problèmes les plus couramment rencontrés. Les erreurs moins fréquentes semblent en revanche insuffisamment documentées. En outre, les messages d'erreur du produit ne sont pas toujours explicites sur la cause exacte du problème.
Ce point a pour conséquence un avertissement relatif à la facilité d'emploi (voir paragraphe 2.3.8.3).

### 2.3.3. **Revue du code source (facultative)**

Sans objet.

#### 2.3.4. Analyse de la conformité des fonctions de sécurité

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

#### 2.3.5. 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.

#### 2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

##### 2.3.6.1. Liste des vulnérabilités connues

Le produit WAPT n'a pas de vulnérabilités connues. Par contre, des vulnérabilités publiques existent sur ses briques logicielles tierces. Cependant dans le contexte défini par la cible de sécurité [CDS] et les conditions d'utilisation du produit par le développeur, aucune d'entre elles n'est exploitable.

##### 2.3.6.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

#### 2.3.7. Accès aux développeurs

Le centre d'évaluation a eu accès aux développeurs pour répondre à des questions sur le produit.

#### 2.3.8. Analyse de la facilité d'emploi et préconisations

##### 2.3.8.1. 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.

##### 2.3.8.2. Recommandations pour une utilisation sûre du produit

L'utilisateur doit appliquer les recommandations suivantes :

- l'administrateur doit s'assurer que les paquets téléchargés sont conformes aux règles de sécurité mises en place dans le SI, avant de les importer dans le dépôt privé de WAPT-Enterprise ;
- malgré la présence de préconisations sur les mots de passe dans la documentation du développeur et de contrôle de la qualité du mot de passe par le logiciel, l'évaluateur préconise de suivre les recommandations [ANSSI-MDP] ;
- le produit n'implémente pas de fonctionnalité de révocation des certificats. Si un certificat est compromis, l'utilisateur doit être en mesure d'effectuer la mise à jour manuelle des certificats directement sur les postes des utilisateurs ;
- le poste d'administration contient des données confidentielles (clé de signature des paquets) et doit être protégé de tout accès physique non autorisé ;
- enfin, les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer à la documentation utilisateur fournie.

#### 2.3.8.3. Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour un utilisateur familier à l'administration d'infrastructures sous Windows.
En revanche, les messages d'erreur ne permettent pas de résoudre tous les problèmes de l'utilisateur. En effet, l'évaluateur s'est confronté à plusieurs blocages liés à la mise en place de certificats issus d'une autorité de certification interne. Un accompagnement de l'utilisateur par le développeur sera probablement nécessaire lors de l'installation.

#### 2.3.8.4. Notes et remarques diverses

Sans objet.

## 2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN.
Celle-ci a relevé des non-conformités mineures au RGS :

- l'utilisation du schéma PKCS# RSA v1.5 ;
- l'utilisation de la fonction de hachage SHA1 dans le mécanisme HMAC-SHA-1 assurant l'authenticité des données.

Cependant, ces non-conformités ne remettent pas en cause la sécurité globale du produit.

En outre, le mécanisme PBKDF1 est utilisé. Ce mécanisme n'est pas recommandé. Cependant, son utilisation dans le contexte défini par la cible de sécurité [CDS] ne remet pas en cause les fonctions de sécurité du produit.

Enfin, l'évaluateur a relevé des vulnérabilités relatives à l'effacement des clés, qui se sont révélées inexploitables dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

## 2.5. Analyse du générateur d'aléas

Le produit utilise plusieurs générateurs d'aléas, implémentés par

- la librairie OpenSSL ;
- le générateur de nombres aléatoires du noyau linux (LNRG) ;
- la fonction CryptGenRandom du système d'exploitation Windows.

Malgré des non-conformités au [RGS], l'évaluateur n'a pas relevé de vulnérabilité exploitable lors de l'analyse.

# 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, version WAPT-Entreprise - version 1.5.0.13 » 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. 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 mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations énoncées dans le présent rapport (voir 2.3.8.2).

De plus, l'évaluation a mis en avant un risque lié à l'import de paquets depuis le dépôt public (https://store.wapt.fr). La configuration par défaut n'utilise pas ce dépôt ; le produit ne doit pas être reconfiguré de façon à réintroduire ce dépôt public dans la configuration.

# Annexe 1. Références documentaires du produit évalué

| | |
|---|---|
| [CDS] | *Cible de sécurité CSPN - Produit WAPT-Enterprise version 1.5.0.13-amo*<br>Référence : CSPN-ST-WAPT ;<br>Version : *1.0.6* ;<br>Date : *8 décembre 2017* |
| [RTE] | *Rapport Technique d'Evaluation CSPN - Produit WAPT - Enterprise version 1.5.0.13*<br>Référence : CSPN-RTE-WAPT2 ;<br>Version : 1.00 ;<br>Date : *27 décembre 2017* |
| [ANA-CRY] | *Expertise des mécanismes cryptographiques - Produit WAPT-Enterprise version 1.5.0.13*<br>Référence : CSPN-CRY-WAPT2 ;<br>Version : 1.00 ;<br>Date : *27 décembre 2017* |

# Annexe 2. Références 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, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014.<br><br>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014.<br><br>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014.<br><br>Documents disponibles sur www.ssi.gouv.fr. |
| [RGS] | 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. |
| [ANSSI-MDP] | Recommandations ANSSI pour le choix des mots de passe : https://www.ssi.gouv.fr/guide/mot-de-passe |