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-2011/05

WinPT version 1.4.3
GnuPG version 1.4.10b

Paris, le 09 mai 2011

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

Patrick Pailloux
[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.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CSPN-2011/05

Nom du produi1

WinPT (Windows Privacy Tray)
GnuPG (Gnu Privacy Guard)

Référence/version du produit

WinPT version 1.4.3
GnuPG version 1.4.10b compilé pour Microsoft Windows

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU
(CSPN, Phase expérimentale)

Développeur(s)

WinPT Project
http://winpt.gunpt.de
GnuPG Team
http://www.gnupg.org

Commanditaire

Ministère du Budget, des Comptes publics, de la Fonction publique et de la Réforme de l'État

Centre d'évaluation

Silicomp-AQL
4, rue de la Châtaigneraie CS 51766
35517 Cesson-Sévigné CEDEX
Tél : 0299125000, mél : cesti@aql.fr

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 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 le moteur cryptographique GnuPG, version 1.4.10b et son interface graphique WinPT, version 1.4.3.

GnuPG permet, en ligne de commande, de générer et gérer des paires de clés (couple clé publique / clé privée), de chiffrer (respectivement déchiffrer) et/ou de signer (respectivement vérifier la signature) des documents.

Ce produit libre implémente le standard OpenPGP défini par la norme [RFC4880].

WinPT est une interface utilisateur (pour Windows) permettant de faciliter l'utilisation de GnuPG (*user* friendly) et de mettre en œuvre une grande partie de ses fonctionnalités.

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 - firewall
☐ 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 - matériel et logiciel embarqué
☐ 99- Autres

1.2.2. Identification du produit

Une fois installées, les versions de GnuPG et de WinPT sont identifiables en cliquant sur la rubrique « A propos de WinPT » du menu « ? ».

Le hashé (SHA1) de l'installeur est identifié dans le guide d'exploitation [GUIDES].

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la création de bi-clés ;
- l'importation de clés OpenPGP ;
- l'exportation de clés publiques ;
- la suppression de clés ;
- la gestion de clés publiques ;
- la signature de documents ;
- la vérification de signature de documents ;
- le chiffrement de documents ;
- le déchiffrement de documents ;
- la modification de la configuration de GnuPG et de WinPT ;
- la protection de la confidentialité des clés privées de l'utilisateur.

1.2.4. Configuration évaluée

La configuration évaluée est celle décrite dans la cible de sécurité [CDS]. Il s'agit de la configuration par défaut de WinPT utilisant uniquement les algorithmes RSA 2048, AES 256 et SHA256 de GnuPG.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de Sécurité de Premier Niveau en phase expérimentale. Les références des documents se trouvent en annexe 2.

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

35 homme.jour ont été consacrés à l'évaluation de WinPT conformément à ce qui est prévu lors d'une évaluation CSPN d'un produit comportant des mécanismes cryptographiques.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre II « Argumentaire (description) du produit »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre V « Description des biens sensibles que le produit doit protéger »).

2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre VI « Description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre VII « Description des fonctions de sécurité du produit »).

2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre III « Description de l'environnement technique dans lequel le produit doit fonctionner »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Conformément à ce qui est indiqué dans la cible de sécurité [CDS], les éléments de la plate-forme de test utilisée lors de cette évaluation sont des PC fonctionnant sous environnement Windows (architecture 32 bits) XP SP2 et SP3.

2.3.2.2. Particularités de paramétrage de l'environnement

L'installation du produit ne nécessite aucun paramétrage particulier.

2.3.2.3. Options d'installation retenues pour le produit

Sans objet.

2.3.2.4. Description de l'installation et des non-conformités éventuelles

Aucune non-conformité n'a été relevée lors de l'installation du produit à expertiser.

2.3.2.5. Durée de l'installation

L'installation complète de GnuPG et de WinPT prend moins de dix minutes.

2.3.2.6. Notes et remarques diverses

L'installation est simple et ne requiert aucune configuration de la part de l'utilisateur. Le guide d'exploitation [GUIDES] propose toutefois plusieurs « bonnes pratiques » pour préparer l'installation et automatiser le lancement de WinPT au démarrage de Windows.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES], elle est jugée claire, lisible et ne peut pas conduire à de mauvaises interprétations.

2.3.4. Revue du code source (facultative)

La revue du code source a permis de constater que le projet GnuPG semble plus abouti que WinPT :

- Le projet GnuPG, mené par une équipe très active, a abouti a un produit mature. GnuPG est désormais considéré comme stable depuis fin 2006. Des correctifs de sécurité particulièrement soignés ont été émis régulièrement. Il devrait en être de même si de nouvelles failles apparaissaient. Dans l'ensemble, le code source est clair et laisse penser que la portabilité et la fiabilité du code ont été prises en comptes tout au long du développement.

- Le projet WinPT a été arrêté par son auteur (Timo Schulz) en décembre 2009 (bien que la version 1.4.3 ait été rendue disponible en mars 2010 seulement). Dans l'ensemble, le code source est moins clair que celui de GnuPG, le style de codage est hétérogène et n'est pas proprement finalisé.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Chiffrement symétrique de documents	**Réussite**
Déchiffrement symétrique de documents	**Réussite**
Chiffrement asymétrique et/ou signature de documents	**Réussite**
Déchiffrement asymétrique de documents	**Réussite**
Vérification de signature de documents	**Réussite**
Génération de bi-clés OpenPGP	**Réussite** *(voir le 1 du §2.3.7)*
Importation de clés OpenPGP	**Réussite** *(voir le 2 du §2.3.7)*
Gestion de la confiance des clés du trousseau	**Réussite**
Exportation de clés publiques	**Réussite**
Suppression de clés	**Réussite** *(voir le 3 du §2.3.7)*

2.3.6. Fonctionnalités non testées

Sans objet.

2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités

Les tests de conformité ont permis de détecter les non-conformités suivantes :

1. une fois une clé générée en DSA/ELG (en mode normal), toutes les clés suivantes seront également générées en DSA/ELG, que la case soit cochée ou non ;

2. l'importation de clés OpenPGP via un serveur de clés peut aléatoirement entraîner une fermeture forcée de WinPT ;

3. la suppression de l'intégralité du trousseau de clés ainsi que la suppression de plusieurs clés de manière concomitante peuvent entraîner une fermeture forcée de WinPT.

2.3.8. Avis d'expert sur le produit

Le produit WinPT est simple d'utilisation et sa prise en main ne demande pas de connaissance particulière du produit GnuPG. En utilisation « normale » (c'est-à-dire en utilisant WinPT tel que décrit dans le mode d'emploi [GUIDES]), l'application est stable.

Lorsque WinPT est utilisé dans le cadre décrit dans la cible de sécurité [CDS] (utilisateur n'ayant pas de connaissances poussées en informatique), il ne demande pas de compétence particulière si ce n'est de connaître les principes généraux de la cryptographie asymétrique.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés - résistance

Fonctions et mécanismes
Protection en confidentialité et en intégrité des documents
Protection en confidentialité, intégrité et disponibilité des fichiers de configuration
Déchiffrement et vérification de signature de GPG
Génération des bi-clés
Protection par mot de passe de la confidentialité des clés privées de l'utilisateur
Import et vérification de sa clé publique
Export de sa clé publique
Suppression de clés

2.3.9.2. Avis d'expert sur la résistance des mécanismes

La majorité des mécanismes listés dans le §2.3.9.1 étant des mécanismes cryptographiques, leur analyse est décrite dans le §2.4 du présent rapport.

Concernant les mécanismes non-cryptographiques, seule la modification du mot de passe a entraîné une remarque de l'expert. En effet, lors de la modification d'un mot de passe, WinPT ne vérifie pas la robustesse de ce dernier, il est donc possible de changer le mot de passe par une chaîne de caractères peu robuste voire même par une chaîne de caractères vide.

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues ayant un impact sur la sécurité de cette version du produit.

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

L'évaluation a permis de révéler plusieurs vulnérabilités non exploitables dans le contexte d'une configuration respectant les hypothèses d'environnements.

<u>Usurpation d'identité</u>

Il est possible pour un attaquant de piéger une clé pour usurper l'identité d'une personne avec qui l'utilisateur échange des informations chiffrées via WinPT. Lors de l'importation, WinPT ne détectera pas que cette clé est piégée. Cependant, pour que l'attaque aboutisse, l'utilisateur

doit se servir de GnuPG en ligne de commande (et non via WinPT) pour chiffrer son message. Dans ce cas, le message sera chiffré avec la clé de l'attaquant et non avec celle du destinataire légitime. Il est donc nécessaire de vérifier la validité d'une clé avant son importation et de ne pas utiliser WinPT et GnuPG en ligne de commande de manière concomitante (cf. §2.3.12.2).

Modification du fichier de configuration
Si un attaquant parvient à modifier le fichier de configuration gpg.conf, il peut alors récupérer des informations sensibles lors d'une génération de paire de clés.

Poste compromis
Si le poste d'un utilisateur est compromis (par un virus par exemple), un attaquant peut récupérer le mot de passe saisi lors du déchiffrement de la clé privée.

Avis d'expert
Ces deux dernières vulnérabilités doivent être tempérées par le fait qu'elles nécessitent toutes deux un accès au poste de l'utilisateur. Or, un attaquant ayant un tel accès aurait également la possibilité de récupérer les informations disponibles en clair sur le poste avant leur diffusion ou après leur réception. De plus, une protection purement logicielle de telles attaques n'est pas réaliste. Il est donc important de respecter les hypothèses d'environnement d'utilisation du produit pour s'en prémunir (cf. §2.3.12.2).

2.3.11. Accès aux développeurs

Sans objet.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Le choix et l'implémentation de certains algorithmes peuvent être problématiques si la configuration est modifiée sans prendre de précautions (typiquement, sans respecter les règles et recommandations de l'ANSSI concernant les mécanismes cryptographiques [CRY]).

2.3.12.2. Recommandations pour une utilisation sûre du produit

Configuration du produit
Le fichier gpg.conf de WinPT doit être configuré pour que les algorithmes cryptographiques utilisés respectent les règles et recommandations de l'ANSSI [CRY].

On rappelle que cette certification ne couvre pas l'utilisation de DSA/ElGamal[1] (DSA/ELG).

Utilisation de WinPT ou de GnuPG
Il est recommandé d'utiliser soit WinPT, soit GnuPG en ligne de commande (ne pas utiliser les deux conjointement).

[1] La génération de clés publiques à l'aide de l'algorithme DSA/ElGamal repose sur l'utilisation du générateur d'aléas de niveau 0. Ce générateur présente des faiblesses par rapport à l'état de l'art en la matière (cf. §2.5), qui peuvent avoir un impact sur la qualité des clés générées. Cependant, puisque seuls les paramètres publics de ces algorithmes sont concernés, ce point n'est pas jugé critique.

Vérification des clés
Des procédures organisationnelles doivent être mises en place afin de vérifier la validité d'une clé d'un utilisateur avant son importation (vérification de l'intégralité du haché).

Choix du mot de passe
La robustesse du mot de passe n'étant pas vérifiée lors d'une modification de ce dernier, il est recommandé d'utiliser uniquement des mots de passe longs mélangeant majuscules, minuscules, chiffres et caractères spéciaux.

Sécurité du poste
L'utilisation du produit doit être faite sur un ordinateur correctement administré et hébergeant un système d'exploitation à jour de ses correctifs de sécurité. Il doit être protégé par un produit anti-virus (avec bases d'information à jour et proposant des fonctions de détection des infections informatiques furtives - anti-spyware, anti-rootkit, etc.) et un pare-feu correctement configuré.

Le produit ne devrait pas être utilisé en cas de doute sur la sécurité du système.

2.3.12.3. Avis d'expert sur la facilité d'emploi

WinPT est un produit simple à utiliser. Il a été conçu pour utiliser GnuPG de façon intuitive pour l'utilisateur. Il n'est pas nécessaire pour ce dernier de connaître GnuPG ou d'avoir de compétences avancées en informatique.
Les principales fonctions de WinPT sont d'un accès simple (sur le bureau de l'ordinateur ou dans la barre de lancement rapide) et sont regroupées sous :

- le « gestionnaire de clés » pour la gestion du trousseau de clés ;
- le « gestionnaire de fichiers » pour la manipulation des documents.

2.3.12.4. Notes et remarques diverses

Sans objet.

2.4. Analyse de la résistance des mécanismes cryptographiques

L'analyse de la résistance des mécanismes cryptographiques a montré que les algorithmes annoncés dans le document des spécifications cryptographiques [SPEC-CRY] (RIPEMD-160, SHA256, AES-256, RSA 2048) sont correctement implémentés dans GnuPG version 1.4.10.

Cas de l'algorithme ElGamal (DSA/ELG)
Conformément à la cible de sécurité et au paragraphe 1.2.4 du présent document, l'algorithme DSA/ElGamal n'a pas été évalué.

2.5. Analyse du générateur d'aléas

Le produit évalué offre un générateur d'aléas qui peut être utilisé par le logiciel.

Le générateur d'aléas permet de générer trois types d'aléas, niveau 0 (qualité non cryptographique), niveau 1 (qualité moyenne) et niveau 2 (qualité haute).

Les tests statistiques effectués sur le générateur d'aléas de niveau 2 ont validé son fonctionnement.

Les tests statistiques effectués sur le générateur d'aléas de niveau 1 (le plus utilisé) ont montré une certaine faiblesse dans leur production sur un PC sous Windows XP SP3 (32 bits). Cependant, le retraitement cryptographique effectué après la génération permet d'utiliser ce niveau d'aléa de manière sûre.

Les tests statistiques effectués sur le générateur d'aléas de niveau 0 sous Windows XP SP3 (32 bits) ont montré d'importantes faiblesses. Ce niveau étant utilisé uniquement dans le processus de création d'une clé DSA/ElGamal (hors périmètre de l'évaluation), cela n'est pas jugé critique dans le cadre de cette évaluation.

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 « WinPT**,** Version 1.4.3 **»** reposant sur le moteur cryptographique « GnuPG version 1.4.10b » répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS].

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 spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité du produit GnuPG - WinPT ;* *Version 2* ; Date : *07/03/2011*
[RTE]	*Rapport Technique d'Évaluation CSPN ;* Référence : *MEF040-RTE-1.01* ; Date : *11/03/2011*
[SPEC-CRY]	*Spécifications Cryptographiques ;* Référence : *MEF040-SpecCrypto-1.01* ; Date : *10/01/2011*
[GUIDES]	Guide d'installation : *Manuel d'installation de l'outils de chiffrement ;* *Version 1.4* ; Date : *25/06/2010* Guide d'exploitation : *Instruction technique d'exploitation de l'outil de chiffrement ;* *Version 1* ; Date : *07/10/2010* Guide d'utilisation : *Mode d'emploi de l'outil de chiffrement ;* *Version 2.5* ; Date : *07/10/2010*
[RFC4880]	*OpenPGP Message Format ;* Date : *Novembre 2007*

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 (CSPN) des technologies de l'information, version 2. 4, phase expérimentale, n° 915/SGDN/DCSSI/SDR/CCN du 25 avril 2008. Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1. 4. Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1. 3. Documents disponibles sur www.ssi.gouv.fr
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr