Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTERE DU BUDGET, DES COMPTES PUBLICS, DE LA FONCTION PUBLIQUE ET DE LA REFORME DE L'ETAT

Cible de sécurité du produit GnuPG – WinPT

Logiciel GnuPG version 1.4.10
Logiciel WinPT version 1.4.3

Historique des modifications

Version	Date	Objet de la modification
0	25/02/2010	Création du document
1	26/03/2010	Correction du document
2	7/03/2011	Prise en compte des remarques lors de l'évaluation
2.1	10/05/2011	Corrections mineures

Tél. 01 53 44 27 93 Fax. 01 53 44 29 27

Sommaire

I. Identification du produit 3
II. Argumentaire (description) du produit 3
III. Description de l'environnement technique dans lequel le produit doit fonctionner 3
IV. Définition du périmètre d'évaluation 4
V. Description des biens sensibles que le produit doit protéger 5
VI. Description des menaces 5
VII. Description des fonctions de sécurité du produit 5

I. Identification du produit

Organisation éditrice	GnuPG team
Lien vers l'organisation	http://www.gnupg.org
Nom commercial du produit	GPG (Gnu Privacy Guard)
Numéro de la version évaluée	GnuPG 1.4.10b compiled for Microsoft Windows
Catégorie de produit	Stockage sécurisé

Organisation éditrice	WinPT project
Lien vers l'organisation	http://winpt.gnupt.de
Nom commercial du produit	WinPT (Windows Privacy Tray)
Numéro de la version évaluée	WinPT version 1.4.3
Catégorie de produit	Stockage sécurisé

II. Argumentaire (description) du produit

Ce produit permet de chiffrer et déchiffrer des fichiers informatiques sous Windows.

GnuPG est un logiciel permettant, en ligne de commande, de générer des bi-clés de chiffrement et de chiffrer (respectivement, déchiffrer) et/ou signer (respectivement, vérifier la signature) de documents. Ce produit libre implémente le standard OpenPGP définit par la norme RFC 4880.

WinPT est une interface utilisateur de GnuPG, pour Windows, permettant de réaliser par son intermédiaire une large part des fonctions de ce produit :
- Modification de la configuration de GPG (et de WinPT) ;
- Création de bi-clés ;
- Gestion des clés publiques ;
- Signature et/ou chiffrement de documents ;
- Déchiffrement et/ou vérification de documents.

III. Description de l'environnement technique dans lequel le produit doit fonctionner

Ce produit est prévu pour fonctionner sur un poste de travail de type bureautique Windows 32 bits. Le produit démarre à l'ouverture de la session et reste actif en permanence.

Ce produit est destiné à des utilisateurs, n'ayant pas de connaissance poussée de l'informatique ni de Windows, disposant des droits nécessaires sur leur poste de travail et désirant assurer la confidentialité et/ou la signature des documents qu'ils stockent sur des supports ou échangent via les réseaux qui leur sont disponibles, éventuellement la messagerie électronique.

Des documents peuvent être importés et exportés par l'utilisateur depuis sa messagerie, ou des supports de données amovibles. La machine et le réseau informatique interne font l'objet d'un contrôle de l'innocuité des informations échangées. Seuls les documents chiffrés ne peuvent pas avoir fait l'objet d'un contrôle de leur innocuité. En particulier les clés (au format .asc) ont pu être contrôlées (mais pas pour le respect de la norme OpenPGP).

Une configuration spécifique des paramétrages de GPG (options de fonctionnement, algorithmes imposés…) est mise en place.

Les clés publiques des utilisateurs peuvent être diffusées par tout moyen.

H0 : Le produit installé est conforme à celui diffusé par l'organisation éditrice.
H1 : Le produit est installé sur un poste sain afin d'assurer la protection en intégrité du produit lui-même et des secrets qu'il manipule.
H2 : le poste de travail sur lequel fonctionne le produit doit être correctement configuré et administré (droits des utilisateurs nécessaires et suffisants, activation de mécanismes de verrouillage de session en cas d'inactivité, pare-feu correctement configurés (mais autorisant les documents chiffrés d'extension .gpg), antivirus avec base de donnée à jour, « anti-spyware », anti-rootkit, etc).
H3 : L'utilisateur doit être sensibilisé à la protection de son poste de travail et aux bonnes pratiques en matière de sécurité (règles sur la qualité des mots de passe ou phrases secrètes, règles permettant d'éviter la compromission de ses secrets, etc).
H4 : L'environnement opérationnel ne permet pas à un attaquant d'accéder au poste de travail, celui-ci comporte en effet en permanence des données sensibles (documents non chiffrés, secrets). La protection du poste de travail contre un accès est jugée répondre aux besoins de sécurité de l'organisation.
H5 : L'utilisateur est de confiance et sait utiliser les logiciels.
H6 : Les administrateurs du poste et du réseau interne sont de confiance.
H7 : Les autres utilisateurs externes ou des réseaux ne sont pas de confiance.

IV. Définition du périmètre d'évaluation

Il concernera GnuPG 1.4.10b et WinPT 1.4.3 sous Windows XP. D'autres compilations et extensions existent pour de nombreux autres OS mais elles ne sont pas visées ici.

L'interface WinPT utilisée est en langue française.

L'utilisation de cette solution de chiffrement est prévue pour une communauté restreinte de correspondants qui se connaissent (peuvent échanger en face à face, par tel, mel…).

Les clés sont générées directement sur le poste de l'utilisateur et seule sa clé publique est diffusée à ses correspondants. L'empreinte de la clé de signature est diffusée aux correspondants par un autre vecteur de communication que la clé publique (ou en face à face).

La confiance des clés publiques importées est attribuée individuellement par l'utilisateur après vérification de l'empreinte de la clé, et les clés sans confiance ou obsolètes sont supprimées du trousseau de clés.

Les documents sont signés&chiffrés et déchiffrés avec le gestionnaire de fichier de WinPT (pas le presse-papier ni dans la fenêtre active). Les raccourcis de WinPT ne sont pas activés.

La configuration retenue prévoit l'utilisation de RSA 2048, AES 256 et SHA256.

Un certain nombre de fonctionnalités de GPG ne sont pas utilisées (chiffrement symétrique seul, chiffrement non signé…).

V. Description des biens sensibles que le produit doit protéger

Les biens sensibles sont :
B1 : Les documents signés et chiffrés par GnuPG
B2 : La configuration et les documents du PC de l'utilisateur (logiciels, clé privée notamment)

Les fonctions sensibles sont :
F1 : La fonction de génération des bi-clés
F2 : La fonction de chiffrement et de signature de GPG
F3 : La fonction de déchiffrement et de vérification de signature de GPG
F4 : La fonction d'import et de vérification des clés publiques
F5 : La fonction d'export de sa clé publique
F6 : La suppression de clés

	Confidentialité	intégrité	Disponibilité
B1	X	X	
B2	X	X	X
F1		X	
F2	X	X	
F3		X	
F4		X	X
F5		X	
F6		X	X

VI. Description des menaces

M1 : un attaquant récupère le document chiffré d'un utilisateur (B1) lors de sa diffusion sur un réseau ou sur un support qu'il récupère en vue d'accéder à l'information en clair.
M2 : un attaquant modifie le contenu du document signé d'un utilisateur (B1) lors de sa diffusion sur un réseau ou sur un support physique qu'il intercepte.
M3 : un attaquant envoie à l'utilisateur un document signé en se faisant passer pour un correspondant dont la clé publique est connue et a été vérifiée par l'utilisateur.
M4 : un document reçu d'un attaquant et traité par l'utilisateur légitime avec les logiciels WinPT et/ou GPG modifie la configuration ou les documents du PC de l'utilisateur (B2) à son insu (notamment le produit ou son trousseau de clés publiques).
M5 : un attaquant récupère la clé privée protégée par mot de passe d'un utilisateur et tente d'accéder au clair de cette clé en vue de la réutiliser à l'insu de son propriétaire légitime.

VII. Description des fonctions de sécurité du produit

Le produit GPG – WinPT implémente les fonctions de sécurité suivantes
- Chiffrement symétrique de documents
- Déchiffrement symétrique de documents
- Chiffrement asymétrique et/ou signature de documents
- Déchiffrement asymétrique de documents
- Vérification de signature de documents
- Protection par mot de passe de la confidentialité des clés privées de l'utilisateur
- Génération de bi-clés OpenPGP

- Importation de clés OpenPGP
- Gestion de la confiance des clés du trousseau
- Exportation de clés publiques
- Suppression de clés

Les fonctions cryptographiques sont implémentées conformément à la RFC 4880.

○○○