

Configuration publique pour Windows 64 bits

Logiciel GnuPG version 1.4.19
Logiciel WinPT versions 1.4.3c ou d
Logiciel GPGe version 1.4.4
Logiciel GPGe64 version 1

Historique des modifications

Version	Date	Objet de la modification
0	08/03/2012	Création du document
1	14/03/2012	Validation du document
2	16/05/2013	Ajout de la version 1.4.3c de WinPT
3	06/01/2014	Evolution de version des logiciels pour raison de sécurité
4	21/05/2014	Ajout GPGe 1.4.3 pour correction bug avec Outlook
5	10/02/2015	Changement des versions et ajout adaptateur 64 bits
5.1	16/03/2015	Evolution de la version GnuPG pour raison de sécurité

Sommaire

Sommaire	2
I – Les logiciels utilisés avec les OS 64 bits	3
II – Installation réalisée sur un OS 64 bits	3
III – Passage de l’installateur 32 bits à celui 64 bits	4

I – Les logiciels utilisés avec les OS 64 bits

Le dispositif de chiffrement pour les OS Windows 64 bits est composé de 4 logiciels.

GnuPG (GNU Privacy Guard) qui est le véritable logiciel réalisant les opérations de chiffrement, mais qui ne peut s'utiliser directement qu'en ligne de commande. Ce logiciel, existe avec des déclinaisons pour les différents environnements Linux, Unix, MacIntosh et Windows. La déclinaison utilisée ici est faite pour les environnements 32 bits de Windows (NT/2000/ME/XP/Vista/Windows 7). Cette déclinaison fonctionne également correctement dans les versions 64 bits de ces OS car ces versions prévoient une compatibilité pour les applications 32 bits, qui sont installées dans un dossier spécifique **C:\Program Files (x86)**.

WinPT (Windows Privacy Tray) qui est une interface Windows pour GnuPG permettant, avec cette interface plus conviviale, de créer les clés signature et de chiffrement et de stocker les clés publiques des partenaires, ainsi que de chiffrer et déchiffrer des documents. La version utilisée fonctionne dans tous les environnements 32 bits de Windows (NT/2000/ME/XP/Vista/Windows 7), mais également en 64 bits grâce au mode de compatibilité intégré dans les OS 64 bits, comme pour GnuPG.

GPGe (GNU Privacy Guard Explorer Extension) est une extension qui permet de chiffrer et déchiffrer directement depuis l'explorateur Windows, avec un clic droit sur un document. Mais GPGe n'est pas un logiciel autonome, c'est en fait une extension pour l'explorateur Windows (explorer.exe) qui s'exécute dans le cadre du processus de l'explorateur Windows. Il s'agit d'une .dll 32 bits, qui de ce fait ne peut fonctionner qu'avec un explorateur 32 bits et pas 64 bits. **GPGe ne fonctionne donc pas nativement dans un OS 64 bits, contrairement aux 2 logiciels précédents.** Il est de fait incapable de fonctionner dans un explorateur 64 bits, il n'apparaît donc même pas dans le menu contextuel de l'explorateur dans ce cas.

GPGe64 (GNU Privacy Guard Explorer Extension adaptateur 64 bits) est une application 32 bits permettant d'émuler GPGe dans un environnement 64 bits. La première version ainsi diffusée connaît encore quelques limitations (OS n'accepte pas de lancer le chiffrement simultané de plus de 15 fichiers, ne fonctionne que dans l'explorateur Windows et pas sur le bureau ni dans un autre explorateur).

Un installateur spécifique pour les OS 64 bits, installant ces 4 logiciels est présenté par l'« Instruction technique d'exploitation de l'outil de chiffrement ». L'utilisation de l'installateur prévu pour des environnements Windows 32 bits qui était suggérée jusqu'alors, avec en adaptation l'installation d'un explorateur 32 bits n'est plus la solution recommandée pour XP/Vista et Windows 7 64 bits.

II – Installation réalisée sur un OS 64 bits

L'installateur va installer les principaux composants informatiques de la façon suivante sur un OS 64 bits ("user" désigne le profil de l'utilisateur) :

C:\Program Files(x86)\ comporte :

les logiciels (sous dossier GNU).

C:\Users\“user name”\AppData\Roaming\gnupg\ (chemin C:\Documents and Settings\“user name”\Application Data\gnupg\ sous XP) comporte :

- le fichier de configuration de GPG (gpg.conf) ;
- le trousseau de clés avec leur niveau de confiance (pubring.gpg, secring.gpg et trustdb.gpg).

C:\Users\“user name”\Documents\GPG\Clés\ (chemin C:\Documents and Settings\“user name”\ Mes documents\GPG\Clés\ sous XP) comporte :

- des copies du trousseau de clés mises à jour à chaque arrêt de WinPT (sekring-bak.gpg pour les clés secrètes et 3 copies tournantes des clés publiques pubring-bak-0 à 2.gpg).

III – Passage de l’installateur 32 bits à celui 64 bits

Pour un ordinateur 64 bits déjà installé sans GPGee64 (avec un installateur 32 bits), il convient de commencer par désinstaller les logiciels de chiffrement avec l’installateur précédent (et éventuellement d’enlever aussi QDir ou l’autre explorateur 32 bit installé). Après avoir redémarré la machine, le nouvel installateur 64 bits pourra alors être utilisé.

○○○