Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

Instruction technique d'exploitation de l'outil de chiffrement public

Logiciel GnuPG version 1.4.19
Logiciel WinPT version 1.4.3c ou d
Logiciel GPGee version 1.4.4
(Logiciel GPGee64 version 1)

Historique des modifications

Version	Date	Objet de la modification
0	6/9/2010	Création du document
1	7/10/2010	Compléments
2	21/09/2011	Prise en compte des remarques des évaluateurs avec la v1.4.3a
2.1	13/09/2012	Ajout d'éléments sur les OS 64 bits
2.2	16/05/2013	Correction de bugs supplémentaires avec la v1.4.3c
2.3	6/01/2014	Changement de versions pour raison de sécurité
2.4	21/05/2014	Ajout GPGee 1.4.3 pour correction bug avec Outlook
3	5/03/2015	Montée de version (sécurité) et ajout d'un adaptateur 64 bits
3.1	16/03/2015	Changement de version de GnuPG pour raison de sécurité

Fax. : 01 53 44 29 27

Sommaire

A - Présentation des logiciels

1) Le logiciel **GnuPG** (GNU Privacy Guard), encore appelé **GPG** par raccourci, est l'utilitaire GNU (ancien projet libre concurrent d'Unix) permettant des communications et le stockage de données sécurisés. On peut s'en servir pour chiffrer des données avec différents protocoles et pour créer des signatures numériques. Doté d'un système évolué de gestion de clés, il respecte le standard OpenPGP décrit par la RFC 4880. Il s'efforce aussi d'être compatible avec le logiciel commercial PGP de NAI Inc.

http://www.gnupg.org/ est le site de la communauté faisant évoluer ce logiciel.

GnuPG fait partie de la famille d'outils et d'applications GNU conçus et distribués en accord avec la General Public License (GPL). En conséquence le logiciel peut être librement copié, utilisé, modifié et distribué tout en respectant les termes de cette licence.

Ce logiciel, fonctionne dans les environnements Linux, Unix, MacIntosh et Windows 95/98/NT/2000/ME/XP/Vista/Windows 7 (32 et 64 bits).

Ce logiciel est accessible en ligne de commande, aussi, un outil complémentaire est nécessaire pour en permettre une utilisation plus conviviale sous Windows avec une interface utilisateur facile d'emploi, notamment permettant d'utiliser la souris.

2) **WinPT** (Windows Privacy Tray) est une interface de GnuPG pour Windows permettant 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 Win32 (NT/2000/ME/XP/Vista/Windows 7), mais également en 64 bits.

http://winpt.wald.intevation.org est le site de la communauté faisant évoluer ce logiciel.

La version 1.4.3c est une évolution faite par l'administration française de la version 1.4.3, réalisée pour prendre en compte les remarques suite à la certification, corrigeant quelques bugs pour améliorer sa sécurité et clarifier le libellé de certains messages. La 1.4.3d améliore quelques écrans.

3) **GPGee** (GNU Privacy Guard Explorer Extension) est une extension qui permet de chiffrer et déchiffrer directement depuis l'explorateur Windows à partir d'un clic droit sur un document. Cela ouvre un menu contextuel permettant de réaliser les principales opérations de chiffrement et déchiffrement. La version utilisée fonctionne dans les environnements Win32 uniquement. La dernière version 1.4.4 a été corrigée par l'administration et sa diffusion reste pour l'instant spécifique. Elle gère 4 langues : anglais, français, allemand, portugais.

Ce logiciel était diffusé sur le site excelcia.org, qui ne semble plus fonctionner que de façon erratique depuis 2008.

4) **GPGee64** (GNU Privacy Guard Explorer Extension adaptateur 64 bits) est une nouvelle application 32 bits permettant d'émuler GPGee 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). L'installation de cet adaptateur remplace la solution de contournement précédemment proposée pour les OS 64 bits.

Tous ces logiciels sont distribués sous une licence GNU General Public Licence qui vous donne le droit de les utiliser librement et gratuitement, mais pas de les vendre ou de les distribuer sous une autre forme de licence.

L'espace disponible nécessaire pour installer l'ensemble des 3 premiers logiciels sur une machine 32 bits est de 6.4 Mo (GPG : 3.1 Mo. ; WinPT : 1.1 Mo GPGee : 2.2 Mo), et en 64 bits, avec les 4 logiciels, de 6.9 Mo (GPGee64 0.5 Mo).

Des réglages importants pour la sécurité, ne sont pas forcément bien configurés sur les logiciels téléchargeables sur Internet (ni les bonnes versions, en particulier en français), aussi deux installateurs sont mis à disposition par le ministère du budget, des comptes publics et de la réforme de l'état afin de bien réaliser leur installation.

Un premier installateur est uniquement prévu pour des environnements Windows 32 bits Win32 (NT/2000/ME/XP/Vista/Windows 7 32 bits) installe les 3 premiers logiciels.

Un second installateur prévu pour Windows 7 64 bits installe les 4 logiciels.

B – Les étapes de l'installation du logiciel

L'installation complète des logiciels doit être réalisée à l'aide de l'installateur mis à disposition par le ministère du budget, des comptes publics et de la réforme de l'état.

Cette installation comporte également en plus les opérations suivantes :

- L'ajustement de l'environnement de travail sous Windows ;
- La création des clés (bi-clé) de chiffrement de l'utilisateur.

Il convient que l'utilisateur soit présent pour cette dernière opération afin de pouvoir définir son mot de passe attaché à l'utilisation de son bi-clé et récupérer la sauvegarde de son bi-clé.

Pour pouvoir utiliser en pratique le logiciel, l'utilisateur aura encore besoin d'importer les clés publiques de ses partenaires et de leur transmettre la sienne. Ces actions sont décrites par le mode d'emploi utilisateur.

C – Cas de l'installation d'une nouvelle version des logiciels

Pour un poste 32 bits comportant déjà une précédente version des logiciels.

Il convient d'identifier si cette installation a été faite avec une version antérieure de cet installateur ou par un autre moyen :

- Si c'était avec une précédente version de cet installateur, le nouveau va correctement modifier les éléments préexistants. Pour contrôler ce point il est possible de vérifier dans Panneau de configuration de Windows, si la fenêtre « Désinstaller ou modifier un programme » comporte bien un précédent installateur « WinPT Vxxx, GnuPG Vyyy, GPGee Vzzz » édité par la DGFIP. Après avoir arrêté les logiciels (notamment quitté WinPT qui peut être dormant dans la barre de tâches), il suffit alors de procéder comme indiqué au D et éventuellement de tester l'installation comme indiqué au F.
- Dans le cas contraire il est préférable, après les avoir arrêtés, de désinstaller ces logiciels (par exemple avec les uninstall de GPG et GPGee, et pour WinPT en supprimant le dossier dans Program_Files\GNU). Redémarrez ensuite le PC, puis recherchez et supprimez toutes les clés de base de registre (utiliser la commande regedit) évoquant WinPT et GPGee qui pourraient subsister (la nouvelle installation de GPGee pourrait sinon être perturbée). Le nettoyage de la base de registre devrait notamment vous conduire à supprimer :
  - les clés software\GNU ; GPGEE ; et WinPT de HKEY$\« user » et de HKEY$\local machine (lorsqu'elles existent).
  - la chaine HKEY$\« user »\Control panel\MingW32\NLS\MODir et la clé HKEY$\« user »\Control panel\MingW32 si elle ne comporte plus rien d'autre.

  Par contre, ne supprimez pas de document ou dossier dans Mes_Documents ou dans Application_Data. Après un nouveau redémarrage du PC, procédez comme indiqué au D et éventuellement testez comme indiqué au F.

Pour un poste 64 bits comportant déjà une précédente version des logiciels.

Si une installation 32 bits des logiciels préexistait, il convient de la désinstaller en préalable (avec le msi utilisé pour cette première installation, …), et de redémarrer le PC avant de passer à la nouvelle installation.

Si c'est un installation réalisée avec une version précédente de l'installateur 64 bits, il suffit alors de procéder comme indiqué au D et éventuellement de tester l'installation comme indiqué au F.

L'installation de la nouvelle version de GPGee fera oublier : les groupes de clés déjà créés et la clé de signature par défaut. Ces données seront à recréer. Les trousseaux de clés préexistants, eux, ne seront pas modifiés, aussi la création de clé présentée au E n'est pas à réaliser. Il est cependant recommandé de faire préalablement une sauvegarde des clés (cf. mode d'emploi).

D - Installation des logiciels

Préparation du poste de travail

Ces logiciels de chiffrement devant traiter des données ayant un caractère confidentiel, ils doivent être installés sous un profil utilisateur individuel réservé à cette personne et nécessitant une authentification par mot de passe (et **pas sous le profil de l'administrateur**). Par ailleurs sur la machine l'écran de veille doit être activé avec une reprise protégée par mot de passe (Propriété de l'affichage Windows) et la machine doit être équipée des outils de protection classiques. Enfin si le PC équipé est un portable pouvant quitter l'enceinte de l'organisme, la mise en place d'une protection particulière des données sur les disques durs est nécessaire (par exemple leur chiffrement).

Dans le dossier « Mes document » de l'utilisateur créez un sous-dossier « Mes documents\GPG » qui n'est pas partagé avec d'autres utilisateurs. Ce dossier servira à stocker les documents chiffrés échangés et les documents déchiffrés, en attendant leur suppression. Créer également un sous-dossier « Mes documents\GPG\Clés », non partagé, qui servira à enregistrer les clés publiques transmises par les correspondants et à recevoir la copie des trousseaux de clés destinée à être sauvegardée.

Pour pouvoir utiliser la fonctionnalité de création automatique du mel d'envoi, il faut que le composant mapi soit installé et correctement paramétré.

Au niveau de la boite de messagerie (mel) de l'utilisateur, créer dans un dossier d'archivage des mels un sous-dossier GPG. Ce sous-dossier servira à stocker les messages reçus et transmis avec une pièce jointe cryptée, en attendant leur suppression.

Installation des logiciels

Démarrer sur son ordinateur une session pour l'utilisateur devant être doté de ces logiciels de chiffrement. Accroître éventuellement les droits attribués à ce profil le temps de l'installation pour que le .msi puisse s'exécuter.

Fermez toutes les fenêtres et les applications en fonctionnement.

L'installateur comportant les bonnes versions des logiciels pour un OS windows 32 bits est « Install_32 bits_WinPT_1.4.3d_GnuPG_1.4.19_GPGee_1.4.4_v9.0.msi ». Ce MSI daté du 12/03/2015 fait 3 049 984 octets et son empreinte SHA1 est : 3073ac80bbb99466faa65fb41e6fa9245d1b4285.

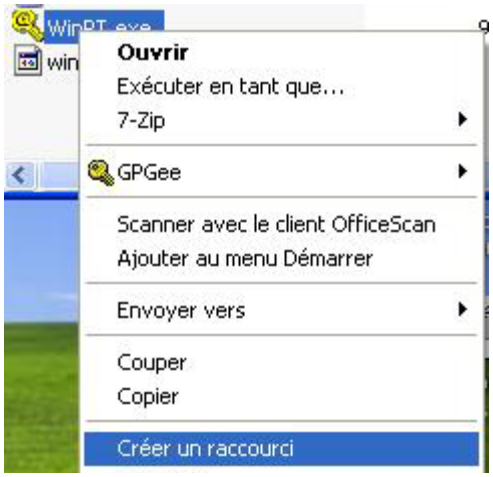
L'installateur comportant les bonnes versions des logiciels pour un OS windows 64 bits est « Install_64 bits_WinPT_1.4.3d_GnuPG_1.4.19_GPGee_1.4.4_GPGee64_1_v7.msi ». Ce MSI daté du 12/03/2015 fait 3 297 280 octets et son empreinte SHA1 est : 1dc8cd00eebcc66292c9258728c768b3eef2f79f.

Lancer l'installateur en double-cliquant dessus.

L'interface d'installation se lance et il suffit de la suivre pas à pas en sélectionnant le bon dossier d'installation des programmes. L'installation dure normalement 1 minute.

Améliorations pour l'utilisateur

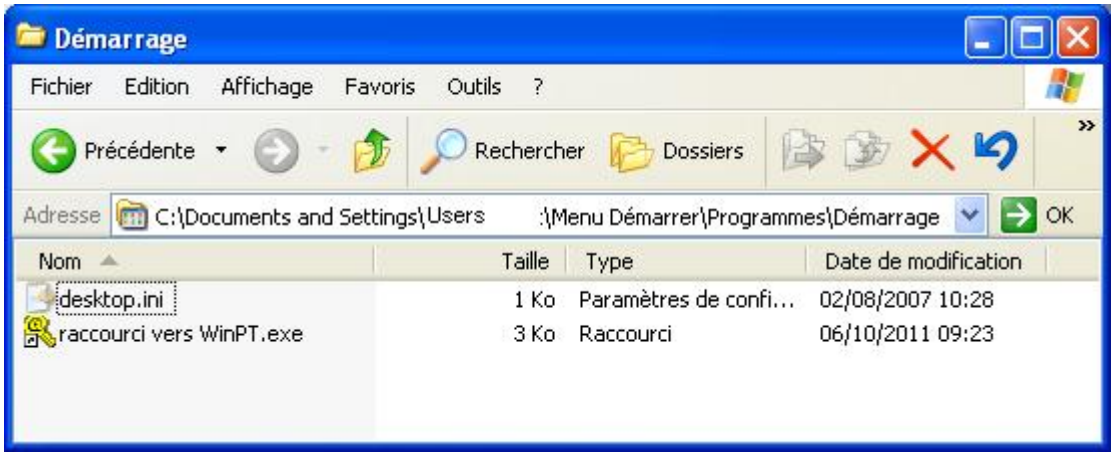
Dans le dossier C:\Program Files\GNU\WinPT (C:\Program Files (x86)\GNU\WinPT en 64 bits), faites un clic-droit sur WinPT.exe et choisir de « Créer un raccourci »



Pour permettre le lancement automatique de WinPT au démarrage de l'ordinateur copiez ce raccourci « WinPT » dans le dossier de démarrage à l'emplacement :

C:\Users\"user name"\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup (ou C:\Documents and Settings\« user name»\Menu Démarrer\Programmes\Démarrage sous XP).

Ce dossier doit alors au moins comprendre l'élément suivant :



En plus (ou à la place) du raccourci créé sur le bureau par l'installateur vous pouvez, ajouter le raccourci WinPT dans la barre de lancement rapide.

Ça y est les logiciels sont prêts à fonctionner.

Redémarrez alors l'ordinateur sous le profil de l'utilisateur. Vous allez alors passer à l'étape de création des clés de chiffrement.

E - Création des clés personnelles

Lors du redémarrage de l'ordinateur et de WinPT, celui-ci va automatiquement vous demander de créer le couple de clés privées et publiques (bi-clé) de l'utilisateur.

Avant de démarrer ces étapes l'utilisateur doit être présent (pour définir son mot de passe) vous devez vous pourvoir également d'une disquette, d'une clé USB ou de tout autre support de sauvegarde amovible.

Ouvrir alors une session sous le profil de l'utilisateur.

Démarrage de WinPT

Normalement WinPT démarre automatiquement. Si ce n'est pas le cas, cela signifie qu'une des opérations précédente n'a pas été correctement réalisée. Si vous voulez quand même lancer WinPT cliquez sur le raccourci WinPT situé sur le bureau (ou dans la barre de lancement rapide).

L'écran suivant apparaît alors, vous demandant de créer le bi-clé de l'utilisateur :

Cliquez sur le bouton « OK ».

Saisie des identifiants

Vous obtenez maintenant un écran qui va vous permettre de créer le bi-clé de l'utilisateur.

Aucune parenthèse ( ) ou crochet < > ne doit être utilisée lors de cette saisie, évitez également d'utiliser des lettres accentuées (é, â ù…).

Par souci de lisibilité des clés ainsi créées, pour les partenaires, il est recommander de saisir dans le champ « Nom » :

- la structure d'appartenance de l'utilisateur (sigle avec le n° de département d'implantation ou la ville ; par exemple : DDEF 96) ;
- éventuellement suivi de l'unité dans la structure (si plusieurs unités participent aux échanges) ;
- et puis, si ils ne figurent pas dans l'adresse mel, le nom et prénom de l'utilisateur séparés par un espace.

Saisissez l'adresse mel professionnelle utilisée pour les échanges (celle de l'utilisateur, celle d'une boite fonctionnelle…).

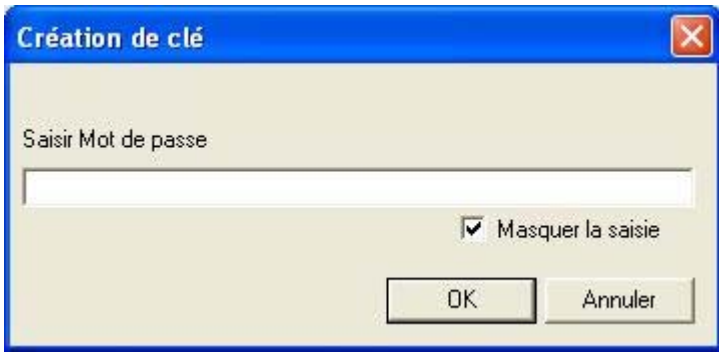
Ne pas cocher la case « Créer des clés DSA/ELG ». Ce format de clé ne présente pas un niveau de sécurité suffisant. La saisie doit avoir l'apparence indiquée ci-dessus.

Cliquez maintenant sur le bouton « OK ».

Saisie du mot de passe

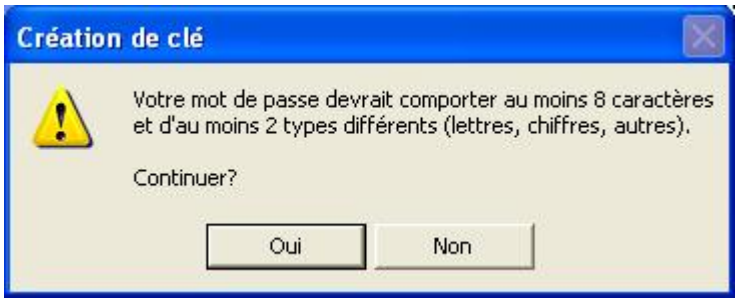
L'écran suivant apparaît vous demandant un mot de passe (« Saisir Mot de passe ») pour la clé privée. Décochez éventuellement la case « Masquer la saisie » pour pouvoir voir la saisie. L'utilisateur saisi son mot de passe qui doit comporter au minimum des chiffres et des lettres (ou des caractères spéciaux) et comporter au moins 8 caractères (exemple : maison28).

Ce mot de passe doit être facilement mémorisé par l'utilisateur car sa perte empêchera de chiffrer et déchiffrer les documents. Il est possible que l'utilisateur note son mot de passe sur un document qui doit alors être conservé à un emplacement sûr (par exemple tiroir fermé à clé).



Cliquez ensuite sur le bouton « OK ».

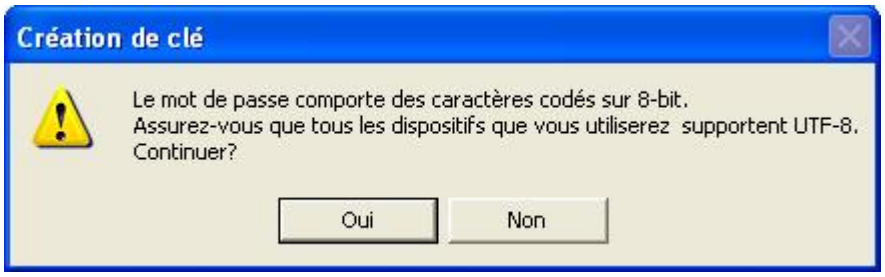
(Si le mot de passe ne répond pas aux critères indiqués ci-dessus un écran d'alerte apparaît.



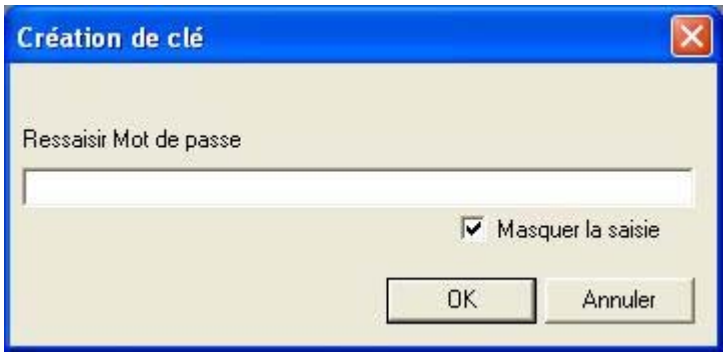
Si vous souhaitez quand même utiliser ce mot de passe cliquez sur le bouton « Oui » sinon cliquez sur le bouton « Non » pour revenir à l'écran précédent et recommencer.)

Un nouvel écran vous demande de saisir un seconde fois le mot de passe (« Ressaisir Mot de passe »).

(Si le mot de passe comporte des caractères « très » spéciaux, vous pouvez également obtenir le message d'alerte suivant :



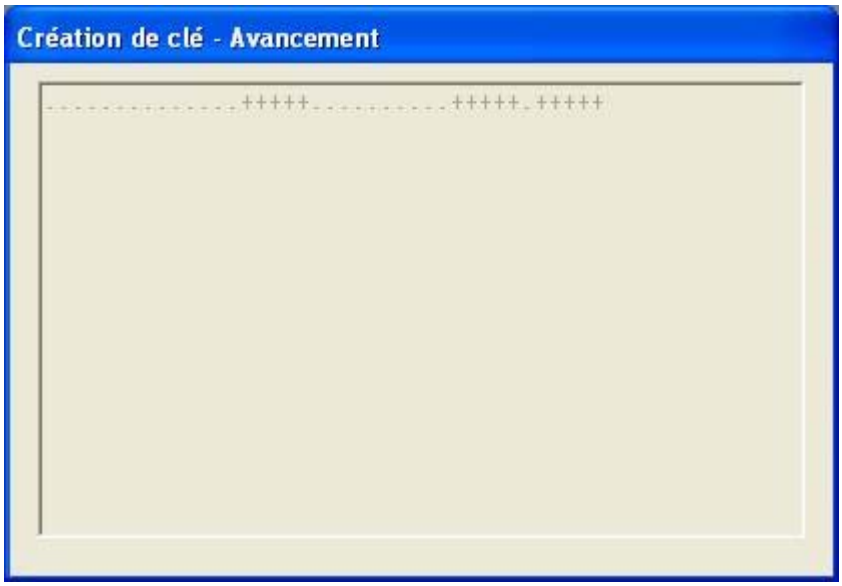
Si vous devez utiliser votre clé de chiffrement sur une autre machine installée différemment, cliquez sur le bouton « Non » pour revenir à l'écran précédent et recommencer, sinon cliquez sur le bouton « Oui ».)



Décochez la case « Masquer la saisie » pour pouvoir voir la saisie. L'utilisateur ressaisi le même mot de passe que sur le premier écran, puis cliquez sur le bouton « OK ».

Génération des clés

L'écran suivant apparaît pendant la génération des clés. Remuez votre souris, tapez sur le clavier, pour augmenter le hasard dans la génération des clés (et passer le temps).

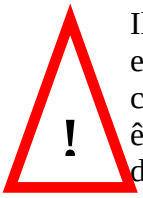


Lorsque la génération des clés est terminée, l'écran suivant d'avertissement apparaît pour vous le signaler.

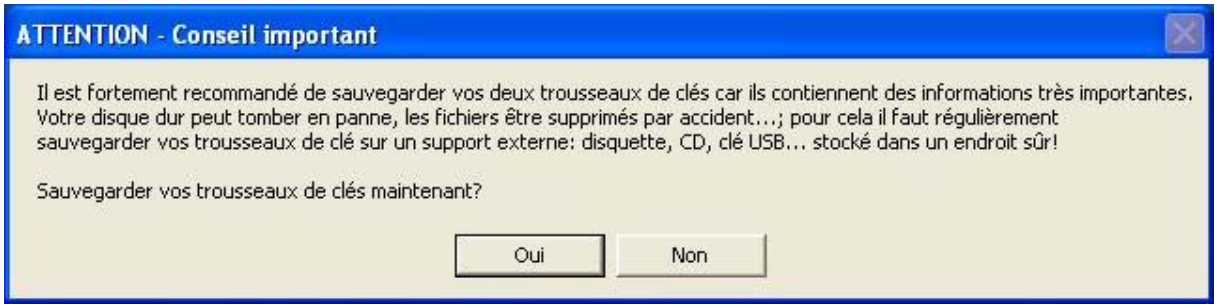
Cliquez sur le bouton « OK ».

Création d'une sauvegarde

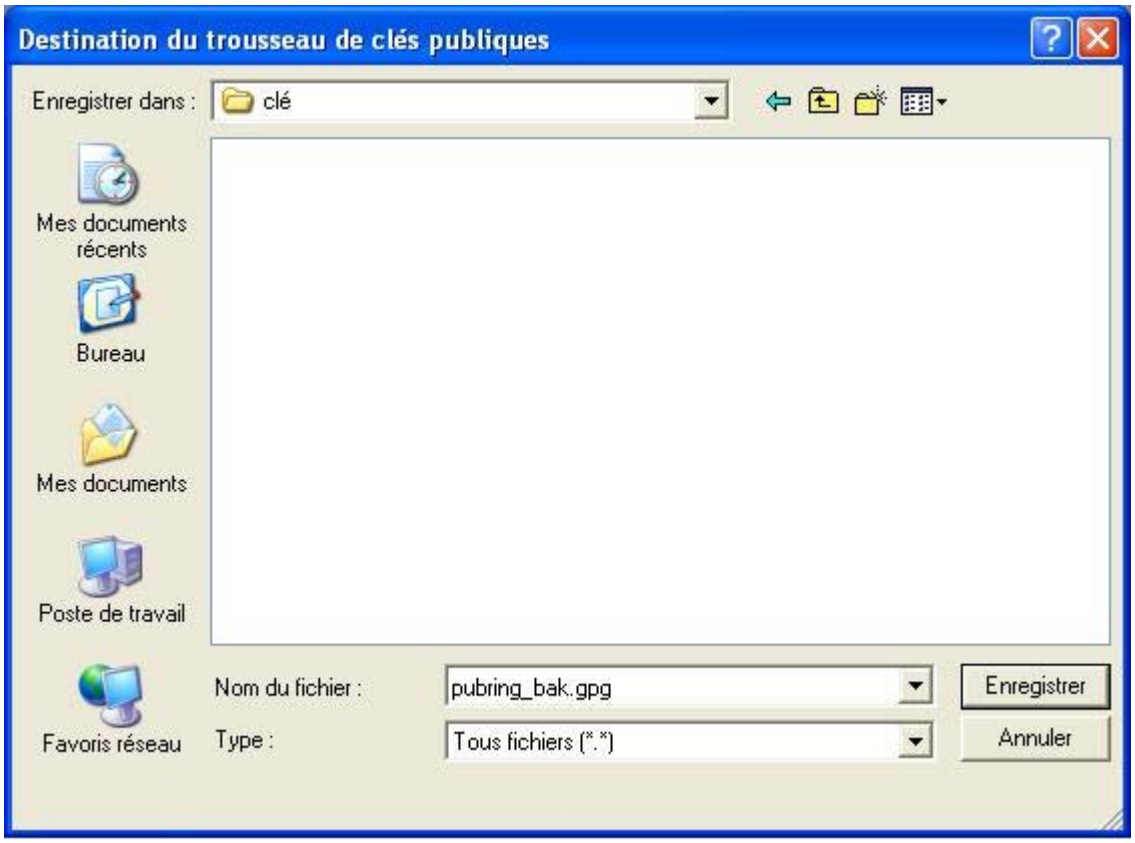
Un écran d'avertissement vous propose alors de réaliser une sauvegarde de vos clés.



Il est indispensable d'effectuer une sauvegarde du bi-clé de chiffrement car sa perte empêchera tout déchiffrement des documents ayant été émis ou reçus. Le support comportant ce bi-clé doit également être conservé dans un emplacement sûr. Ce peut être un espace réservé à cet utilisateur sur un disque réseau sauvegardé (Raid…) ou une disquette dans un tiroir fermé à clé.

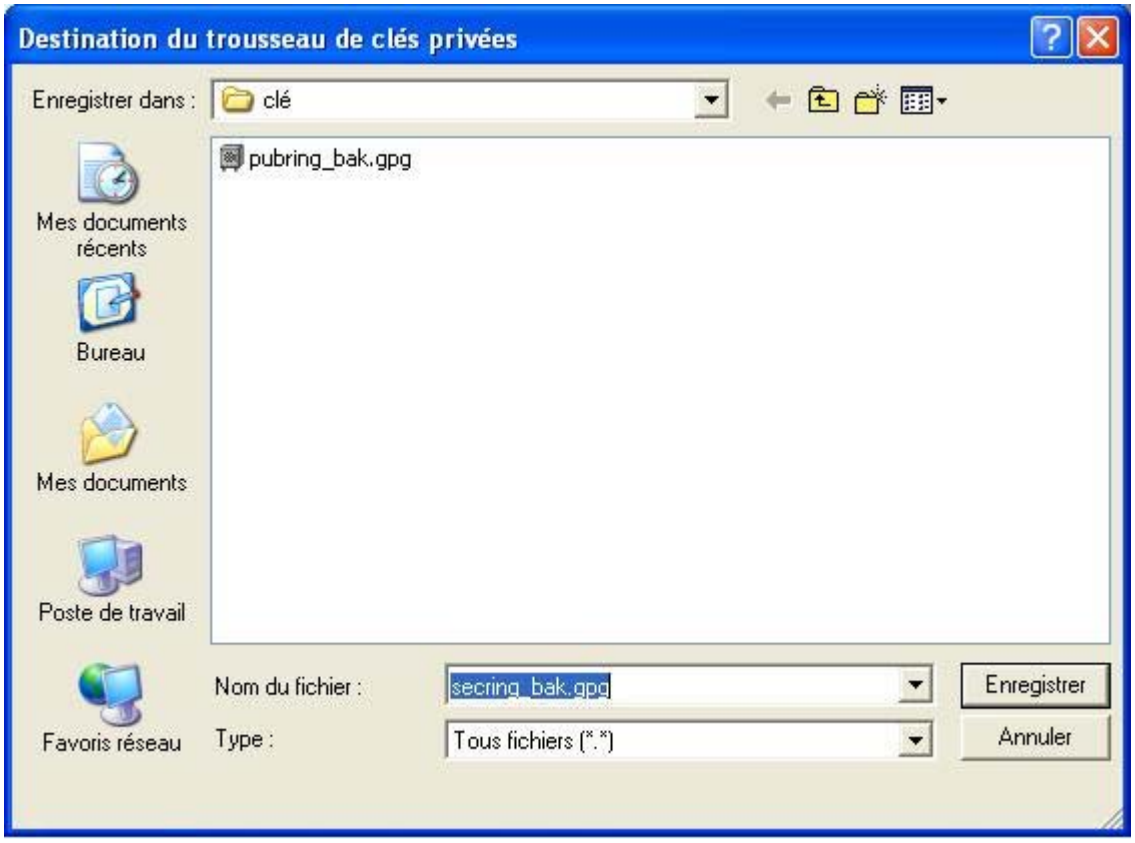


Cliquez sur le bouton « Oui ». Un écran apparaît pour vous permettre de choisir le nom et l'emplacement de sauvegarde de votre clé publique. Choisir de l'enregistrer sur un support amovible (clé USB, disquette…).



Puis cliquez sur le bouton « Enregistrer ».

Un second écran apparaît pour vous permettre de choisir le nom et l'emplacement de sauvegarde de votre clé privée (en fait le bi-clé complet). Choisir de l'enregistrer sur le même support amovible.



Puis cliquez sur le bouton « Enregistrer ».

F – Test de l'installation

Pour contrôler le bon fonctionnement des logiciels installés les opérations suivantes peuvent être conduites et leur résultat contrôlé. La clé publique nécessaire à ce test est fournie par l'installateur.

Démarrage de WinPT

Redémarrez l'ordinateur sous le profil de l'utilisateur. A la fin du démarrage de l'ordinateur WinPT est normalement démarré (mais ne s'affiche pas dans une fenêtre à l'écran), seule son icône doit apparaître dans la barre de tâches en bas à gauche de l'écran (à côté de l'heure).

L'icône du logiciel apparaît sous la forme d'une clé comportant un @ 

Par exemple comme cela : 

Remarque : si l'icône n'est pas visible cliquez sur la flèche,  pour « Afficher les icônes cachées » pour la voir.

Si l'icône n'apparaît toujours pas une anomalie existe. Sinon passez à l'étape suivante.

Import d'une clé publique

Localiser la clef publique test.asc qui a été enregistrée sur le poste, par l'installateur, dans le répertoire dédié GPG\clés de Mes documents. Elle doit y être représentée avec l'icône suivante : 

Faites un Double clic (gauche) sur l'icône de cette clé.

Un écran de WinPT s'ouvre vous indiquant ce qui est importé (1 clef publique).

Validez en cliquant sur le bouton « OK ». Si cette fenêtre n'est pas en français mais en anglais, vous avez sans doute mal procédé à l'installation (pas fait dans le profil utilisateur).

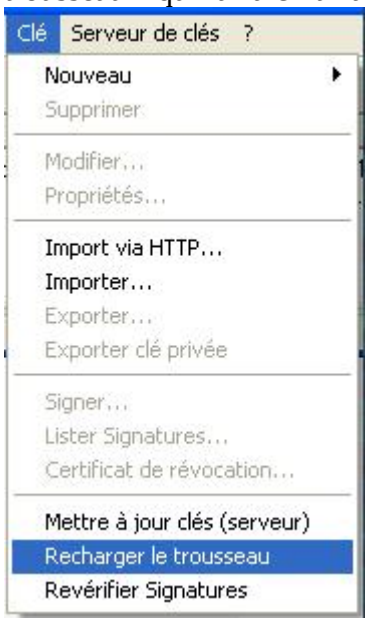
Aller sur l'icône indiquant le logiciel WinPT en fonctionnement située dans la barre de tâche (à proximité de l'horloge).

Faire un clic droit dessus pour ouvrir le menu contextuel de WinPT,

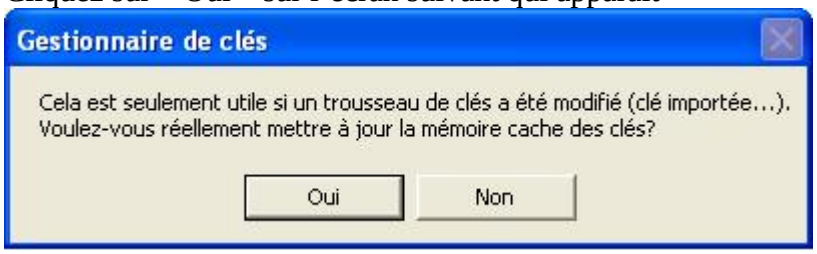
cliquez alors sur la fonction : « Gestionnaire de clés »

L'écran de « Gestionnaire de clés » apparaît alors.

La clé importée n'apparaît pas, mais dans le menu « Clé » choisir la fonction « Recharger le trousseau » qui rafraichit l'affichage des clés.

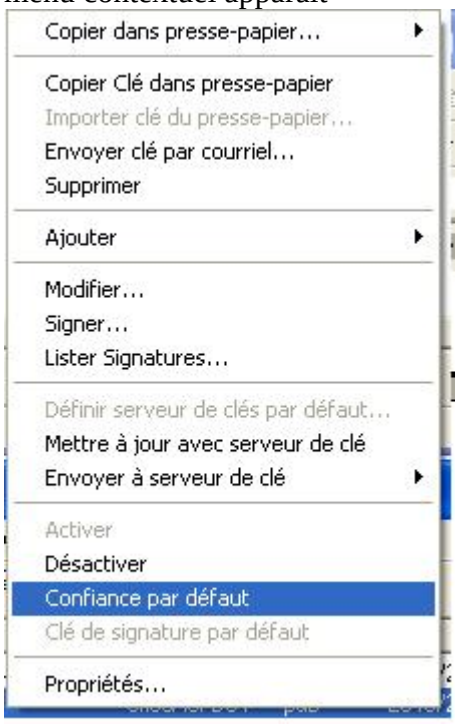


Cliquez sur « Oui » sur l'écran suivant qui apparaît



La nouvelle clé importée doit alors apparaître en bleu comme ci-dessous.

Si la clé n'apparaît toujours pas une anomalie existe.
Sinon faite un Clic Droit sur la ligne de la clef de test, dans le « Gestionnaire de clés », un menu contextuel apparait

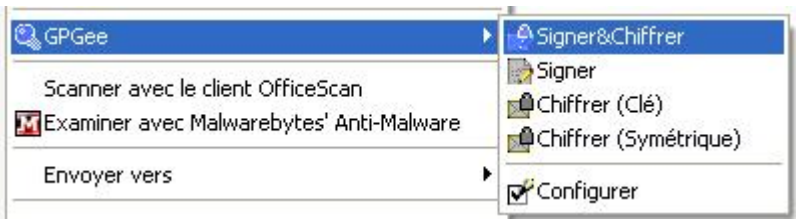


Cliquer sur « Confiance par défaut ».

La clé apparaît alors avec un confiance et une validité « Absolue ». Vous pouvez alors passer à l'étape suivante. Sinon une anomalie existe.

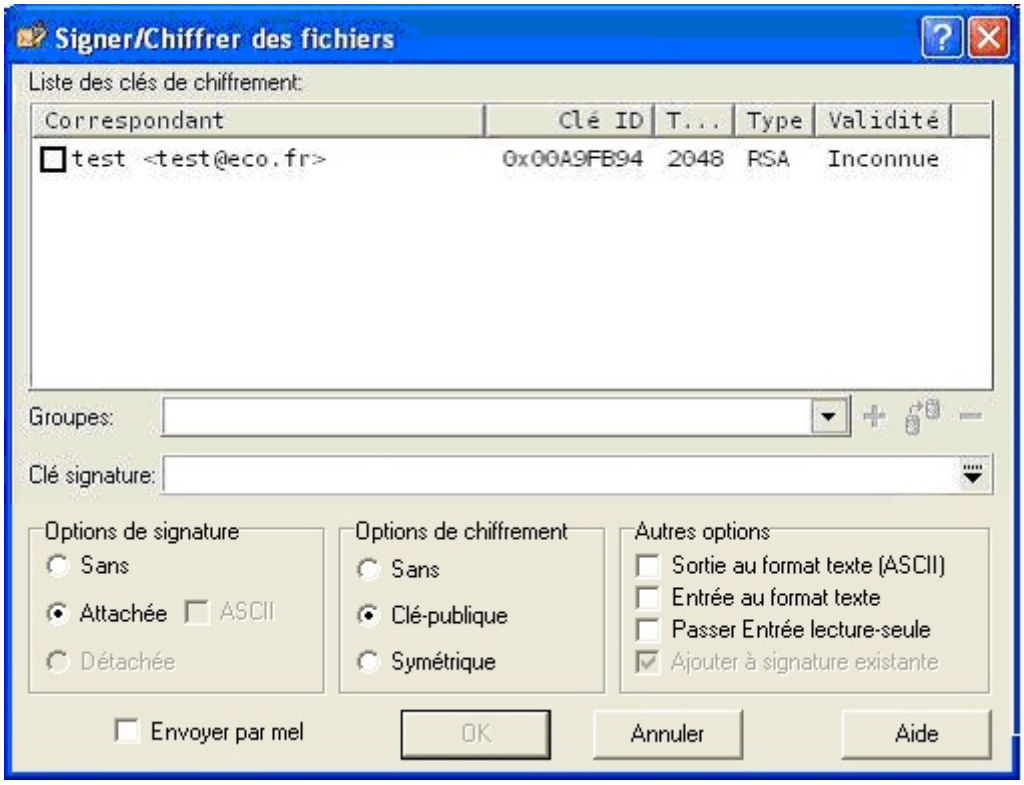
Chiffrer un document avec GPGee

- Pour le test, copiez un document dans le dossier Mes Document\GPG (ici : essai.rtf)
- Dans Mes Document\GPG, faites ensuite un Clic droit sur ce document
- Dans le menu contextuel qui apparaît choisir GPGee, puis « Signer&Chiffrer »

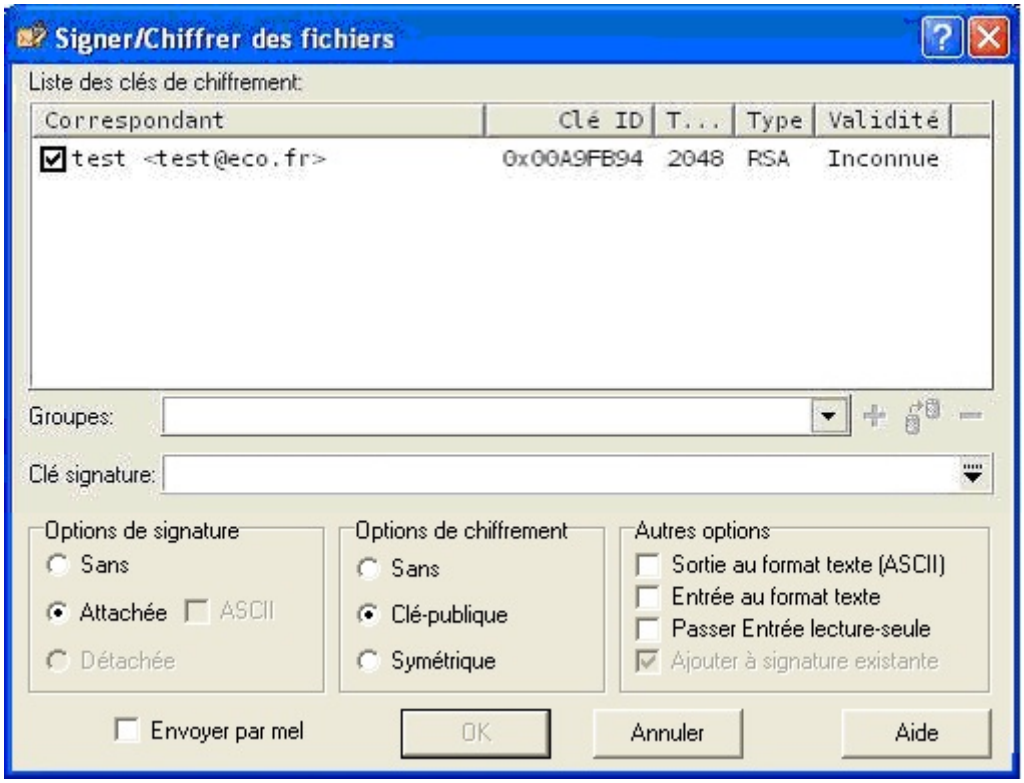


Si la fonction GPGee n'apparaît pas dans le menu contextuel, et si vous n'êtes pas sur OS 64 bits (voir dans ce cas la note spécifique), vous avez peut être mal procédé à l'installation (pas fait dans le profil utilisateur).

- L'écran suivant apparaît alors :



Cochez la clé de test comme destinataire.



Sélectionnez votre clé privée dans la zone « Clé signature » car elle n'apparaît pas par défaut pour la première utilisation.

Ne modifiez aucune des options cochées.

- Vous pouvez cocher la case « Envoyer par mel » (en bas à gauche), ce qui générera automatiquement le courriel d'envoi du fichier chiffré. Si le composant Mapi n'est pas correctement installé et paramétré la création du mel n'aboutira pas, même si le document a été chiffré.
- Puis validez en cliquant sur le bouton « OK » qui est maintenant actif.
- Saisir le mot de passe de votre clef privée sur l'écran suivant qui apparaît

En décochant la case « Cacher saisie », votre mot de passe s'affiche en clair

- Puis valider en cliquant sur OK

Le document chiffré est alors créé à coté du document d'origine. Il porte le nom essai.rtf.gpg, (l'extension « .gpg » a été rajoutée). Il apparaît avec l'icône suivante :

Si essai.rtf.gpg n'apparaît pas, et avec cette icône, il y a une anomalie. Sinon passez à l'étape suivante.

Déchiffrement d'un document avec GPGee

Dans Mes Document\GPG supprimez le document essai.rtf. Faites y ensuite un Clic droit sur essai.rtf.gpg.

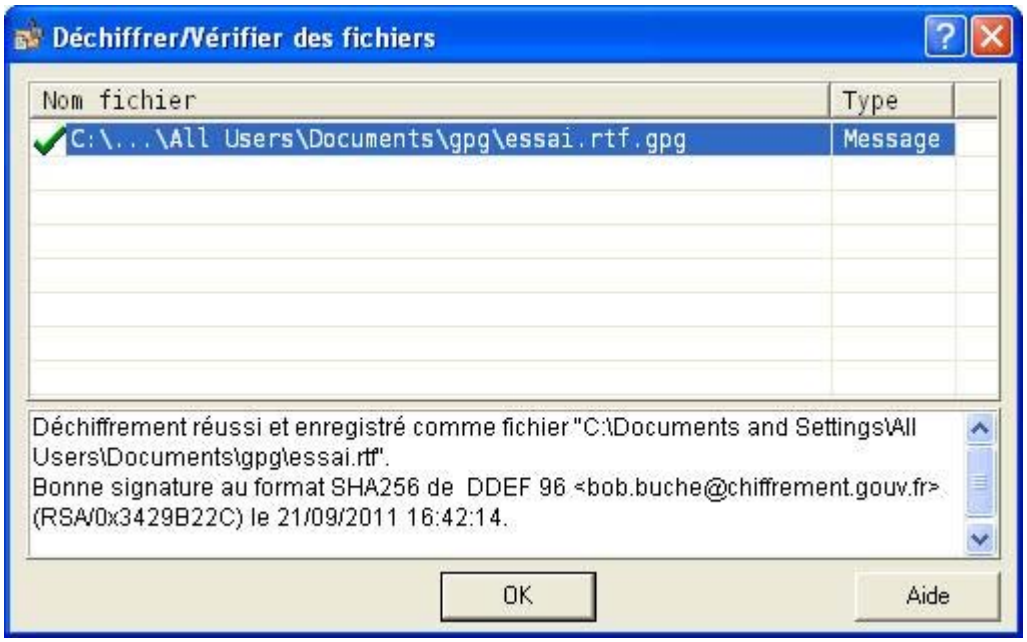
Dans le menu contextuel qui apparaît choisir GPGee, puis « Déchiffrez&Vérifiez »

- Dans la fenêtre qui apparaît, saisir le mot de passe de la clef privée de l'utilisateur dont l'identifiant est affiché

En décochant la case « Cacher saisie », votre mot de passe s'affiche en clair

- Valider en cliquant sur le bouton « OK »

Un écran d'information apparaît alors vous faisant un compte rendu du déchiffrement et de la vérification de la signature.



Cet écran rappelle le nom et l'emplacement du document déchiffré (le même dossier que le document chiffré)

La coche obtenue doit être verte comme sur cet écran. Il doit être mentionné SHA256 pour le format de la signature.

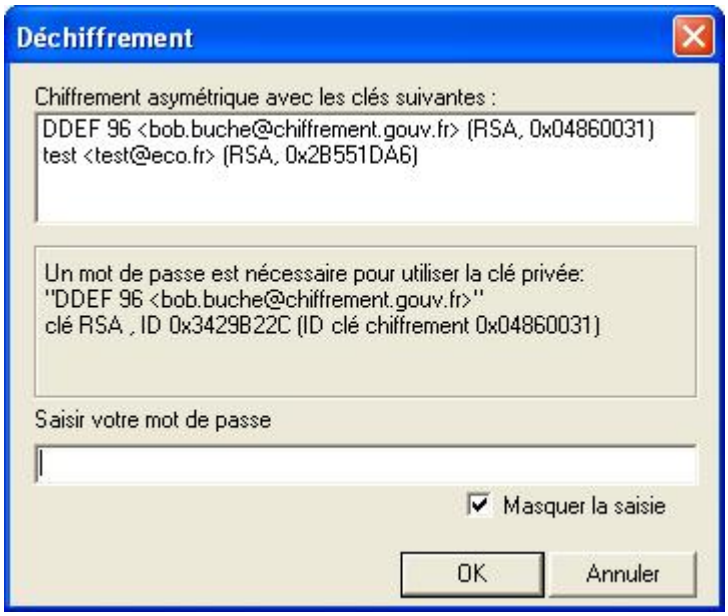
Si vous n'avez pas pu réaliser ces opérations, ou pas obtenu ces informations, il y a une anomalie. Sinon cliquez sur le bouton « OK » et passez à l'étape suivante.

Le document obtenu doit être identique au document original.

Déchiffrement d'un document avec WinPT

Dans Mes Document\GPG supprimez le document essai.rtf. Faites y ensuite un double clic (gauche) sur essai.rtf.gpg.

Sur l'écran qui apparaît saisir le mot de passe de la clef privée de l'utilisateur dont l'identifiant est affiché



En décochant la case « Masquer la saisie », votre mot de passe s'affiche en clair

- Valider en cliquant sur OK

Vous devez normalement obtenir le message suivant qui indique qu'il n'y a pas de problème :

Si l'opération ne s'est pas déroulée comme indiquée il y a une anomalie. Sinon passez à l'étape suivante.

Le document obtenu doit être identique au document original.

Suppression de la clé de test

Ré-ouvrez le « Gestionnaire de clés » si vous l'avez fermé. Supprimez la clé de test en faisant un clic gauche sur la ligne de cette clé pour la sélectionner. Elle passe alors sur fond bleu (vidéo inversée).

Appuyer alors sur la touche « Suppr » de votre clavier. Un écran apparaît vous demandant de confirmer la demande de suppression de la clef

- Confirmer en cliquant sur « Oui ». La clé de test doit avoir maintenu disparu du « Gestionnaire de clés »

Si la clé de test ne disparaît pas une anomalie existe. Sinon vous avez correctement terminé le test.

G – Utilisation

Se référer au mode d'emploi correspondant aux versions WinPT 1.4.3c et d.

Les principaux composants informatiques utiles sont normalement disposés ainsi dans les différents dossiers ("user" désigne le profil de l'utilisateur) :

C:\Program Files\ comporte :

les logiciels (sous dossier GNU).

C:\Users\"user name"\AppData\Roaming\gnupg\ (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\ (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 (secring-bak.gpg pour les clés secrètes et 3 copies tournantes des clés publiques pubring-bak-0 à 2.gpg).

H - Désinstallation du logiciel

Les logiciels GPG, WinPT et GPGee peuvent être désinstallés en suivant les différentes étapes détaillées ci-après. Il faut faire attention car en supprimant ainsi ces logiciels et tous leurs composants l'utilisateur ne sera plus capable de lire des documents chiffrés. Il est préférable que tous aient été déchiffrés auparavant et qu'une copie du bi-clé privé soit réalisée.

Lancer l'installateur (cf. D) en double-cliquant dessus.

Dans l'écran qui s'affiche sélectionner « Supprimer WinPT, GnuPG et GPGee », puis cliquer sur le bouton « Terminer ».

Une fois la suppression terminée redémarrez le PC.

Puis finir de nettoyer le PC, au cas où des éléments n'auraient pas été bien supprimés, en réalisant les opérations suivantes :

-Supprimez les dossiers :
C:\Users\"user name"\AppData\Roaming\gnupg\ (qui comporte encore des documents) ;
C:\Program Files\GNU (qui peut comporter des sous-dossiers GnuPG, WinPT et GPGee) ;

et les autres dossiers que vous avez créés par vous même (normalement « Mes Documents\GPG »).

-Supprimez le contenu du dossier Temporary internet Files, pour les documents que vous auriez essayé de traiter directement dans la messagerie.

-Supprimer le raccourci WinPT du dossier de démarrage (et de la barre de lancement rapide si il y a été ajouté) :

C:\Users\"user name"\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup.

-Puis videz au moins la corbeille, éventuellement réalisez une réécriture des secteurs du disque dur ainsi libérés (pour les effacer physiquement).

-Nettoyer la base de registre (lancer la commande regedit) :

- supprimer les clés software\GNU ; GPGEE ; et WinPT de HKEY$\« user » et de HKEY$\local machine (lorsqu'elles existent).
- supprimer la chaine HKEY$\« user »\Control panel\MingW32\NLS\MODir et la clé HKEY$\« user »\Control panel\MingW32 si elle ne comporte plus rien d'autre.

Fermez les différentes fenêtres et puis redémarrez le PC.

En cas de changement d'affectation du PC ou au dé-commissionnement des volumes de stockage utilisées (disques durs…), si ceux-ci ne sont pas physiquement détruits, de manière à rendre inexploitables les données décryptées ayant pu y figurer, procéder à un reformatage de bas niveau pour supprimer toutes les données qui pourraient encore être extraites.

○○○