Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

Mode d'emploi de l'outil de chiffrement

Logiciel GnuPG version 1.4.19
Logiciel WinPT versions 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	6/10/2009	Création du document
1	12/10/2009	Prise en compte de remarques
2	22/10/2009	Modification suite à vérifications
2.1	7/12/2009	Prise en compte modification des spécifications techniques et des simplifications retenues pour la formation.
2.2	15/01/2010	Complément du mode d'emploi et francisation
2.3	25/03/2010	Corrections
2.4	27/05/2010	Compléments
2.5	7/10/2010	Compléments
2.6	15/11/2010	Modification envoi des clés
2.7	7/10/2011	Prise en compte remarques évaluateurs
2.8	6/01/2014	Changement de versions pour raison de sécurité
2.9	21/05/2014	Correction d'un bug avec GPGee 1.4.3
2.10	5/03/2015	Montée de version (sécurité) et ajout d'un adaptateur 64 bits
2.11	19/03/2015	Changement de version GnuPG pour raison de sécurité

Fax. : 01 53 44 29 27

Avertissement

Chaque personne est responsable de la protection des informations confidentielles dont il a connaissance dans le cadre professionnel (données personnelles...). La divulgation, même involontaire, de ces informations peut être sanctionnée pénalement.

L'internet (messagerie électronique, site web http…) n'assure généralement pas de protection des informations qui y sont échangées. Aussi l'utilisation d'un moyen de protection des informations confidentielles qui pourraient être transmises par ce média est nécessaire.

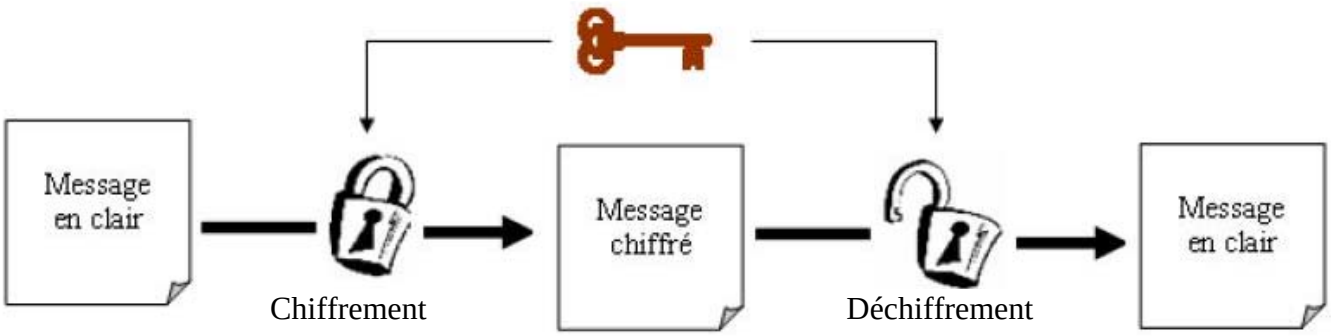
La solution de chiffrement mise à disposition doit être utilisée en respectant ses règles d'utilisation. Les éventuels messages d'alerte doivent être examinés avec attention, et conduire aux actions nécessaires pour entretenir la sécurité mise en place.

Sommaire

A - Présentation des procédés de chiffrement

Le chiffrement à clé secrète

Le mode de chiffrement classique utilise une seule clé de chiffrement (ou mot de passe), dite clé secrète, qui permet de chiffrer et déchiffrer les documents. Ce procédé est également dit symétrique. C'est en quelque sorte une clé unique qui permet de fermer comme d'ouvrir le coffre dans lequel vous avez placé un document.



Chiffrement à clé secrète : la même clé est utilisée pour chiffrer et déchiffrer

Ce procédé de chiffrement peut générer des difficultés lorsque les documents ainsi chiffrés doivent être échangés avec de multiples destinataires. En effet :

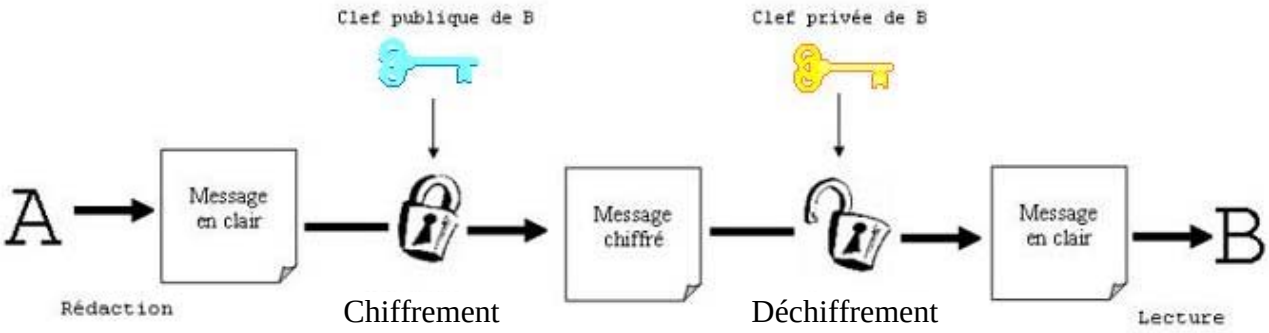
- soit la clé de chiffrement est modifiée pour chaque document, ce qui complique la gestion et la communication de ces clés ;
- soit la clé de chiffrement n'est pas modifiée et sa diffusion large peut conduire des personnes qui n'auraient pas du être destinataire du document à en prendre connaissance. Par ailleurs le déchiffrement du document ne garantit pas qu'il provient bien de la bonne personne.

Le chiffrement asymétrique

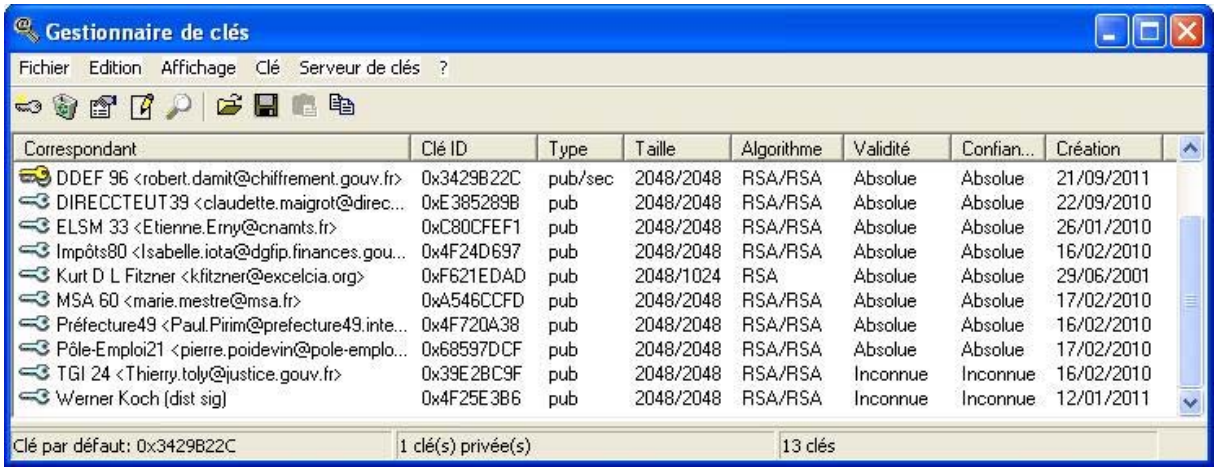
Pour résoudre ces difficultés un procédé particulier de chiffrement a été mis au point. Ce procédé utilise un couple de clés (bi-clé). Lorsqu'une de ces deux clés a servi à chiffrer un document, seule l'autre clé permet de le déchiffrer.

Chaque utilisateur possède un bi-clé. Une de ces clés reste personnelle (la clé privée figurée en jaune) et l'autre clé (la clé publique figurée en bleu), est diffusée à tous ses contacts. Les documents chiffrés avec la clé publique de B ne peuvent être déchiffrés que par lui.

Le coffre fort qui est fermé par une clé, ne peut être ouvert que par l'autre clé. Il est crucial de ne jamais divulguer sa clé privée car c'est elle qui est l'élément fondamental de la sécurité.



Les utilisateurs se trouvent ainsi en possession d'un trousseau de clés, avec leur clé privée et leur clé publique (leur bi-clé), et les clés publiques de tous leurs interlocuteurs.

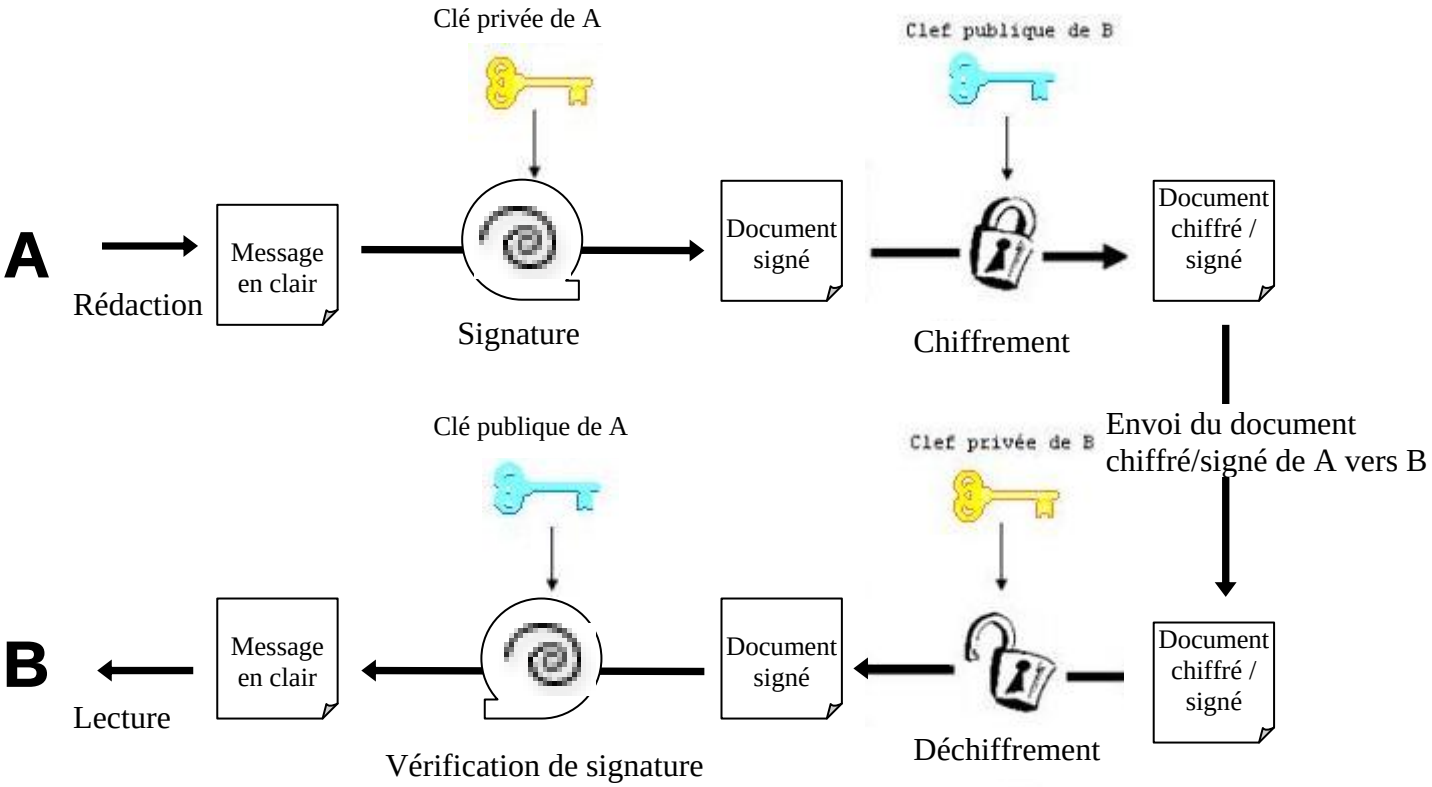


Sur cette écran de WinPT vous voyez les clés publiques de nombreuses personnes (celles en bleu) et un bi-clé avec un clé jaune (la clé privée) sur une clé publique, pour « robert Damit ».

Utilisation du procédé asymétrique : signer & chiffrer

Une clé publique (par exemple celle de B) étant largement diffusée, le risque pourrait exister que quelqu'un se fasse passer pour A en envoyant un document chiffré à B. Pour éviter ce risque, le bi-clé de A est également utilisé pour authentifier le document (on dit le signer), mais en inversant les clés utilisées par rapport au chiffrement.

L'utilisation normale de ce procédé de signature&chiffrement est alors le suivant :



Pour un échange de document chiffré de A vers B, il va en fait y avoir 2 opérations de réalisées. A va signer le document avec sa clé privée et le chiffrer avec la clé publique de B. Cette opération est désignée sous le nom de signer&chiffrer. Et B va déchiffrer le document

avec sa clé privée (ce qu'il est le seul à pouvoir faire) et la clé publique de A, ce qui l'assure que le document provient bien de A. On parlera là seulement de déchiffrement malgré tout.

Ce sont les logiciels qui réalisent ces enchainements de tâches. L'utilisateur doit seulement leur donner les bonnes instructions.

Durant ce processus chaque partenaire n'a besoin que des clés de son trousseau : sa clé privée et la clé publique de l'autre partenaire.

Ce procédé peut même être utilisé pour créer un document chiffré pour plusieurs destinataires simultanés, en chiffrant avec plusieurs clés publiques en même temps (cf. annexe). C'est ce procédé de signature&chiffrement qui doit être utilisé.

Synthèse sur l'usage des différentes clés

ACTION	Opérations	Remarque	Exemples d'utilisation
Alice utilise sa clé publique	Chiffrement	Seule Alice peut déchiffrer avec sa clé privée	Protection de ses données personnelles : chiffrement du contenu d'un répertoire ou d'un disque
Alice utilise sa clé privée	Signature	Toute les personnes ayant la clé publique d'Alice peuvent vérifier cette signature	Signature de mail ou de documents
Alice utilise la clé publique de Bob	Chiffrement	Seul Bob pourra déchiffrer avec sa clé privée	Chiffrement de données à destination d'une personne précise
Alice utilise la clé privée de Bob	Impossible	La clé privée de Bob ne doit pas être diffusée. Bob doit protéger sa clé et la renouveler s'il pense qu'une personne a pu y avoir accès	
Alice utilise la clé publique de Bob et sa clé privée (clé d'Alice)	Signature et Chiffrement	Seul Bob pourra déchiffrer avec sa clé privée. Bob aura l'assurance, grâce à la signature d'Alice, que le chiffrement a bien été réalisé par Alice	Chiffrement de données à destination d'une personne précise. Avec une garantie sur l'identité de l'auteur du chiffrement
Alice utilise sa clé publique et la clé publique de Bob	Chiffrement	Seuls Alice et Bob peuvent déchiffrer les données avec leur clé privée	A l'issue du chiffrement Alice est en mesure de vérifier ce qu'elle a chiffré
Alice utilise sa clé publique et sa clé privée ainsi que la clé publique de Bob	Signature et Chiffrement	Seuls Alice et Bob peuvent déchiffrer les données avec leur clé privée et sauront grâce à la signature d'Alice, que le chiffrement a bien été réalisé par Alice	A l'issue du chiffrement Alice est en mesure de vérifier ce qu'elle a chiffré. Bob a une garantie sur l'auteur du chiffrement

B - Installation du logiciel

Pour l'installation, comme pour la mise à jour ou la désinstallation des logiciels, il convient de se référer à la dernière version de l'instruction technique d'exploitation, qui permet de le faire dans des conditions de sécurité, et en particulier d'installer les bonnes versions avec une interface en français.

La création de vos clés de chiffrements personnelles devrait être réalisée lors de l'installation des logiciels. Si vous ne réalisez pas vous même l'installation il convient donc que vous soyez présent pour pouvoir définir le mot de passe de vos clés.

Trois logiciels différents vont, en fait, être installés pour les PC sous Windows 32 bits (l'utilisation sous Linux ou Mac n'est pas traitée ici). Le logiciel GnuPG chiffre et déchiffre mais est d'utilisation ardue et ne sera pas utilisé en direct. Les deux autres logiciels servent d'interface pour utiliser facilement GnuPG.

GPGee qui permet de réaliser les opérations de signature&chiffrement/déchiffrement directement en cliquant avec un clic droit sur les documents.

WinPT qui permet de gérer les clés de chiffrement (et éventuellement de signer&chiffrer et déchiffrer sans utiliser GPGee).

La seule différence entre les versions 1.4.3c et 1.4.3d de WinPT concerne l'agrandissement d'un écran et le changement de case cochée par défaut pour la signature des clés.

Pour l'utilisation sous Windows 64 bits, un adaptateur GPGee64, fait fonctionner GPGee dans les dossiers de l'explorateur windows (mais pas sur le bureau).

Disposition :

Une fois le logiciel installé, les principaux éléments utiles sont normalement disposés ainsi dans les différents dossiers (emplacements Windows 7 32 bits):

Dans C:\Program Files\ :

les logiciels (sous-dossier GNU).

Dans C:\Users\"user name"\AppData\Roaming\gnupg :

le fichier de configuration de GPG (gpg.conf) ;

le trousseau de clés avec leur niveau de confiance (pubring.gpg, secring.gpg et trustdb.gpg).

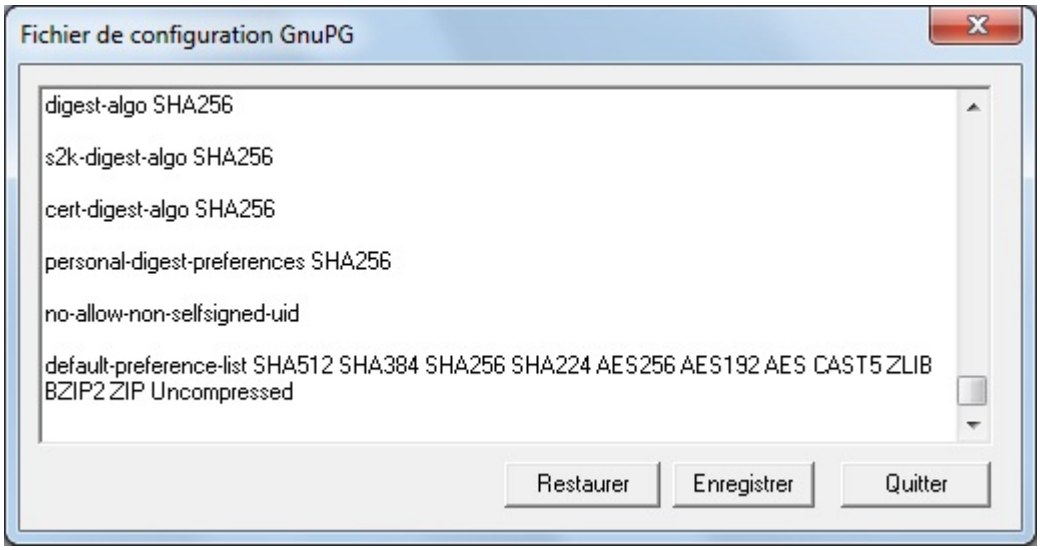
Dans C:\ Users\"user name"\Mes documents\GPG\Clés\ :

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).

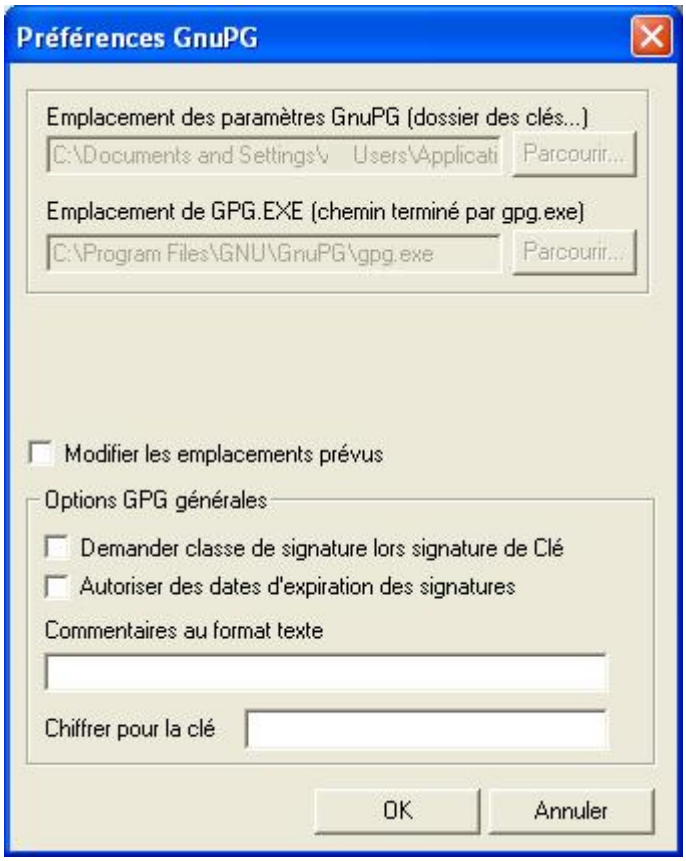
Paramètres :

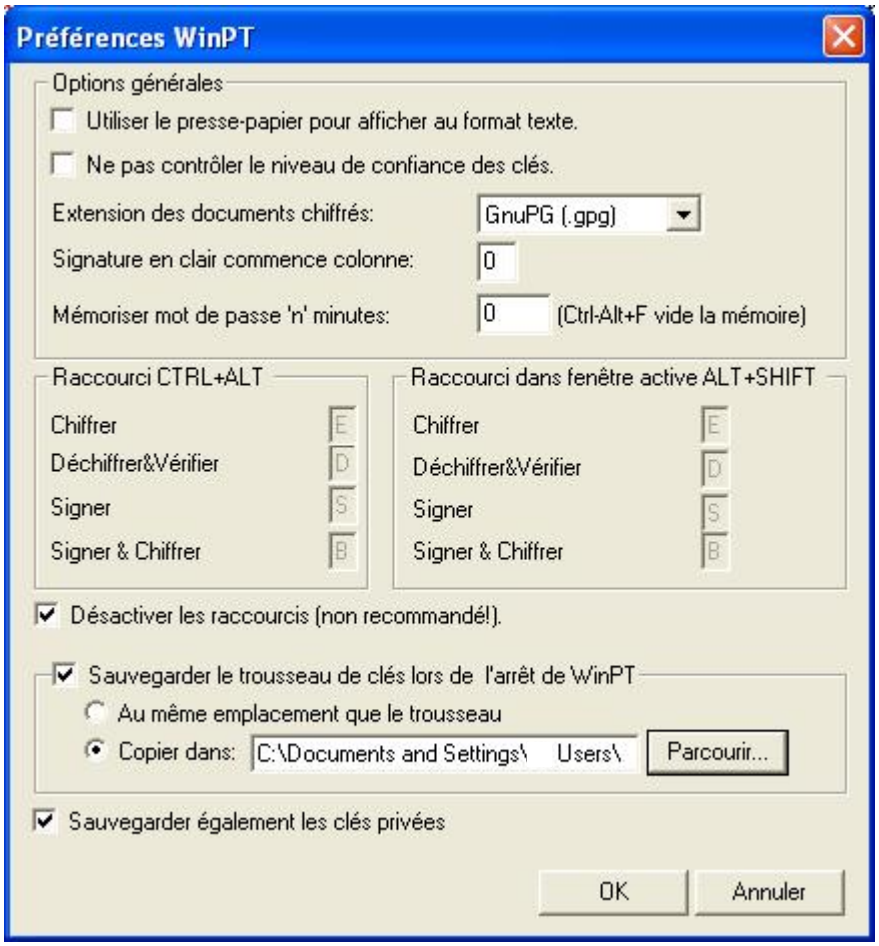
Les différents écrans de paramétrage doivent avoir les aspects suivants (et ne pas être modifiés) :

Dans WinPT (y accéder par le Gestionnaire de clés, le menu Edition, puis Préférences) :

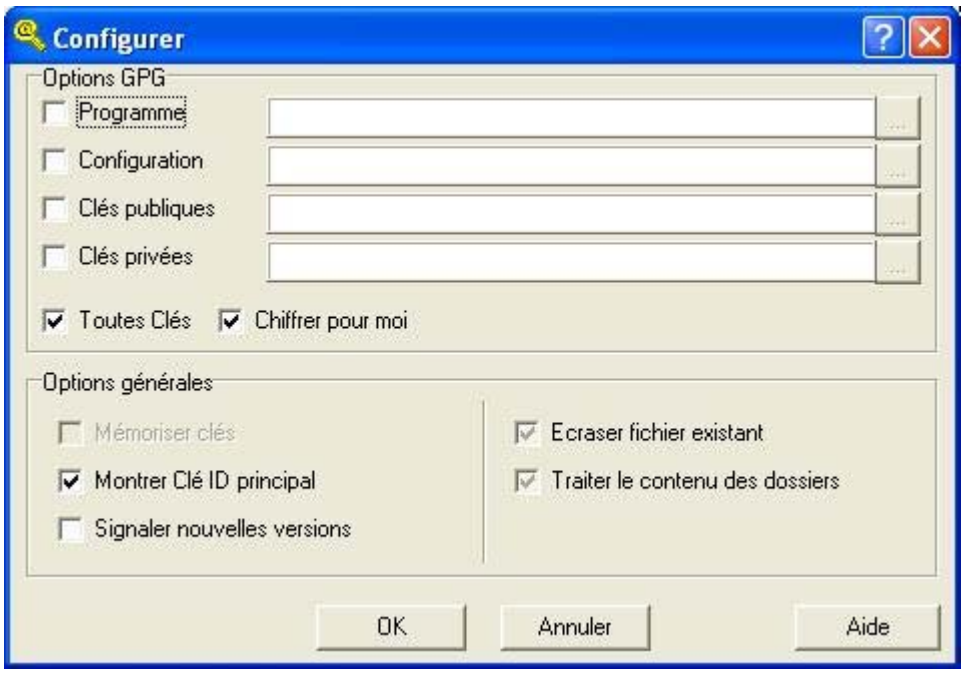


Les dernières lignes indiquées devront bien être celles apparaissant ci-dessus.





Dans GPGee (après un clic-droit, dans le menu contextuel apparu, GPGee-> Configurer) :



C – Principes de fonctionnement des échanges sécurisés

Cadre légal

L'utilisation de logiciels de chiffrement est libre sur le territoire français. Cependant, l'utilisation de ce dispositif informatique doit respecter les dispositions de la loi informatique et liberté (78-17).

Il convient notamment de respecter l'interdiction de traiter des données visées à l'article 8 de la loi 78-17 (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale, données de santé ou vie sexuelle).

Ce dispositif peut être utilisé comme solution de chiffrement pour des échanges faisant l'objet de démarches auprès de la CNIL (fichiers chiffrés sur CD-Rom, télétransmission de fichiers chiffrés…).

Il peut aussi servir à protéger des documents devant rester confidentiels sans qu'ils comportent de données personnelles.

La mise en place de ce dispositif et son utilisation pour le chiffrement de documents échangés par la messagerie professionnelle peut s'inscrire dans le cadre d'une déclaration de conformité à la norme simplifiée 46 (notamment pour l'annuaire composé par le trousseau de clés et la protection des données échangée).

Les échanges d'informations ainsi réalisés doivent cependant également bien être autorisés par le cadre juridique en vigueur (droit de communication, levée du secret professionnel…) lorsque ces échanges ont lieu entre des services administratifs différents.

Organisation

Les outils proposés sont prévus pour une utilisation lors d'échanges entre un faible nombre de personnes qui sont déjà en contact (2 personnes ensemble ou un groupe de travail, par exemple).

Dans le cas d'un groupe, une personne pourra être chargée de diffuser un trousseau des clés publiques à jour (pubring.gpg), en une fois, à tous les participants, ainsi qu'une liste des éléments d'identification des clés (mais celle-ci ne doit pas l'être en clair par mel).

Equipement informatique

Chaque utilisateur aura les logiciels GnuPG, GPGee et WinPT installés sur son PC professionnel. Ils ne doivent pas être installés sur des PC portables sans mise en place d'une protection des disques durs (chiffrement), ni sur des équipements de connexion à distance aux messageries (comme des téléphones portables BlackBerry), ni dans des environnements non sécurisés (domicile des agents…) pour assurer la protection des documents échangés, une fois déchiffrés.

Les PC utilisés sont protégés par un accès des utilisateurs avec Identifiant et Mot de passe et ils doivent également avoir un écran de veille activé avec une reprise protégée par mot de passe.

Il est nécessaire que les formats .asc et .gpg soient autorisés par les pare-feux pour les pièces jointes des courriels.

Au dé-commissionnement des volumes de stockage utilisées (disques durs…) ceux-ci feront l'objet d'un reformatage de bas niveau pour supprimer toutes les données ou ils seront physiquement détruits, de manière à rendre inexploitables les données décryptées ayant pu y figurer.

Gestion des clés

Le bi-clé personnel (clés privée et publique) de chaque utilisateur est produit avec le logiciel WinPT. Une sauvegarde de ce bi-clé sera conservée sur un support externe placé à un emplacement protégé, accessible au seul utilisateur. Les clés qui sont de longueur 2048 bits peuvent être utilisées jusqu'en 2020.

L'utilisation de la clé privée pour décoder les documents chiffrés avec votre clé publique, ou pour signer les documents que vous signez & chiffrez, est protégée par un mot de passe de plus de 8 caractères (comportant des chiffres et des lettres ou d'autres caractères non alphabétiques). Ce mot de passe doit rester secret et, s'il est noté sur un document, celui-ci doit être conservé dans un endroit sûr (tiroir fermé à clé…), différent de celui où se trouve la sauvegarde des clés. La perte du bi-clé ou du mot de passe rendent indéchiffrables les éléments encore chiffrés reçus. Un bi-clé sera changé en cas de perte, de vol, de risque de divulgation...

Il ne faut pas transmettre par messagerie électronique les mots de passe, bi-clés (clés privées) et documents déchiffrés.

Chaque utilisateur transmet par mel, en clair, sa clé publique (.asc) à ses correspondants, ou la remet en face à face lors de réunions. Lorsque sa clé n'est pas remise en face à face, il communiquera les éléments d'identification de sa clé par un autre moyen que le mel (téléphone, en face à face…) pour que ses correspondants puissent s'assurer être en possession de la bonne clé.

Dans le cas d'un groupe, une personne pourra être chargée de diffuser le trousseau des clés publiques à jour (pubring.gpg), à chaque modification, à tous les participants, ainsi que les clés à supprimer et une liste des éléments d'identification des clés (mais celle-ci ne doit pas l'être en clair par mel).

A chaque fois, pour correspondre de manière sécurisée avec un correspondant, il faut sa clé publique, et qu'il dispose aussi de la votre. Lors de l'import d'une clé publique il faut contrôler qu'elle est bien la bonne (avec les éléments fournis par le correspondant ou sur la liste) et la valider en attribuant un niveau de confiance à la clé (Absolue).

Les clés publiques des anciens correspondants (ou celles remplacées) sont supprimées au plus tôt (dans WinPT) de son trousseau de clés par chaque utilisateur, et dans un délai maximum de 6 mois (tous les documents reçus de cette personne doivent avoir été déchiffrés entre-temps).

Echanges d'informations

Dans le cas d'un échange par mel, la demande ou les informations à transmettre sont reprises sur un document informatique (.doc, .rtf, .txt, pdf, jpg…) qui doit pouvoir être lu par le destinataire. L'intitulé du document informatique ne doit pas comporter d'informations nominatives (car il n'est pas chiffré). Ce document est signé et chiffré avec le logiciel GPGee en définissant le(s) destinataire(s). La version chiffrée du document (.gpg), est ensuite transmise, aux destinataires, en pièce jointe d'un message électronique dans lequel (ni en objet, ni dans le corps du message) aucune information à protéger ne figurera en clair.

Chaque destinataire enregistre le document chiffré reçu sur son PC (dans Mes Documents/GPG) et le déchiffre avec le logiciel GPGee en utilisant son mot de passe. Le document déchiffré est imprimé (ou basculé dans une gestion électronique de documents si cela est prévu) et reprend le circuit normal d'un courrier papier. Le document informatique est alors détruit.

Les utilisateurs ne doivent pas créer un fichier (papier ou informatique) des informations échangées. Il n'est, en particulier, pas tenu un fichier papier (classeur…) comportant tous ces échanges (fichier qui pourrait nécessiter une déclaration spécifique à la CNIL).

Les messages de transmission, les documents chiffrés et déchiffrés doivent être détruits au plus tôt après leur réception et leur traitement. Tous les de 6 mois l'utilisateur doit vérifier qu'il ne reste pas des éléments oubliés, dans sa messagerie, dans MesDocuments\gpg, et même dans C:\Documents and Settings\ « user » \Local Settings\Temp\gpg et supprimer ceux retrouvés.

La corbeille doit également être vidée après suppression des documents (sinon ceux-ci restent présents dans la corbeille).

Conduite à tenir en cas d'anomalie

Lorsque la clé publique importée apparaît ne pas correspondre à celle prévue, que le document chiffré n'est pas déchiffrable ou n'est pas signé avec une clé valide, l'utilisateur doit gérer cette alerte. Il doit vérifier que son trousseau de clés est à jour et ses logiciels correctement paramétrés, puis contacter l'émetteur par téléphone pour identifier une éventuelle cause expliquant cette situation. Si la cause de l'anomalie apparaît être liée aux clés ou à la mise à jour de la liste, une nouvelle diffusion de clé publique ou de la liste sera réalisée si nécessaire.

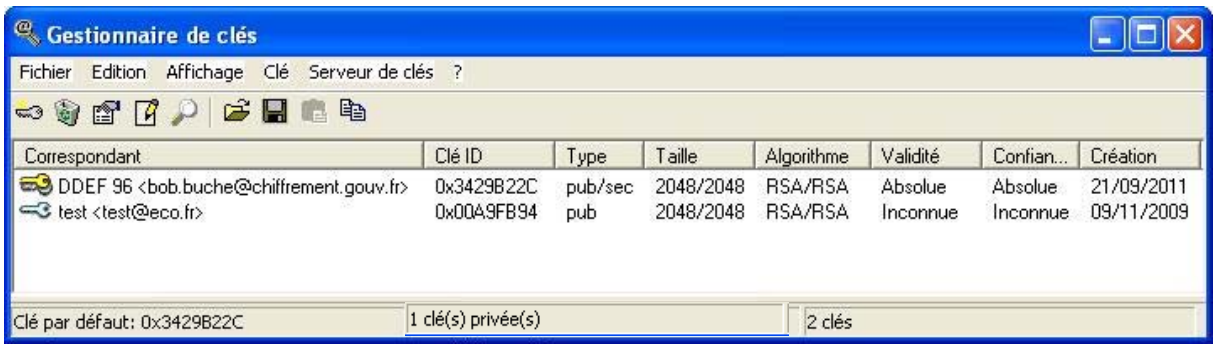
En l'absence de cause satisfaisante trouvée à l'anomalie, une tentative de malversation doit être envisagée et une réponse appropriée apportée par l'organisme de l'utilisateur : information de vos correspondants, mise en quarantaine des documents concernés (chiffrés et déchiffrés), information des responsables de sécurité des systèmes d'information .

La suite de ce mode d'emploi présente l'usage dans un environnement Windows XP

D – Première Utilisation de WinPT

Votre bi-clé personnel a normalement été créé lors de l'installation du logiciel. Si ce n'est pas le cas ou si vous n'avez notamment pas connaissance du mot de passe lié à votre bi-clé, re-contacter la personne qui s'est chargée de l'installation.

WinPT utilise un code visuel, votre bi-clé comporte 2 clés l'une sur l'autre, la première, jaune, représente votre clé privée et le seconde en dessous en bleu est votre clé publique. Vous verrez une seule clé bleue pour les clés publiques que vous importerez de vos correspondants. Le type de clé est aussi indiqué dans la colonne « Type » (pub : publique ou pub/sec : bi-clé)



D - 1. Démarrer WinPT

Normalement WinPT démarre automatiquement. Dans ce cas son icône figure dans la barre des tâches (zone en bas à droite de l'écran comportant l'heure).

L'îcone de WinPT  , représente une clé.

Si l'icône n'est pas visible cliquez sur la flèche,  pour afficher les icônes cachées, et vérifier qu'elle n'est pas cachée.

Si WinPT n'a pas démarré ou que vous l'avez arrêté, cliquez sur le raccourci WinPT situé soit :

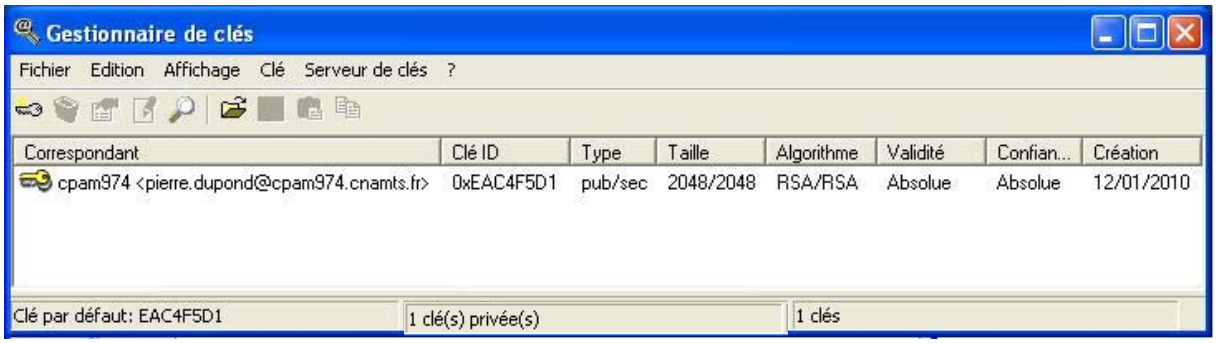
- dans la barre de lancement rapide  (en bas et à gauche de l'écran, à côté de « démarrer »).
- ou sur le bureau 

.

Une fois WinPT démarré il n'affiche pas de fenêtre à l'écran. Vous pouvez uniquement vous en rendre compte par la présence de son icône dans la barre des tâches (cf. ci-dessus).

En cliquant sur cette icône le menu de WinPT apparaît.

Cliquez sur « Gestionnaire de clés » (clic gauche). L'écran du « Gestionnaire de clés » est maintenant ouvert. Il comporte au début une seule clé, la votre (votre bi-clé).



D – 2. Transmission à vos partenaires de votre clé publique

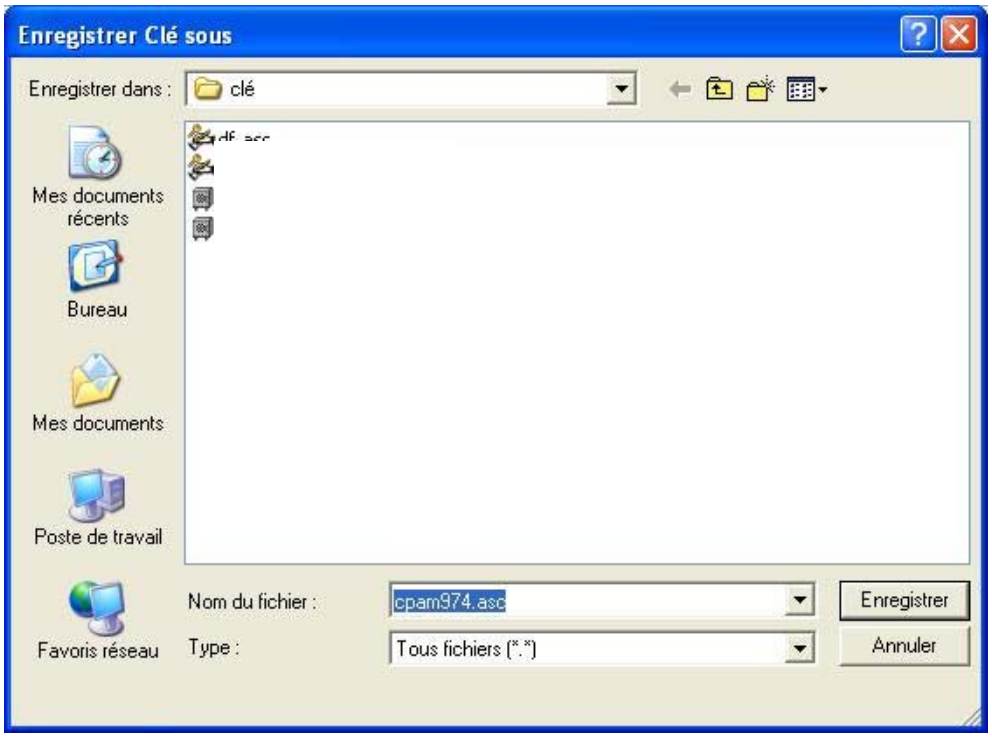
Pour transmettre votre clé publique plusieurs méthodes sont possibles. Celle qui vous est recommandée, car elle devrait toujours bien fonctionner, est indiquée ci-après.

Les éléments d'identification de votre clé (Clé ID…) doivent être également transmis, mais pas seulement par mel (lors d'une réunion ou par téléphone), à vos correspondants.

Le « Gestionnaire de clés » étant ouvert, sélectionnez votre bi-clé en faisant un clic gauche dessus (la ligne apparaît alors sur fond bleu).

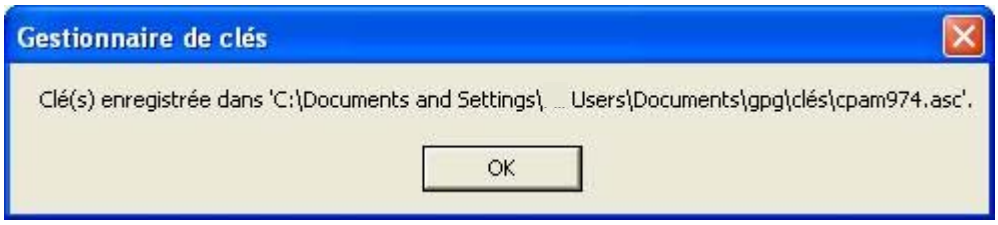
Puis cliquez sur le bouton "Exporter clé publique", qui représente une disquette, dans la barre des icônes au dessus du trousseau

Un écran apparaît pour vous permettre de choisir le nom et l'emplacement d'enregistrement de votre clé publique.



Choisir l'emplacement (« Mes Documents/GPG/Clés »), normalement vous n'avez pas besoin de modifier le nom du fichier (gardez toujours l'extension .asc), puis cliquez sur le bouton « Enregistrer ».

Un écran vous averti du bon déroulement de l'opération.



Cliquez sur le bouton « OK ».

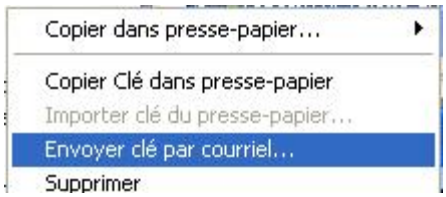
Vous pouvez maintenant copier cette clé publique sur un support amovible (clé USB, disquette…) qui sera donné ou l'envoyer par mel à vos correspondants en l'attachant comme pièce jointe (le fichier .asc), depuis l'emplacement où vous l'avez enregistrée.

Vous la reconnaitrez avec son nom et son icône qui doit être la suivante. 

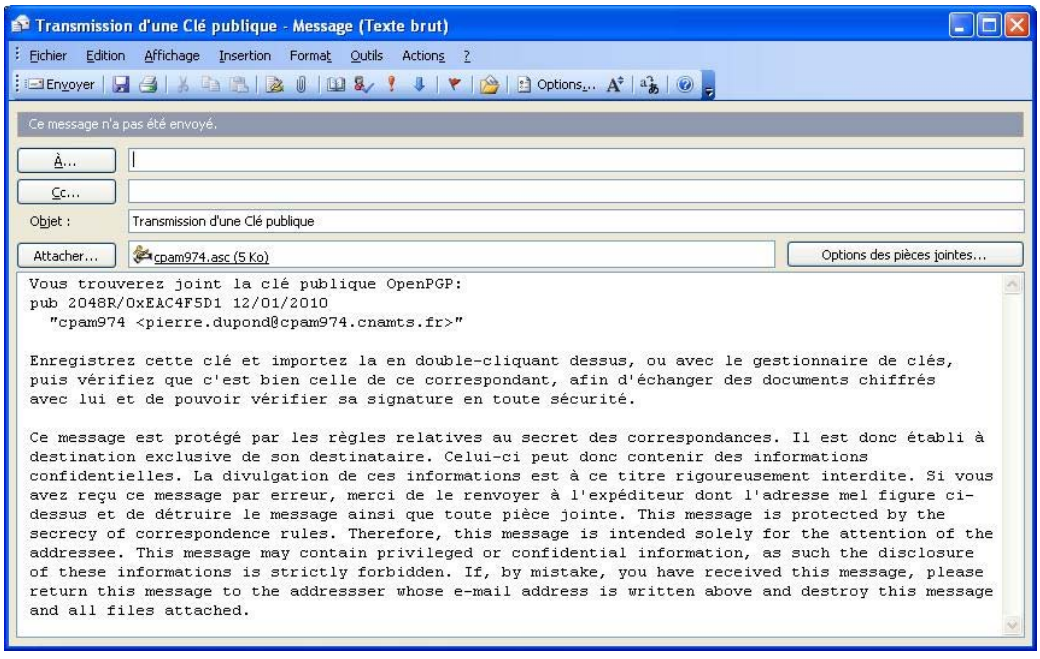
Méthode alternative d'envoi de la clé par mel directement depuis WinPT

Parmi les autres solutions possibles, celle-ci paraît la plus simple, mais elle provoque parfois des difficultés (notamment si mapi n'est pas activé sur votre poste, transformation dans le mel reçu).

Votre messagerie étant ouverte et aucun message en attente d'envoi, dans le « Gestionnaire de clés » de WinPT, faire un clic droit sur votre bi-clé et dans le menu contextuel qui apparaît sélectionner la commande : « Envoyer clé par courriel »



Vous devriez alors voir apparaître une fenêtre avec un mel auquel votre clé publique est attachée (.asc).



Il suffit d'indiquez les différents destinataires et de l'envoyer comme un message normal.

D – 3. Import des clés publiques des correspondants

Vous allez recevoir (sur un support ou en pièce jointe de mel) les clés publiques des différents correspondants avec lesquels vous pourrez être amenés à échanger (fichiers .asc). Enregistrez les clés publiques (fichiers .asc) dans le répertoire « Mes Documents/GPG/Clés ». Les clés sont normalement identifiées dans Windows par l'icône suivante : 

Vous allez d'abord importer la clé puis ensuite devoir vérifier qu'elle est bien celle du correspondant indiqué.

Importer une clé

Pour importer une clé publique au moins deux méthodes sont possibles (décrites en **a)** et **b)**). :

a) En cliquant sur la clé

Double-cliquez sur le fichier .asc de la clé que vous souhaitez importer. L'écran d'importation s'ouvre alors automatiquement en vous indiquant ce que vous êtes en train d'importer (ici 1 clé publique) :

Cliquez sur le bouton « OK ». La clé est alors importée dans votre trousseau de clés.

Vous pouvez répéter cette opération pour chacune des clés à importer, avant de passer à l'étape suivante.

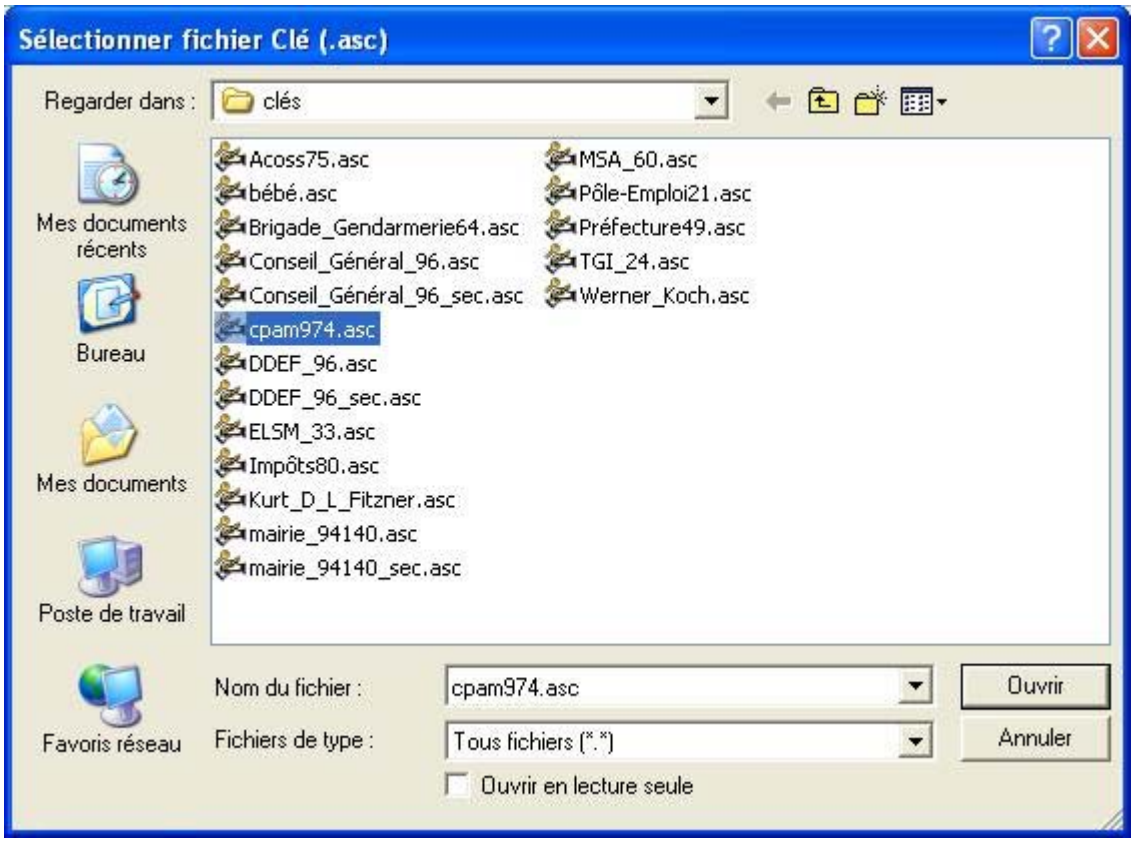
Ensuite, après avoir démarré WinPT, si il ne l'était pas déjà, ouvrez l'écran du « Gestionnaire de clés » et passez à l'étape « Vérifier la clé ».

b) Depuis le « Gestionnaire de clés »

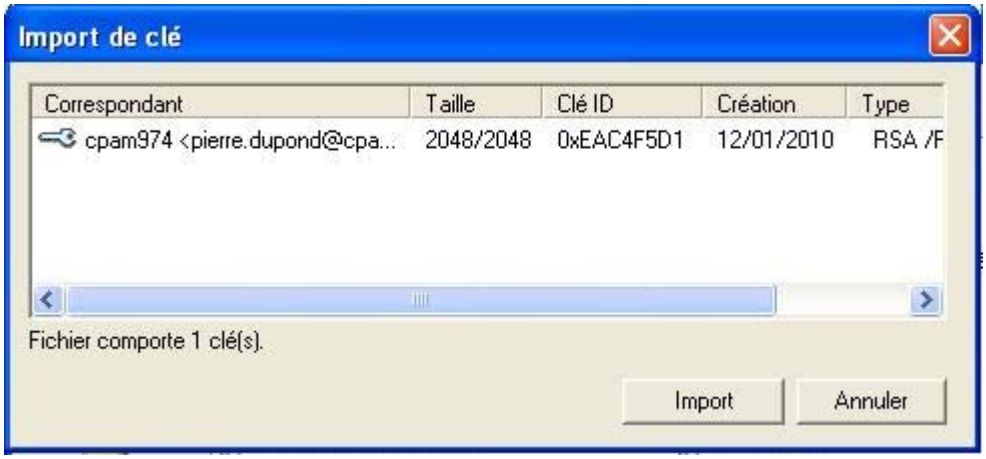
Ouvrez le « Gestionnaire de clés » de WinPT (après avoir lancé WinPT si il n'était pas déjà démarré).

Puis cliquez sur le bouton "Importer clé dans trousseau", qui représente un « dossier qui s'ouvre » dans la barre des icônes.

Un écran apparaît pour vous permettre de choisir les clés publiques à importer (et leur emplacement).



Une fois la clé publique sélectionnée cliquez sur le bouton « Ouvrir ». Une nouvelle fenêtre s'ouvre et vous détaille le contenu que vous allez importer (N.B. vous pouvez dans ce cas commencer la vérification de la clé à ce stade et décider d'annuler l'import si la clé n'était pas bonne. Il convient alors quand même, pour les clés importées, de réaliser l'opération de validation de clé prévues à la fin de l'étape de vérification).



Cliquez sur le bouton « Import ». Une nouvelle fenêtre s'ouvre.

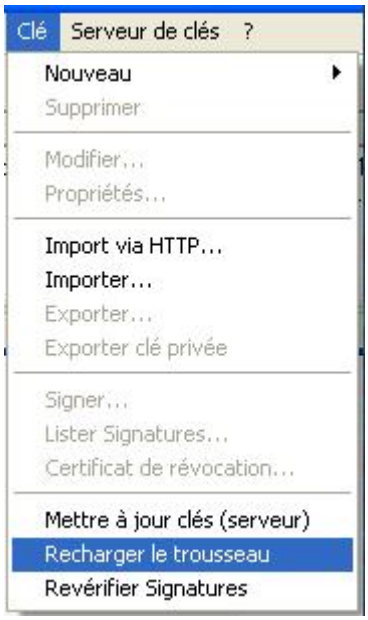
Cliquez sur le bouton « OK ». Vous retrouvez alors l'écran du gestionnaire de clés.

Vous pouvez répéter cette opération pour chacune des clés à importer, avant de passer à l'étape suivante.

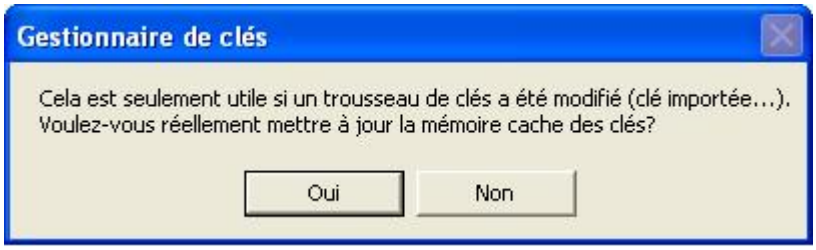
Ensuite passez à l'étape « Vérifier la clé ».

Vérifier la clé

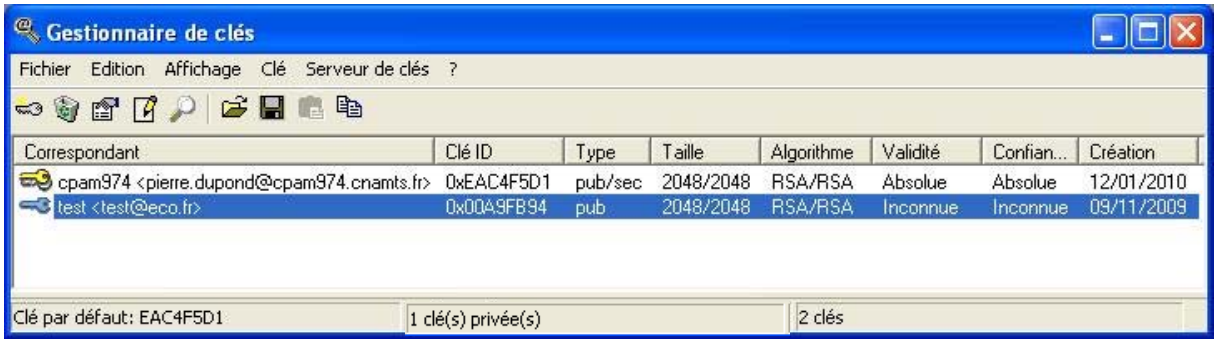
Si la(es) nouvelle(s) clé(s) n'apparaît pas dans le « Gestionnaire de clés », aller dans le menu « Clé » choisir la fonction « Recharger le trousseau »



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

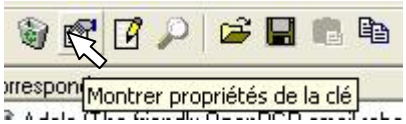


Toutes les nouvelles clés publiques importées apparaissent alors dans le « Gestionnaire de clés ». Vérifier les informations présentes pour chacune des clé publiques importées. Vous devriez normalement vérifier : nom de structure et mel du Correspondant, Clé ID - identifiant de la clé (l'information la plus difficile à usurper), la taille 2048/2048 et l'algorithme de chiffrement RSA/RSA.

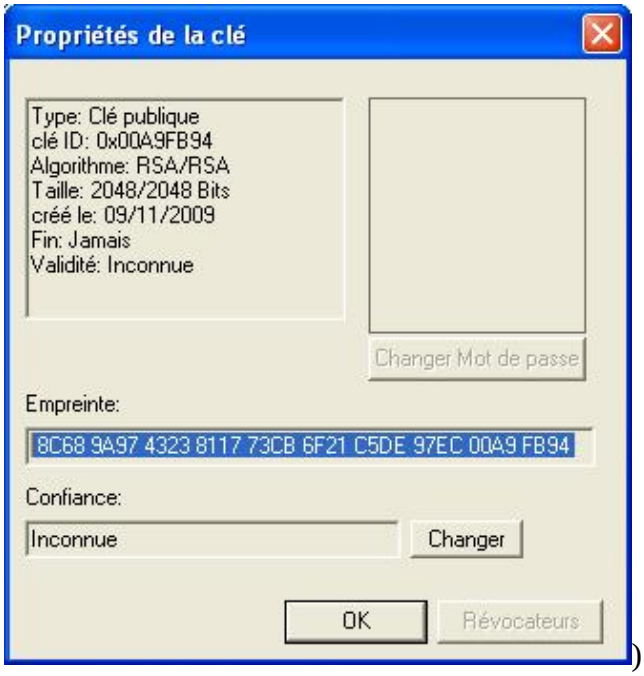


(Si la clé ne vous a pas été transmise de façon sûre, il convient de contrôler toute l'empreinte de la clé, et pas seulement son Clé ID (8 derniers caractères de l'empreinte). Il faut pour cela demander son empreinte au propriétaire de la clé, et la vérifier de la même façon.

Sélectionnez la clé. Le fond de la ligne de la clé devient bleu. Puis cliquez sur le bouton « Montrer propriétés de la clé » de la barre des boutons, qui représente une main tenant un document dans la barre des icônes, au dessus du trousseau (vous pouvez également faire un « Clic droit » sur la clé et choisir « Propriétés… » dans le menu contextuel apparu).



Un écran avec les principales informations sur la clé (dont l'empreinte) apparaît alors.

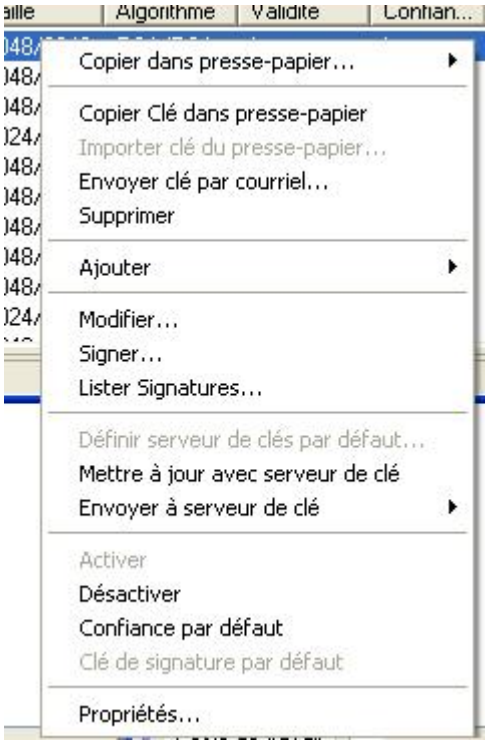


)

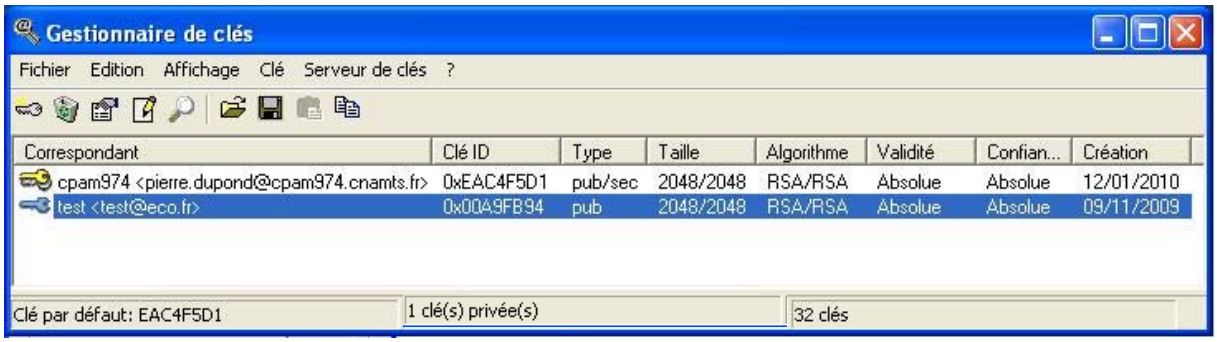
Si une clé n'est pas bonne, supprimez la du « Gestionnaire de clés » et si nécessaire alertez les personnes concernées.

Valider la clé

Pour chaque clé, si les informations sont exactes, attribuez lui votre confiance en faisant : « Clic droit » sur la clé. Un menu contextuel apparaît.



Sélectionner la commande « Confiance par défaut ». La confiance et la validité de cette clé deviennent alors « Absolue ».



Répétez cette opération pour chacune des clés importées.

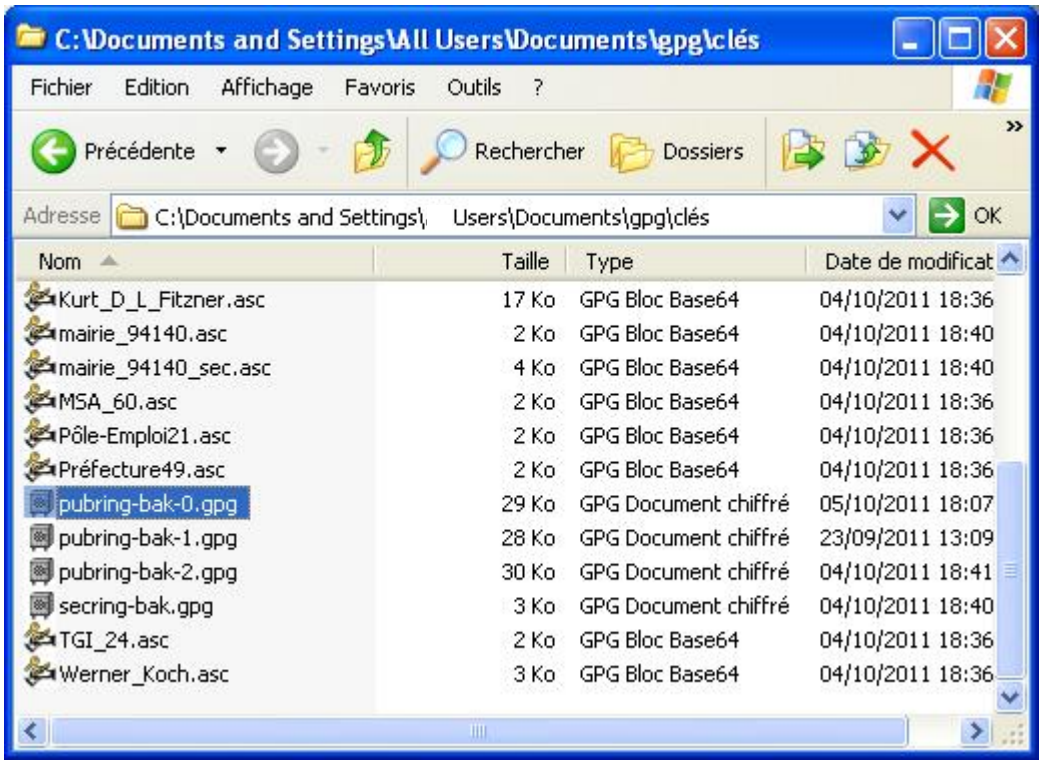
D - 4. Sauvegarde du trousseau de clé

Vous avez intérêt, après toute modification de votre trousseau de clés (ou de votre bi-clé), à faire une sauvegarde de celui-ci sur un support externe, dont l'accès est protégé, pour pouvoir restaurer votre bi-clé et le trousseau de clés même en cas de perte de votre disque dur.

L'arrêt de WinPT met à jour une copie du trousseau permettant de réaliser la sauvegarde. Cette copie du trousseau est réalisée automatiquement dans le dossier « Mes Documents/GPG/Clés », à l'arrêt de WinPT, si il a été modifié depuis la dernière utilisation. Cela met à jour les 2 fichiers de sauvegarde : un pour les clés publiques (pubring) et une autre pour votre bi-clé (secring). Pour les clés publiques, 3 copies tournantes pubring-bak-0 à 2.gpg seront générées (la date indique la plus récente et pas le N°).

Pour cela, arrêtez WinPT : réalisez un Clic sur l'îcone de WinPT dans la barre des tâches (zone en bas à droite de l'écran comportant l'heure) , puis dans le menu contextuel qui apparaît cliquez sur « Quitter ».

ouvrir le dossier « Mes Documents/GPG/Clés ». Sélectionner le pubring-back-x.gpg, dont la date d'enregistrement est la plus récente, et secring-back.gpg.



Copier (ou coupez puis collez) les fichiers sur le support externe prévu (disque, réseau, …). Vous pouvez supprimez ces fichiers ils seront recréés à la prochaine utilisation de WinPT.

Pour importer ces sauvegardes, voir le chapitre correspondant.

E – Utilisation courante

E – 1. Chiffrement et déchiffrement en cliquant sur le document

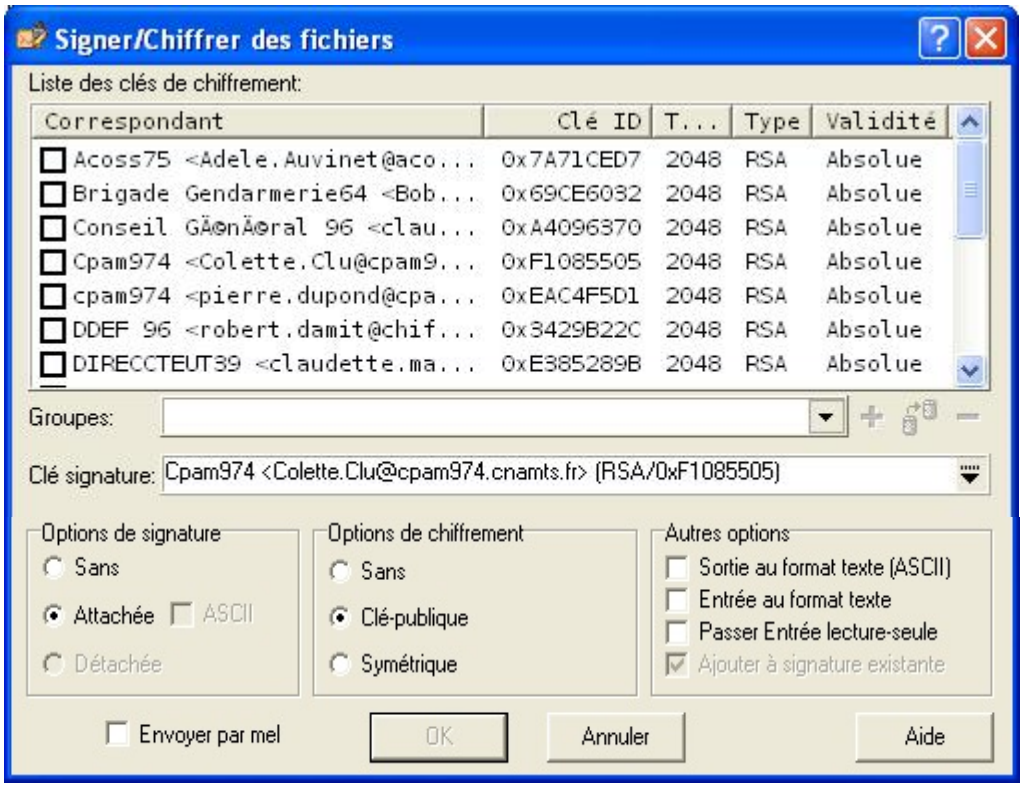
La méthode recommandée (la plus simple) de chiffrement et déchiffrement consiste à utiliser un menu contextuel qui s'ouvre en cliquant sur le document (avec un clic droit). Cela nécessite que l'outil GPGee soit opérationnel sur votre PC (ainsi que GPGee 64 pour un OS 64 bits).

Signer et chiffrer un document.

Commencer par copier le document que vous souhaitez transmettre dans le sous-dossier de « Mes Documents/Gpg ». Il est recommandé d'utiliser toujours ce dossier pour plus facilement pouvoir procéder aux suppressions nécessaires (et vous rendre compte d'oublis). L'intitulé de ce document ne sera pas modifié, aussi il ne doit pas comporter d'informations nominatives.

Dans l'explorateur Windows, sélectionner le(s) document(s) que vous souhaitez signer et chiffrer (il ne convient pas de seulement chiffrer un document) et cliquez avec le bouton droit dessus afin d'afficher le menu contextuel. Choisir la commande « Signer&Chiffrer » du menu « GPGee » (« GPGee64 » dans le cas d'un OS 64 bits). Si plusieurs documents sont sélectionnés, ils seront chiffrés en une fois, pour les mêmes destinataires. Cela produira un document chiffré par document sélectionné.

L'écran suivant apparaît alors :



Sélectionner, en cochant la case devant, la (ou les) clé(s) de chiffrement à utiliser : celle(s) de votre(vos) destinataire(s). Si nécessaire vous pouvez descendre dans la liste de destinataires avec l'ascenseur situé à droite de la liste. Votre propre clé est normalement utilisée par défaut,

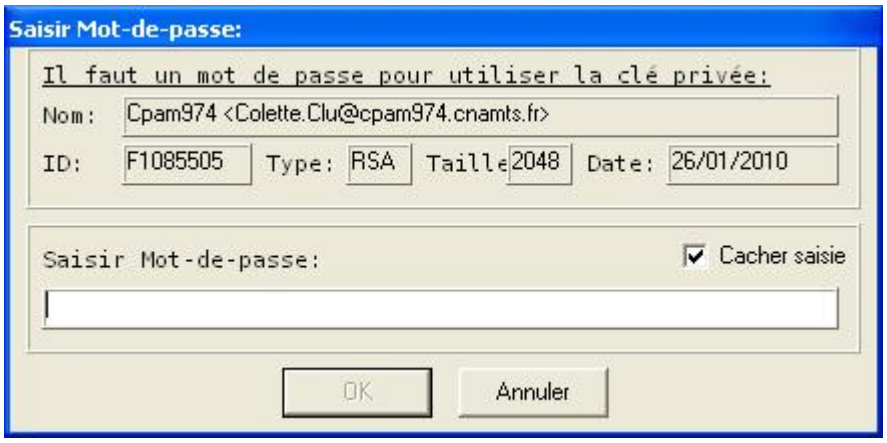
même si elle n'est pas cochée, ce qui vous permettra ensuite de vérifier le contenu du document chiffré en cas de doute.

Lors de la première utilisation, ou si vous avez modifié votre clé privée, cochez votre clé privée dans la liste déroulante « Clé signature ». Celle-ci sera mémorisée pour les fois suivantes.

ATTENTION : Surtout, ne modifiez pas les options qui sont sélectionnées, car sinon vous risquez de ne pas « signer&chiffrer » le document.

Si les paramétrages de votre ordinateur sont adaptés, en cochant la case « Envoyer par mel », un mel aux destinataires sélectionnés sera automatiquement constitué (avec les adresses mels indiquées dans les clés).

Puis cliquez sur « OK ». Le logiciel vous demande alors le mot de passe associé à votre clé privée.



En décochant la case « Cacher saisie », vous pouvez visualiser la saisie de votre mot de passe.

Cliquer ensuite sur le bouton « OK », qui s'est dégrisé, pour lancer le chiffrement et la signature du fichier. Le résultat est placé dans un fichier portant le même nom que le fichier originel, auquel a été rajouté l'extension « .gpg ». Il apparaît avec l'icône suivante : 

Attention, car le logiciel écrase l'éventuelle archive « .gpg » existante qui porterait le même nom que le document sans vous alerter. Il considère que vous faites en une fois l'archive pour tous vos destinataires.

Si vous aviez cocher la case « Envoyer par mel » vous trouvez alors un mel prêt à être envoyer avec le (ou les) documents chiffrés en pièce-jointe et les mels des destinataires pré-remplis.

Vous pouvez alors si vous le souhaitez supprimer le fichier non chiffré.

Déchiffrer un document.

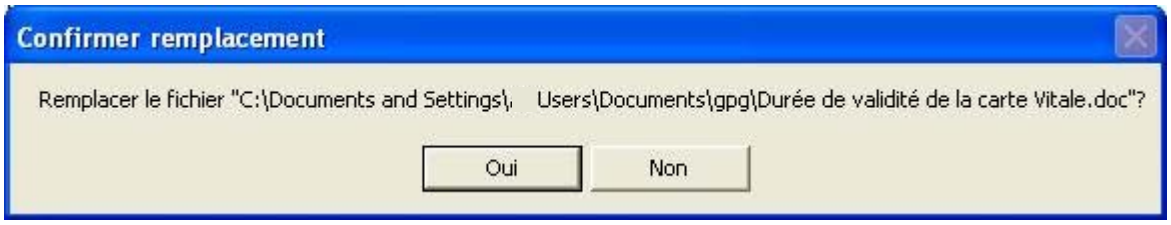
Les fichiers chiffrés portent l'extension « .gpg » et sont représentés avec l'icône : 

Commencer par copier le document chiffré que vous souhaitez déchiffrer dans le dossier « Mes Documents/Gpg ». Il est recommandé d'utiliser toujours celui-ci pour plus facilement pouvoir procéder aux suppressions nécessaires.

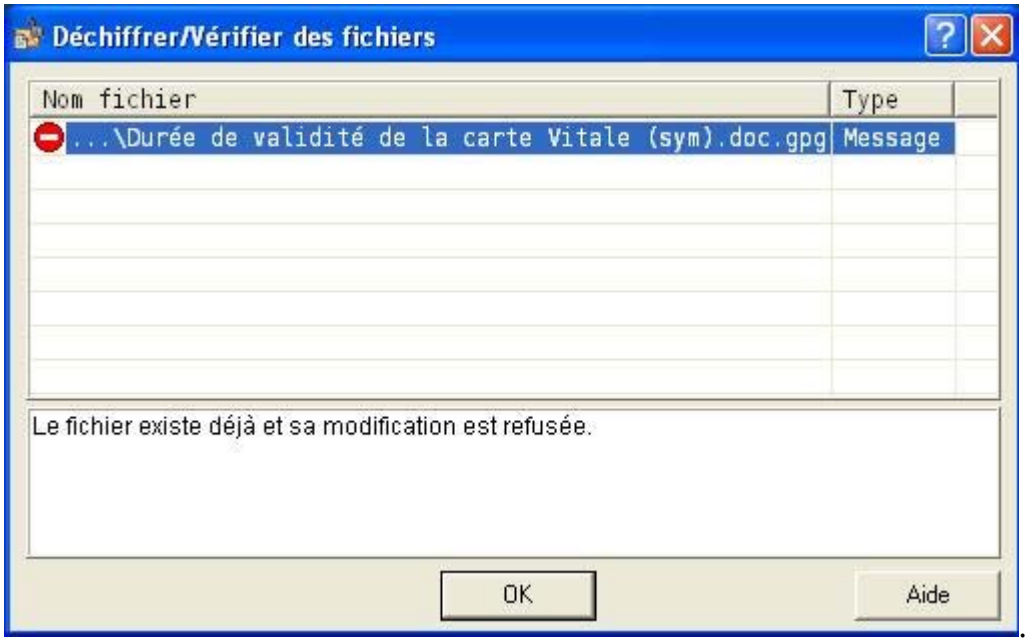
Dans l'explorateur Windows, sélectionner le fichier (ou les fichiers) avec l'extension « .gpg » que vous souhaitez déchiffrer et cliquez avec le bouton droit dessus afin d'afficher le menu contextuel. Choisir la commande « Déchiffrer&Vérifier » du menu « GPGee ».

ATTENTION : Si vous réalisez un double clic avec le bouton gauche (et pas un clic avec le bouton droit), vous lancerez le déchiffrement avec WinPT. Son seul inconvénient est que les messages donnés sont moins clairs qu'avec GPGee.

Si un fichier ayant le même nom que celui qui va être déchiffré existe déjà dans le même dossier, l'écran d'alerte suivant apparaît :



Si vous voulez le remplacer cliquez sur « Oui », sinon cliquez sur « Non » puis cliquez sur « OK » dans l'écran suivant qui apparaît, pour pouvoir modifier le nom de ce fichier avant de recommencer l'opération de déchiffrement.



Sinon le logiciel vous demande alors de saisir le mot de passe de votre clé privée.

En décochant la case « Cacher saisie », vous pouvez visualiser la saisie de votre mot de passe.

Cliquez ensuite sur le bouton « OK », qui s'est dégrisé, et le fichier est déchiffré dans le même répertoire sous le même nom de fichier, mais sans l'extension « .gpg ».

Il convient de faire attention aux informations délivrées par ce dernier écran. La signature doit être indiquée comme étant au format SHA256 et la couleur de la coche située à gauche du nom du document déchiffré doit vous alerter sur des risques potentiels

Le déchiffrement s'est parfaitement déroulé. La zone de texte en dessous du nom de fichier donne quelques informations supplémentaires sur ce qui a été réalisé (et notamment le format de la signature).

Le déchiffrement a été réalisé mais votre attention doit être attiré sur une possible anomalie. La zone de texte en dessous du nom de fichier donne plus d'informations (signature avec une clé non validée, expirée ou révoquée…).

Le déchiffrement ou la vérification de signature ne s'est pas correctement réalisé. Différentes origines sont possibles : erreur de mot de passe, signature inconnue... Il est possible que le document ait été déchiffré (si problème de vérification de la signature).

GPG n'a même pas essayé de déchiffrer ce document. Le motif figure dans la zone de texte en dessous des noms de fichier (vous avez vous même arrêté l'opération…)

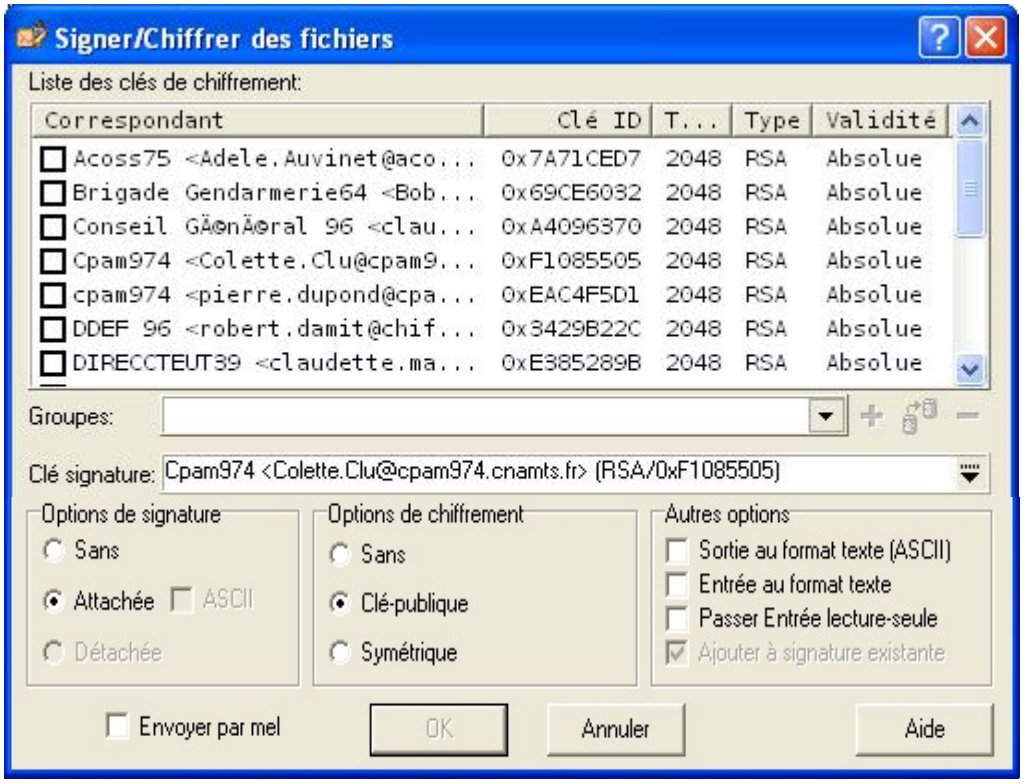
Déchiffrement en cours.

E – 2. Créer et gérer un groupe de destinataires

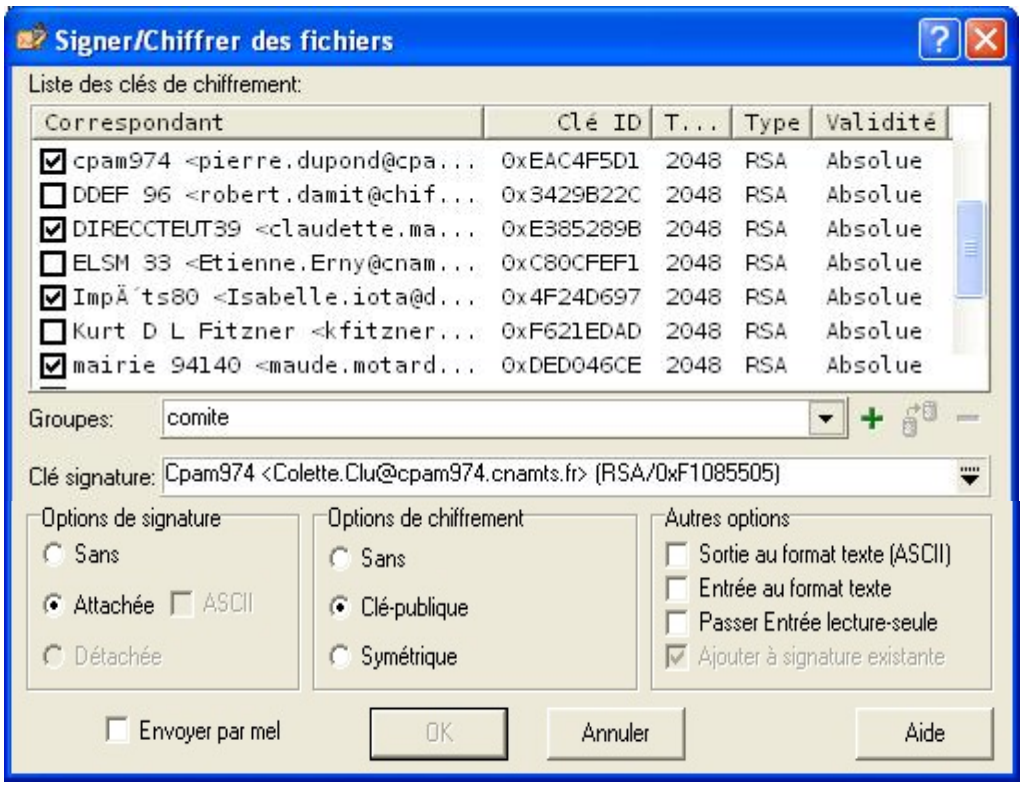
Si GPGee est installé sur votre PC vous pouvez créer et modifier des groupes de destinataires pour vous simplifier l'envoi récurent de documents à un même groupe de destinataires.

Cliquez (avec un clic droit) sur un document à chiffrer et choisir de le signer&chiffrer avec GPGee.

L'écran qui va alors apparaître vous permet également de créer des « Groupes » de destinataires.

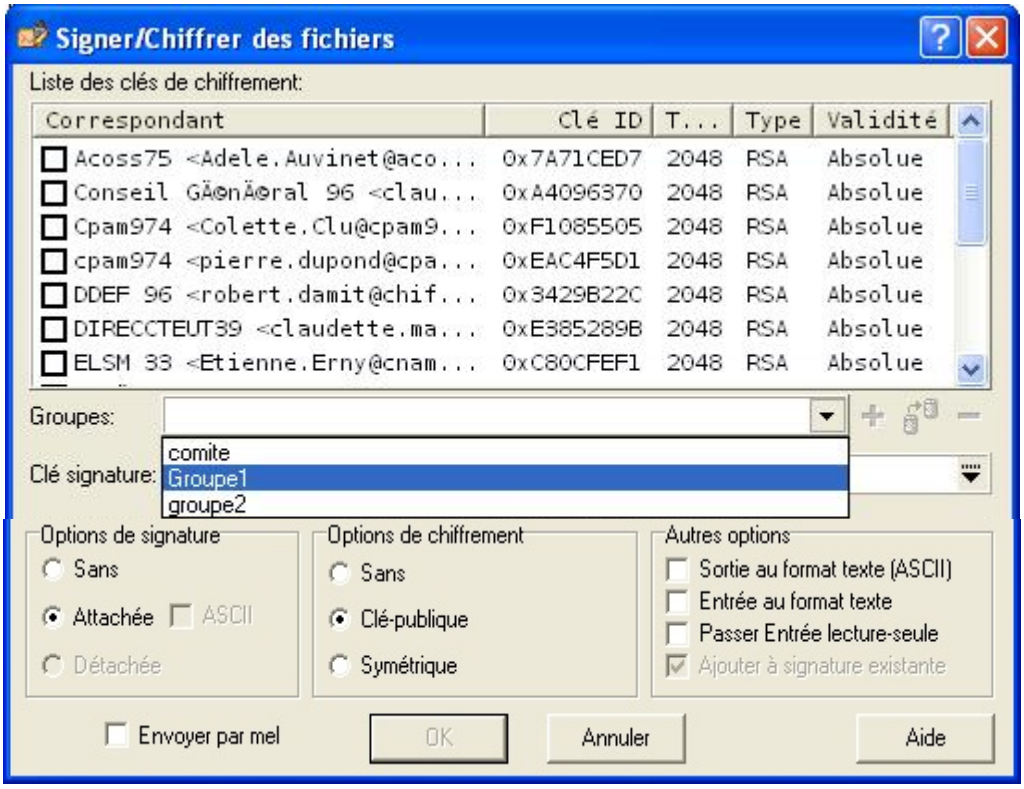


Saisissez d'abord un nom de groupe dans la zone de saisie intitulée « Groupes » (en dessous de la liste des correspondants). Cochez ensuite dans la liste des correspondants les noms des destinataires souhaités.

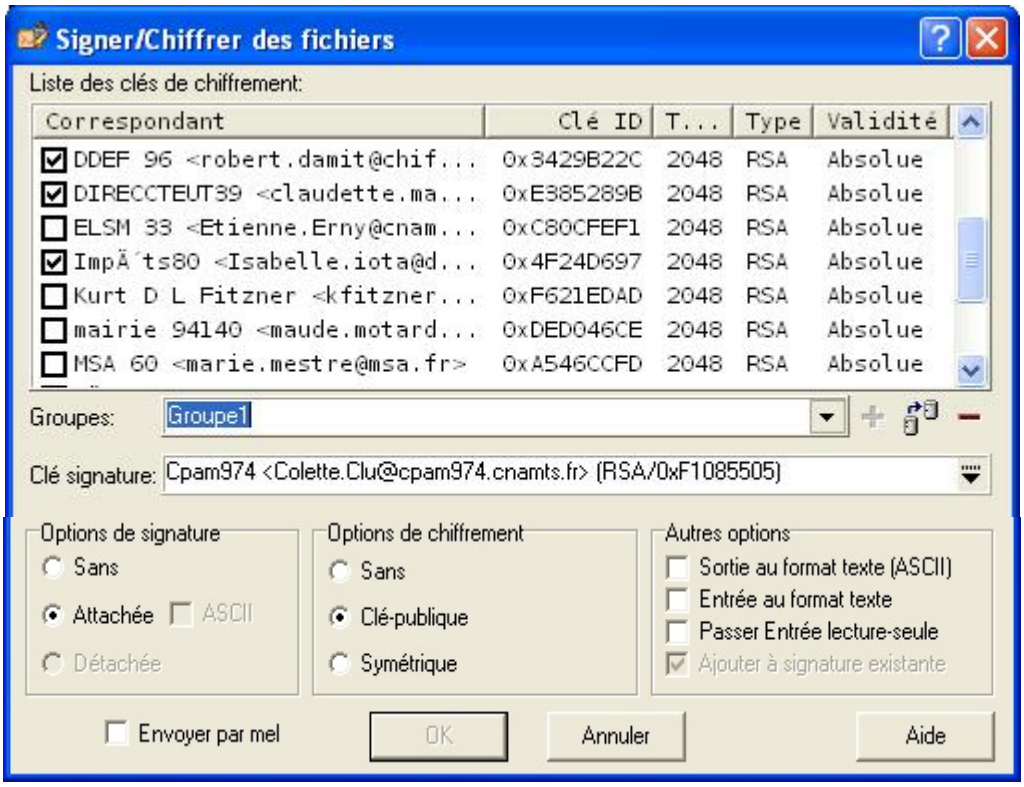


La croix à droite du nom de groupe saisi est maintenant dégrisée. Cliquez sur cette croix ✚ « Ajouter groupe de clés » pour mémoriser votre groupe. Vous pourrez alors le sélectionner avec le menu déroulant lors de votre prochain chiffrement.

A la prochaine tentative de chiffrement, en cliquant sur la flèche du menu déroulant à droite du champ de nom des « Groupes », vous pourrez sélectionner un groupe de destinataires.



Les cases des différents destinataires du groupe sont alors cochées automatiquement.



Une fois le groupe sélectionné, vous pouvez toujours ajouter ou enlever des destinataires en cochant ou décochant des cases devant les noms des destinataires. Cela ne modifie pas automatiquement le groupe enregistré.

Si vous souhaitez remplacez la composition initiale du groupe de destinataires par la nouvelle liste sélectionnée, vous pouvez le faire en cliquant sur le bouton « Modifier groupe de clés » figurant à droite du nom de groupe. Si vous ne cliquez pas dessus, la liste initiale ne sera pas modifiée. Si vous avez importé des clés publiques, il faut penser à modifier la composition des groupes auxquels ces correspondants doivent appartenir. En cas de suppression d'une clé

dans le « gestionnaire de clés », celle-ci est automatiquement supprimée des groupes auxquels elle appartenait.

Pour supprimer le groupe de destinataires sélectionné, cliquez sur le bouton — « Supprimer groupe de clés » figurant à l'extrême droite du nom de « Groupes ». Un écran apparaît alors vous demandant si vous voulez réellement supprimer ce groupe de destinataires :

Cliquez alors sur « Oui » (sauf si ce n'est pas le cas).

E – 3. Démarrer WinPT :

Si WinPT ne démarre pas au lancement de votre session, ou si vous l'avez arrêté il peut être alors nécessaire de démarrer WinPT. La description de la manière de démarrer WinPT est donnée au chapitre D – 1.

E – 4. Arrêter WinPT

WinPT s'arrête automatiquement à la fermeture de votre session. Il lui arrive également parfois de s'arrêter tout seul à cause de l'échec d'une commande (dans ce cas il suffit de le redémarrer comme ci-dessus et de recommencer).

Vous pouvez également l'arrêter (même si des fenêtres comme « Gestionnaire de clés » ou « Gestionnaire de fichiers » sont ouvertes) en faisant un clic droit sur son icône dans la barre de tâche et sur le menu de WinPT qui apparaît en cliquant sur « Quitter ».

Cela génère un fichier de sauvegarde de vos clés (si elles ont été modifiées).

Si vous avez par erreur réalisé des actions non prévues dans ce mode d'emploi, vous pouvez obtenir l'écran d'avertissement suivant avant l'arrêt.

Dans ce cas, cliquez sur « Oui » après avoir coché la case « Ne plus afficher ».

E – 5. Chiffrement d'un document avec WinPT:

Enregistrement du document à chiffrer

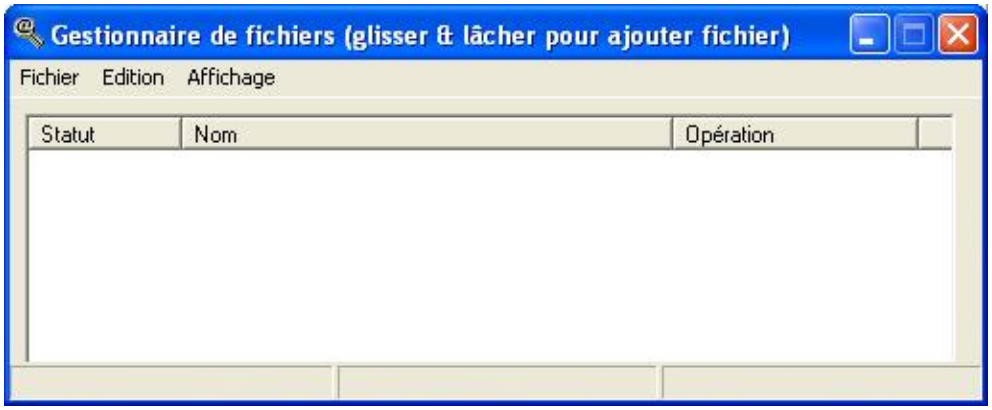
Commencer par copier le document que vous souhaitez transmettre dans le dossier « Mes Documents/Gpg ». Il est recommandé d'utiliser toujours celui-ci pour plus facilement pouvoir procéder aux suppressions nécessaires. L'intitulé du document ne sera pas modifié, aussi il ne doit pas comporter d'informations nominatives.

S'il n'est pas déjà en fonctionnement, démarrez WinPT.

Démarrage du « Gestionnaire de fichiers »

Faites un clic droit sur l'icône WinPT et sélectionner la fonction « Gestionnaire de fichiers ».

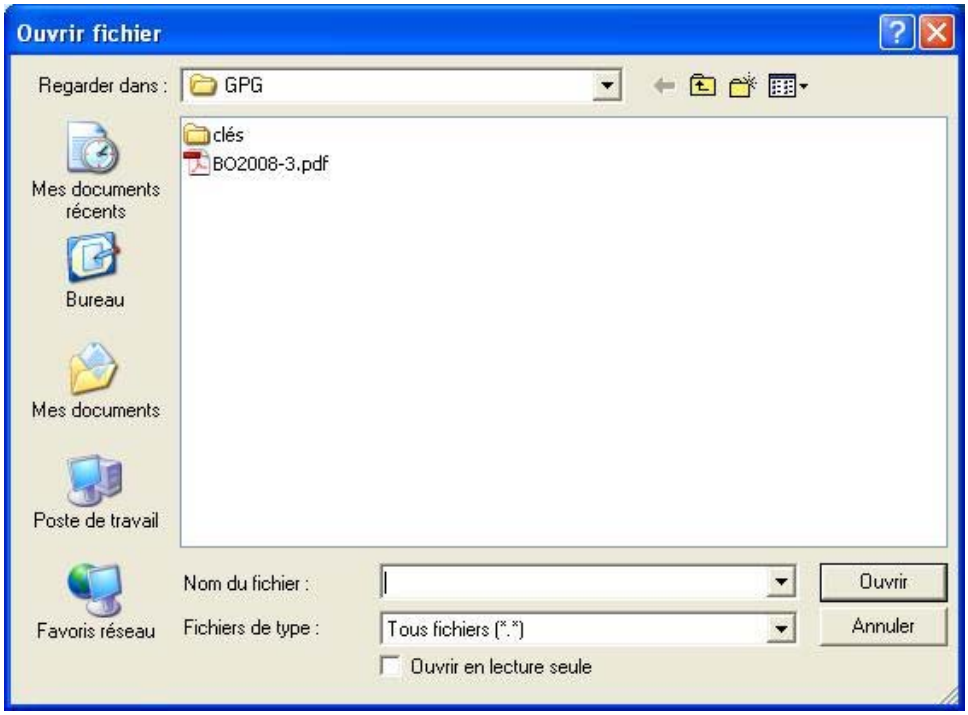
Une nouvelle fenêtre s'ouvre à l'écran.



Sélection du document à chiffrer

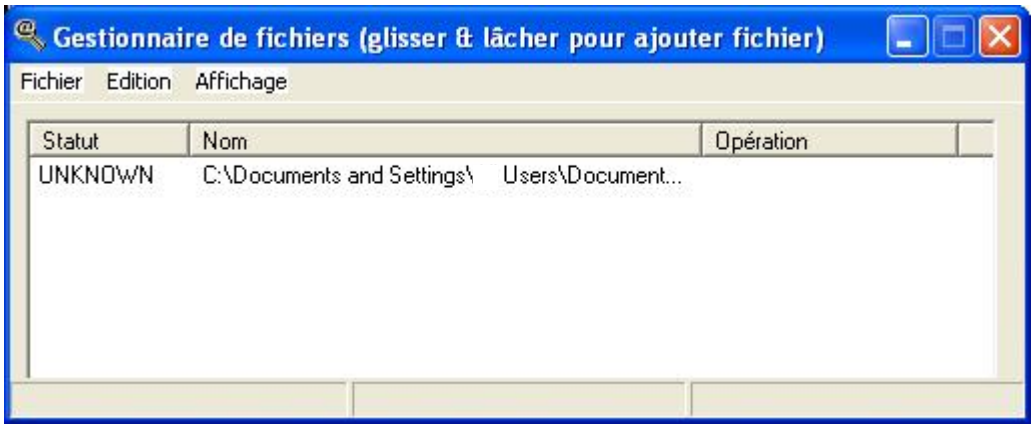
Vous pouvez soit venir déposer le fichier à chiffrer dans cette fenêtre depuis l'explorateur Windows, soit dans le menu « Fichier » choisir la fonction « Ouvrir » et naviguer pour aller chercher le document à chiffrer dans le sous-dossier « Mes Documents/Gpg ».

Dans ce deuxième cas une fenêtre s'ouvre pour vous permettre de sélectionner le document.



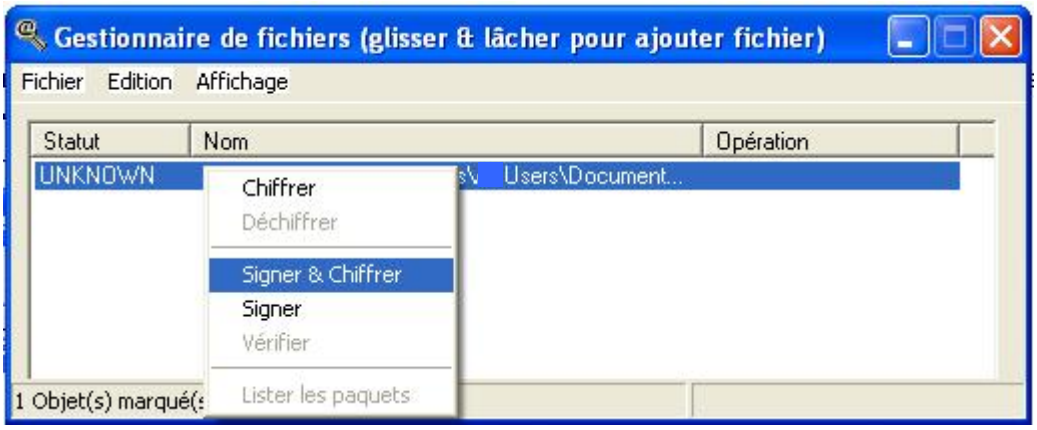
Une fois le document sélectionné (fond devenu bleu), cliquez sur le bouton « Ouvrir ».

Le document à chiffrer est maintenant chargé dans le « Gestionnaire de fichiers ».

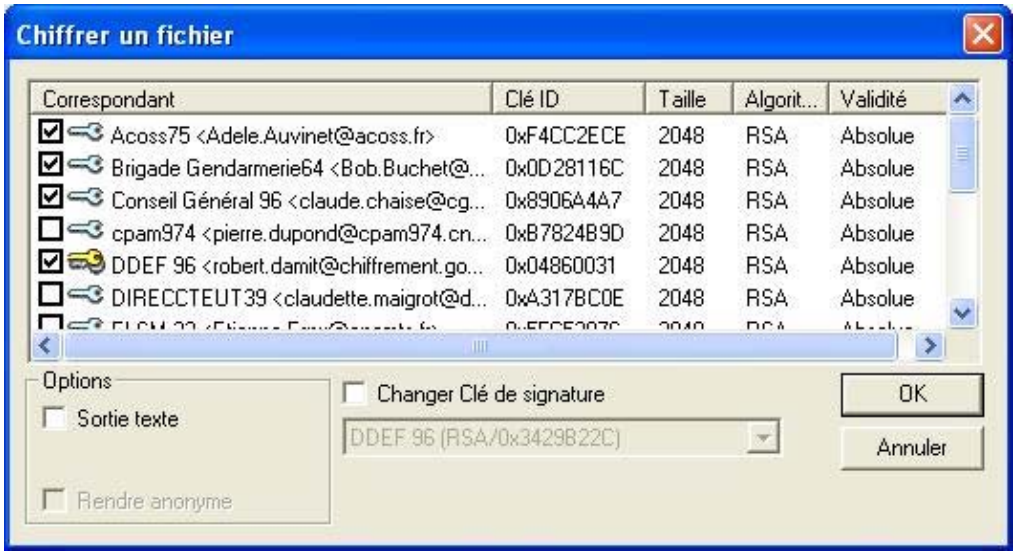


Lancement du chiffrement

Faire un clic droit sur la ligne du document dans le « Gestionnaire de fichiers » et choisissez la fonction « Signer & Chiffrer ». Il convient de toujours signer **et** chiffrer les documents et pas de seulement les chiffrer (encore moins de seulement les signer).

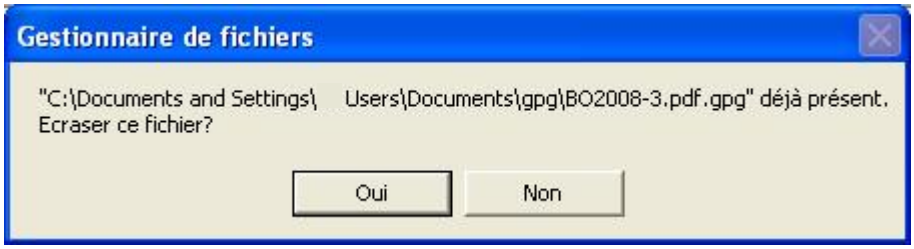


Une nouvelle fenêtre s'ouvre qui vous montre les différentes clés de votre trousseau.

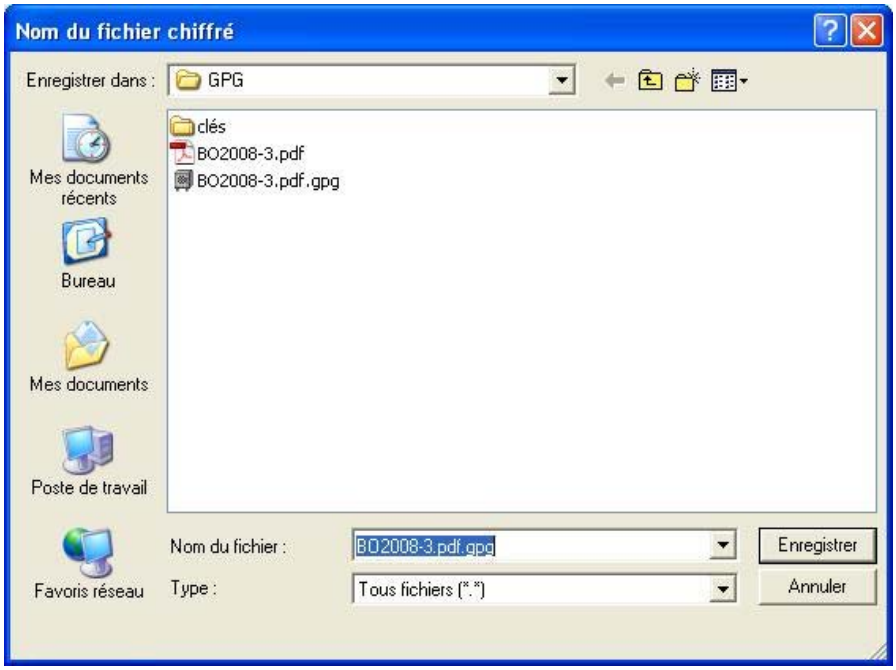


Comme cela est visible sur la copie d'écran ci-dessus, cochez les cases des clés des destinataires auxquels vous voulez envoyer le document. Il convient de toujours vous inclure dans les destinataires, ce qui n'est pas fait par défaut avec WinPT (contrairement à GPGee). Il convient donc à chaque fois de cocher votre clé privée (qui apparaît en jaune) en plus de celles des destinataires. Ne cochez pas d'option. Votre clé de signature qui va être utilisée apparaît sur fond grisé et n'a normalement pas besoin d'être modifiée (sinon cochez la case « Changer Clé de signature »). Cliquez ensuite sur le bouton « OK ».

Si une archive chiffrée ayant le même nom que celle qui va être produite préexiste, WinPT vous alerte avec l'écran suivant.



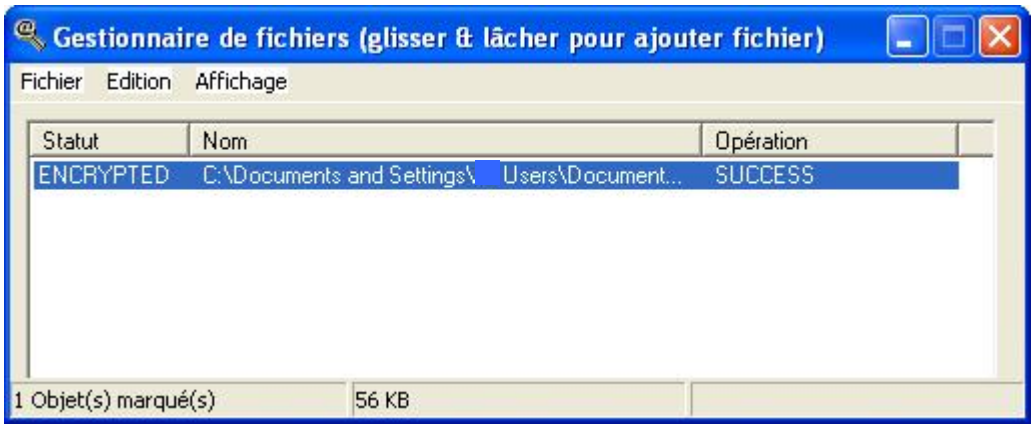
Si vous souhaitez remplacer le document chiffré préexistant, cliquez sur « Oui », sinon cliquez sur « Non ». WinPT va alors vous proposer, avec l'écran suivant, de donner un nom différent au document qui va être créé :



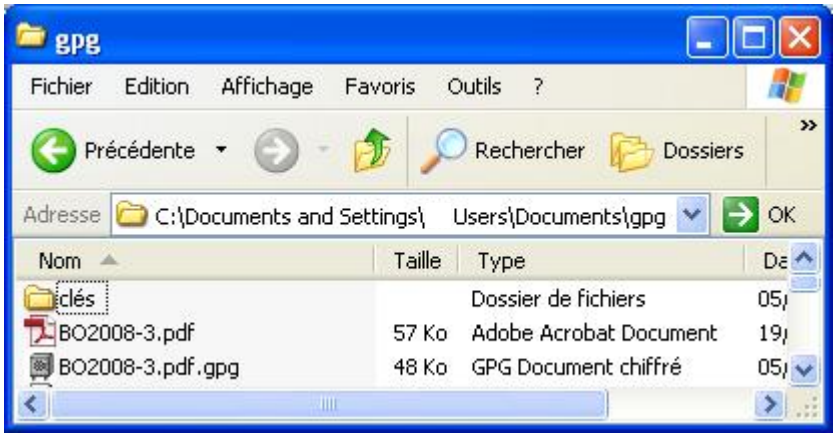
Vous arriverez ensuite à la fenêtre suivante qui vous demande de saisir le mot de passe de votre clé privée pour pouvoir déchiffrer le document.

Décochez la case « Masquer la saisie » pour mieux vérifier votre frappe et saisissez votre mot de passe, puis cliquez sur le bouton « OK ».

Vous retrouvez alors l'écran du « Gestionnaire de fichiers ».



Le statut du document est passé à « ENCRYPTED » (chiffré avec GPG) et l'opération est réussie (« SUCCESS »). Le document chiffré est au même emplacement que le fichier d'origine.



Les fichiers chiffrés portent l'extension « .gpg » et sont représentés avec l'icône : 

E – 6. Déchiffrement d'un document avec WinPT:

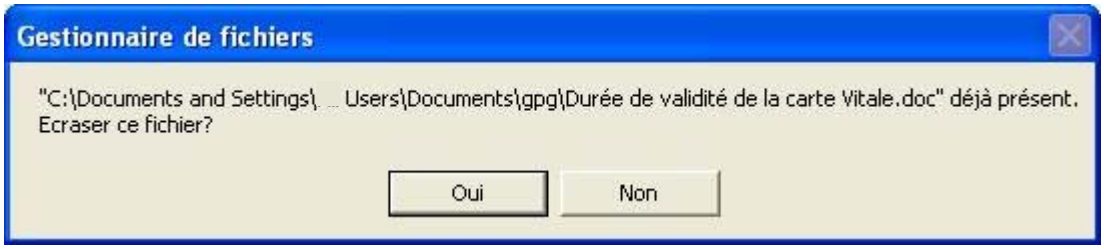
Le document chiffré (archive) vous est normalement parvenu en pièce jointe d'un mel (.gpg). Commencer par enregistrer le document chiffré joint dans le dossier « Mes Documents/Gpg ». Il est recommandé d'utiliser toujours celui-ci pour plus facilement pouvoir procéder aux suppressions nécessaires.

Deux modalités de déchiffrement sont possibles :

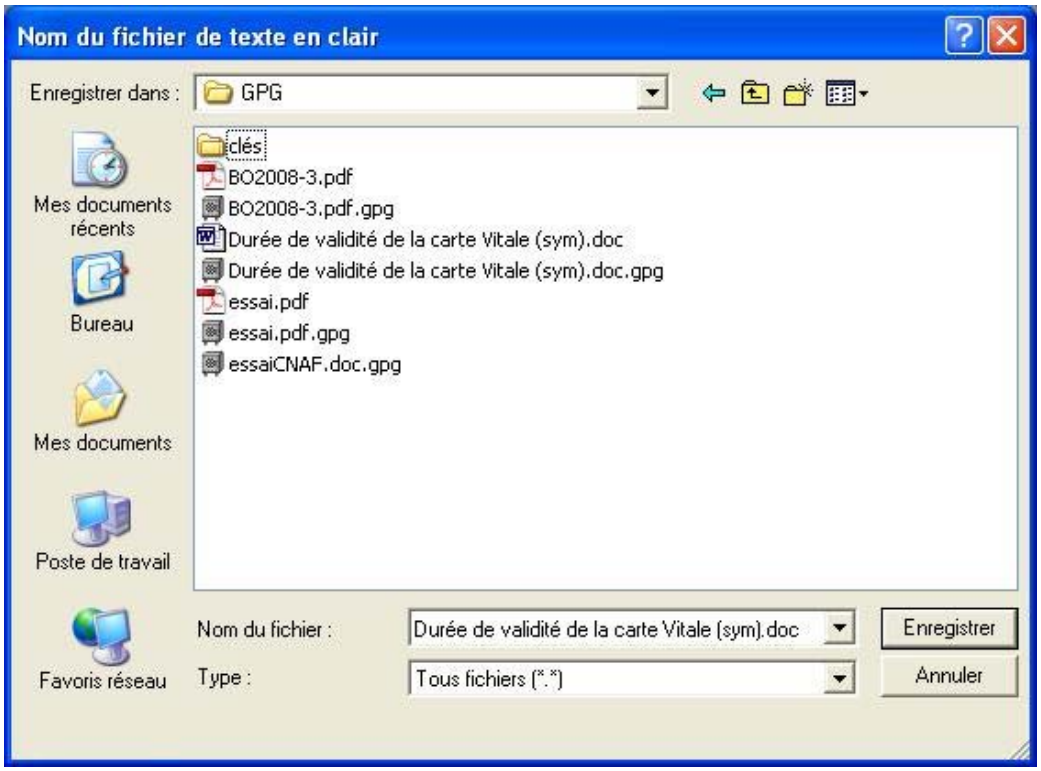
a) Directement en cliquant sur le document

Double cliquez sur le document à déchiffrer (WinPT n'a pas besoin d'être démarré).

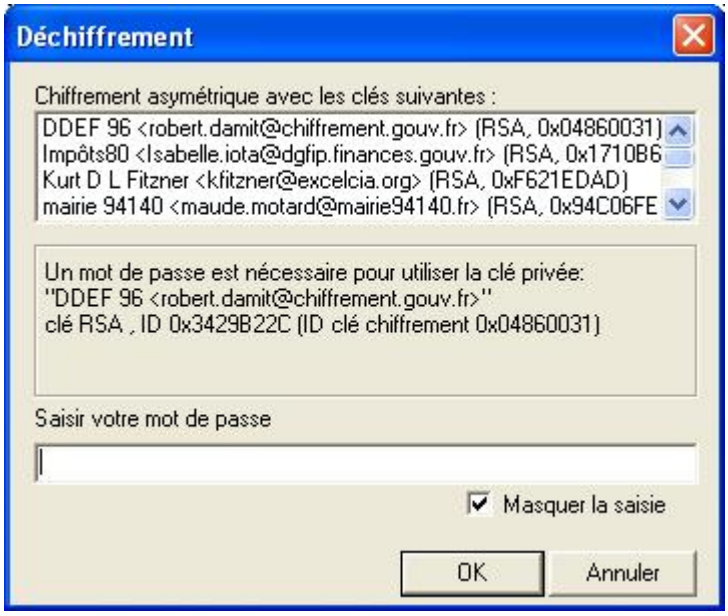
Si un document ayant le même nom que celui qui va être déchiffré est présent, vous aurez l'écran d'alerte suivant :



Si vous souhaitez remplacer le document préexistant cliquez sur le bouton « Oui ». Sinon, si vous cliquez sur le bouton « Non », WinPT va alors vous proposer de donner un nom différent au document qui va être déchiffré avec l'écran suivant :

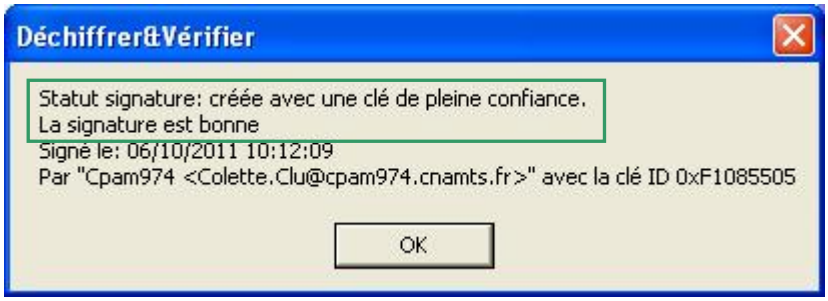


Sinon vous arrivez directement sur l'écran suivant qui vous indique que ce document a été chiffré avec votre clé publique (ici vous êtes Robert Damit de la DDEF 96)) et vous demande de saisir votre mot de passe pour utiliser votre clé privée afin de le déchiffrer (décochez la case « Masquer la saisie » pour pouvoir visualiser votre saisie).



Cliquez ensuite sur le bouton « OK ».

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



Les textes des 2 premières lignes doivent être exactement ceux-là, sinon il peut s'agir d'un message d'alerte présenté ci-après au E-7.

Le document déchiffré est enregistré dans le même dossier que le document chiffré.

b) Utiliser le « Gestionnaire de fichiers »

Si il n'est pas déjà en fonctionnement, démarrer WinPT.

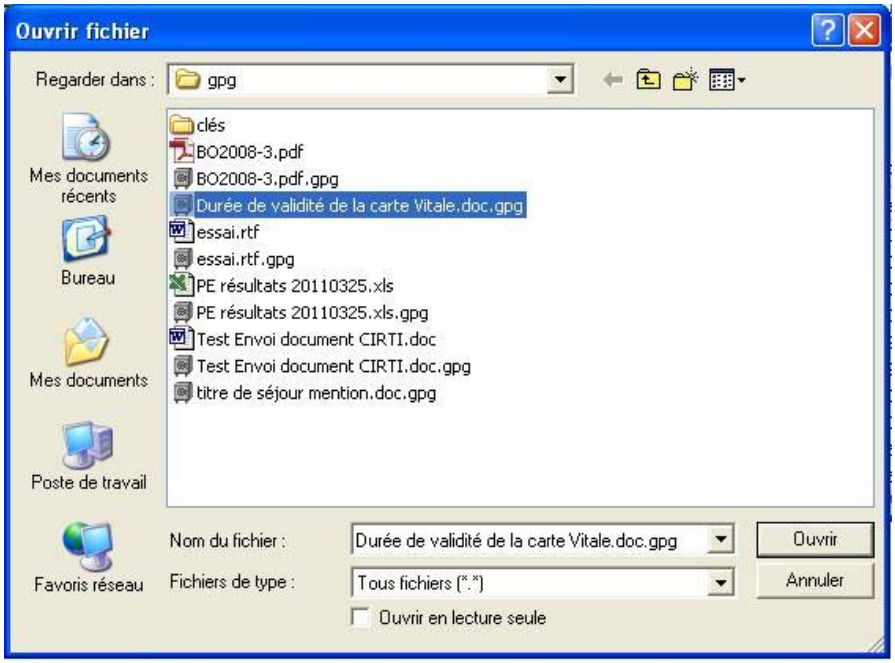
Faites un clic droit sur l'icône WinPT et sélectionnez la fonction « Gestionnaire de fichiers ».

Une nouvelle fenêtre s'ouvre :

Vous pouvez venir déposer le fichier à déchiffrer dans cette fenêtre depuis l'explorateur Windows (en gardant le doigt appuyé sur le clic gauche de la souris après avoir sélectionné le document).

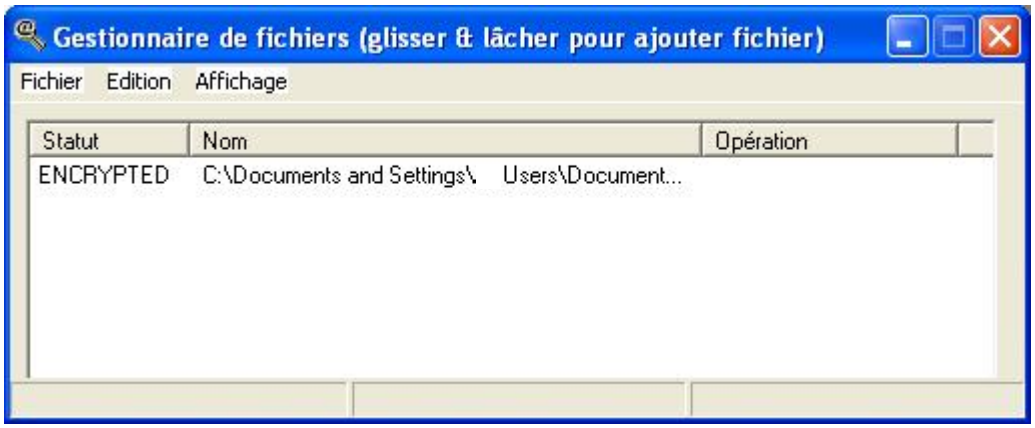
Ou également dans le menu « Fichier » du « Gestionnaire de fichiers » choisir la fonction « Ouvrir » et naviguer pour aller chercher le document à chiffrer dans le sous-dossier Mes Documents/Gpg.

La fenêtre de recherche du document apparaît alors.

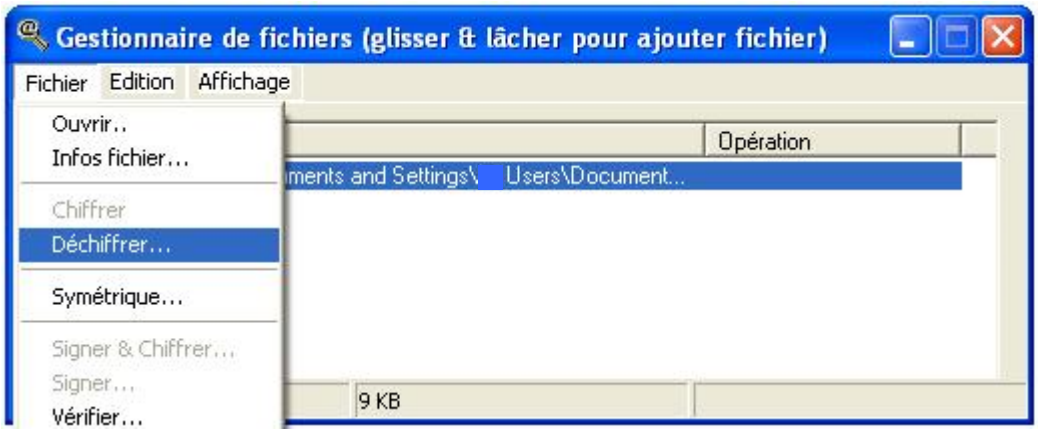


Quand vous avez sélectionné le bon document, cliquez sur le bouton « Ouvrir ».

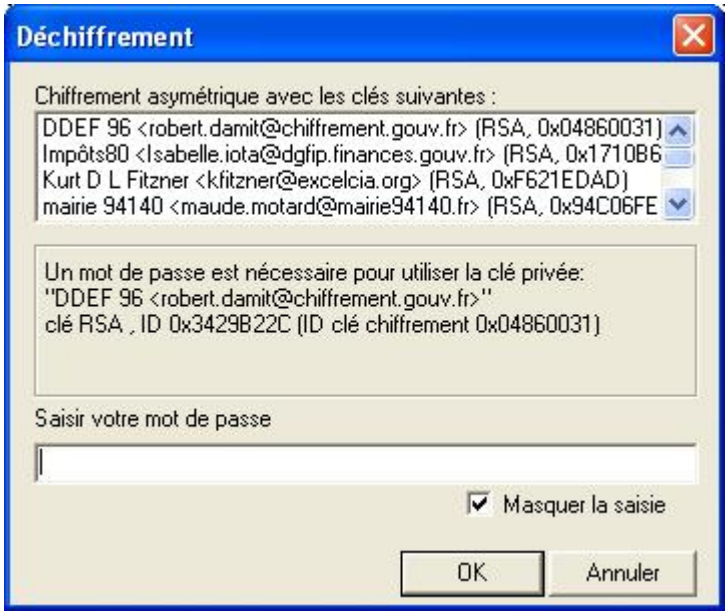
Le document chiffré est alors présent dans le « Gestionnaire de fichiers » avec le statut « ENCRYPTED » (chiffré par GPG).



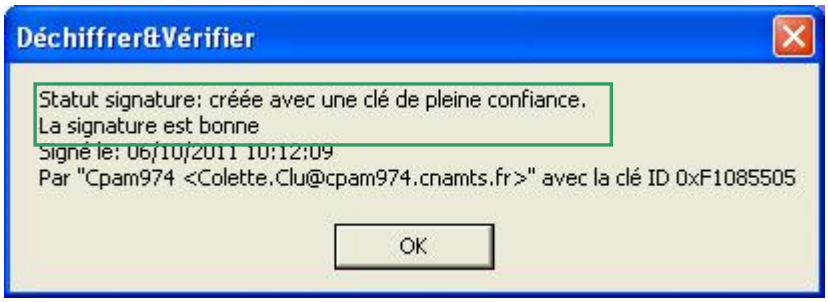
Retournez dans le menu « Fichier » ou faites un clic droit sur la ligne du document chiffré et choisissez la fonction « Déchiffrer » (déchiffre et vérifie la signature).



Un premier écran va vous indiquer que ce document a été chiffré avec votre clé publique (ici vous êtes Robert Damit de la DDEF 96) et vous demande de saisir votre mot de passe pour utiliser votre clé privée afin de le déchiffrer (décochez la case « Masquer la saisie » pour pouvoir visualiser votre saisie).

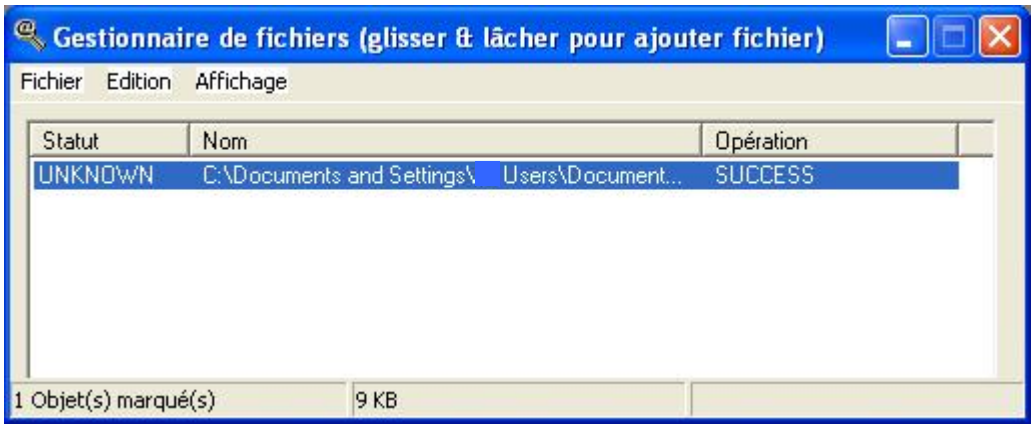


Cliquez ensuite sur le bouton « OK ». Une nouvelle fenêtre s'affiche vous indiquant si la clé utilisée pour signer le document correspond à une clé publique connue de vous et à qui elle appartient.

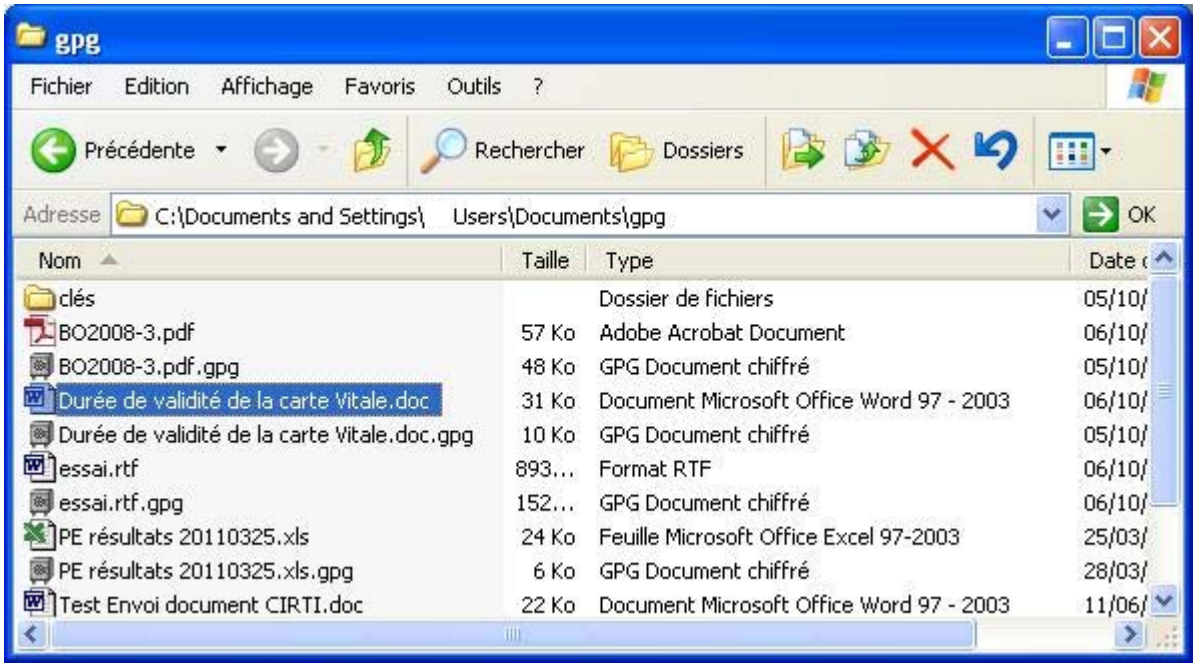


Vous êtes également susceptible d'obtenir tous les autres écrans présentés au E-7, avec les mêmes conséquences.

Cliquez ensuite sur le bouton « OK ». Le statut du document est passé à « UNKNOWN » (non chiffré avec GPG) et l'opération est réussie (« SUCCESS »).



Le document déchiffré est enregistré dans le même dossier que le document chiffré.



Pour vider le « Gestionnaire de fichiers » et traiter un autre fichier il suffit de le fermer en cliquant dans la croix sur fond rouge en haut à droite de sa fenêtre et de le ré-ouvrir depuis l'icône WinPT (ou de faire « Vider écran » dans le menu « Fichier »).

E – 7. Traitement des messages d'alerte lors du déchiffrement avec WinPT

Dans certaines situations, vous pourriez voir apparaître également les messages d'alerte suivants. La conduite à tenir est indiquée en dessous dans chaque cas.

- 

La signature n'est pas bonne, alors que vous disposez bien de la clé correspondante. Le fichier échangé a été corrompu (demandez de vous le renvoyer) ou sinon il s'agit d'une tentative d'usurpation. Il convient de mettre de côté les éléments et d'examiner les éventuelles actions à engager. Faites attention car le document a été déchiffré et peut contenir des « virus informatiques ». Il convient de détruire le document déchiffré sans l'ouvrir.

- 

Ce message est lié au fait que la signature de l'émetteur n'est pas reconnue. Contactez le pour savoir s'il a changé de clé de chiffrement sans vous transmettre sa nouvelle clé publique. Si ce n'est pas le cas le message est une tentative d'usurpation. Il convient de mettre de côté les éléments et d'examiner les éventuelles actions à engager. Faites attention car le document a été

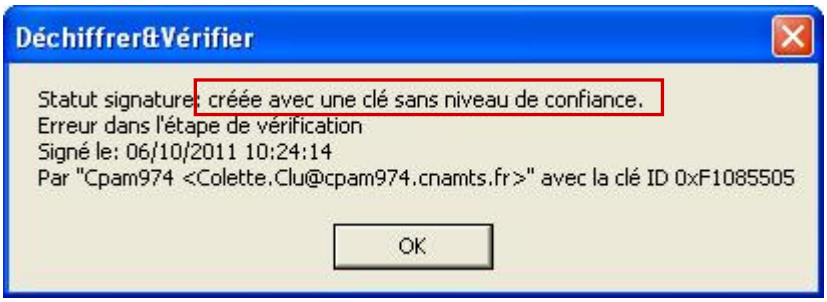
déchiffré et peut contenir des « virus informatiques ». Il convient de détruire le document déchiffré sans l'ouvrir.

- 

Ce message est lié au fait que GPG ne réussit pas à déchiffrer correctement le document. Le document n'est pas un document chiffré avec GPG ou il a été corrompu (demandez de vous le renvoyer), sinon il s'agit d'une tentative d'usurpation. Il convient de mettre de côté les éléments et d'examiner les éventuelles actions à engager. Faites attention car le document peut avoir été déchiffré et peut contenir des « virus informatiques ». Il convient de détruire le document déchiffré sans l'ouvrir.

- 

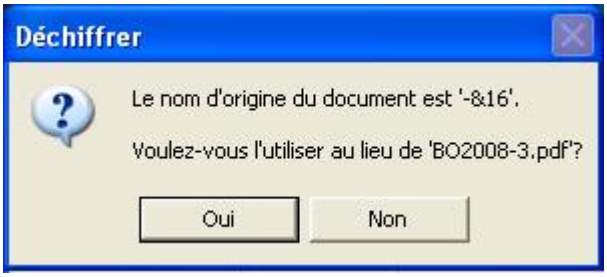
GPG n'a pas réussi à déchiffrer le document. Le document a été corrompu (demandez de vous le renvoyer), sinon il s'agit d'une tentative d'usurpation. Il convient de mettre de côté les éléments et d'examiner les éventuelles actions à engager. Faites attention car le document peut avoir été déchiffré et peut contenir des « virus informatiques ». Il convient de détruire le document déchiffré sans l'ouvrir.

- 

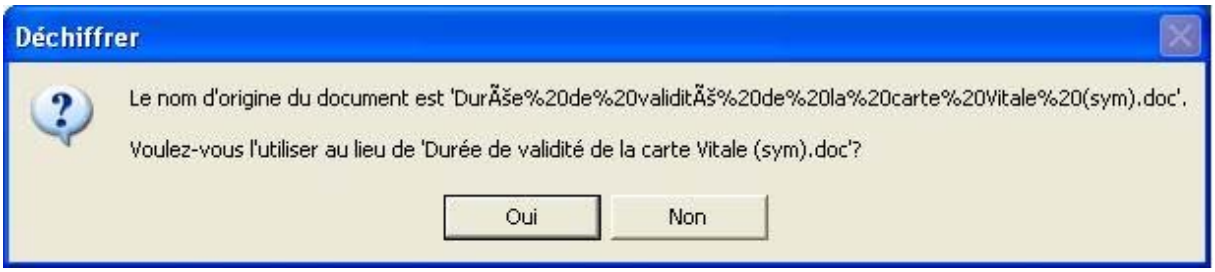
Il semble que vous n'ayez pas attribué votre confiance à la clé publique de l'expéditeur. Soit vous n'avez pas réalisé complètement les actions liées à la vérification de cette clé, soit c'est une clé qui ne devrait pas figurer dans votre trousseau de clés publiques.

- 

Ce message est probablement provoqué par une erreur du paramétrage de GPG sur votre poste qui n'est pas le bon. Alertez votre service informatique pour qu'il fasse mettre à jour votre paramétrage.

- 

Ce message est provoqué par une erreur de paramétrage de GPG chez votre correspondant qui a chiffré le document, mais ne vous empêche pas de déchiffrer le document. Cliquez sur le bouton « Non » et alertez votre correspondant.

- 

Ce message est lié à un problème de format du nom de fichier pour WinPT. Cliquez simplement sur « Non ».

F – Autres fonctions utiles

F – 1 Réimporter une sauvegarde de son bi-clé

- **Dans quel cas :**

Le bi-clé privé est à réimporter sur une machine saine en cas de perte ou de corruption du trousseau de clés (vol de l'ordinateur, installation d'un nouvel ordinateur, ordinateur piraté…), ou de suppression par erreur du bi-clé.

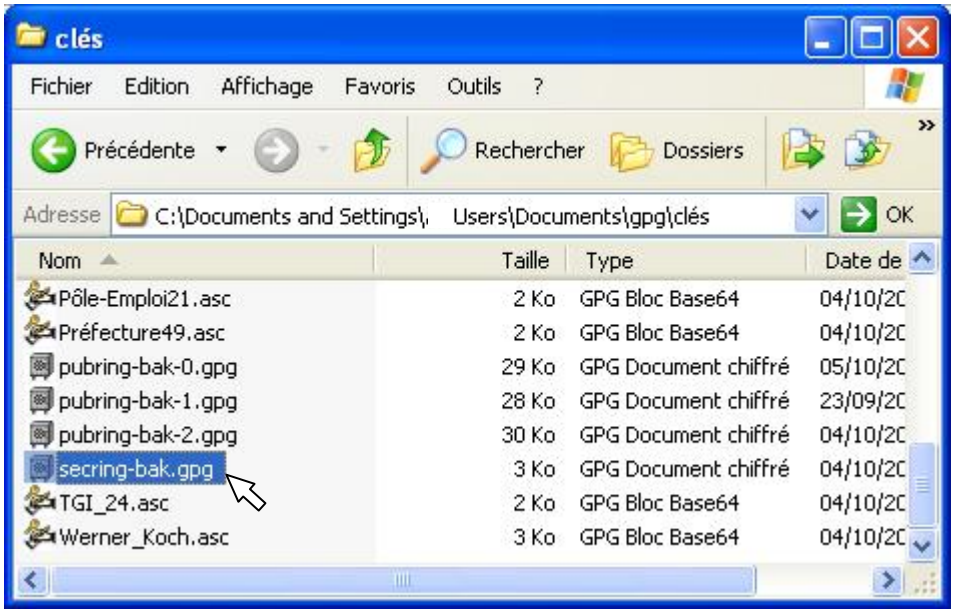
Si vous réinstallez un PC (nouveau PC, Changement de DD…), il convient de procéder à cette opération après l'installation de WinPT mais avant son premier lancement (donc avant de redémarrer le PC). Sinon WinPT va vous demander de créer un nouveau bi-clé.

- **Déroulement**

Connectez votre support de sauvegarde.

Ouvrir le dossier Mes documents/GPG/clés.

Copier, depuis le support de sauvegarde, la sauvegarde de votre bi-clé (« secring-back.gpg ») dans le dossier Mes documents/GPG/clés, en supprimant l'éventuel fichier du même nom qui s'y trouve.



Faites un double clic (gauche) sur le fichier « secring-back.gpg » (WinPT n'a pas besoin d'être démarré).

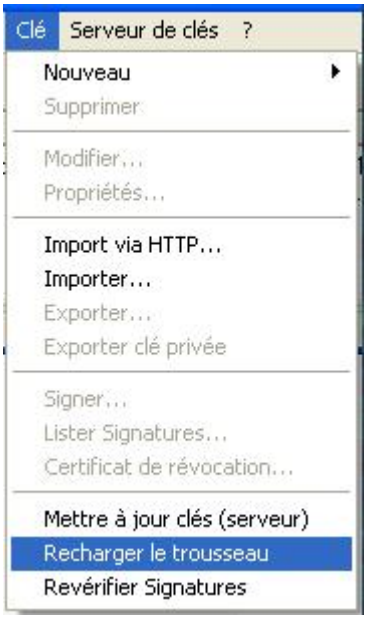
Un écran s'ouvre vous décrivant ce qui est importé (1 clé publique et 1 clé secrète composant votre bi-clé).

Valider en cliquant sur le bouton « OK »

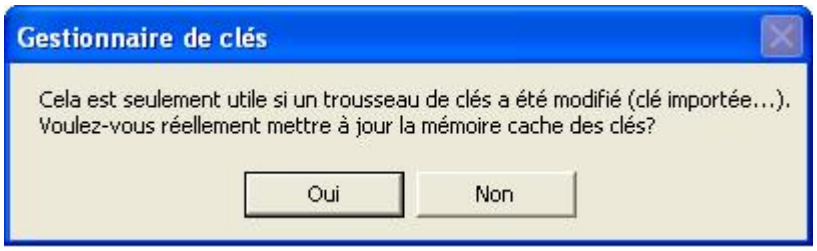
Lancer WinPT puis démarrez le « Gestionnaire de clés ».

Vous pouvez obtenir les messages d'erreur suivant qu'il faut accepter en cliquant chaque fois sur le bouton « OK ».

Si le bi-clé importé n'apparaît pas dans le « Gestionnaire de clés », dans le menu « Clé » choisir la fonction « Recharger le trousseau »



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



Votre bi-clé apparaît alors dans le « Gestionnaire de clés ». Faites un « clic droit » sur ce bi-clé. Un menu contextuel apparaît. Sélectionner la commande « Confiance par défaut ».

Faire un second « clic droit » sur le bi-clé pour faire réapparaitre le menu contextuel. Sélectionnez la commande « Clé signature par défaut ».

Vous pouvez alors fermer le « Gestionnaire de clés ».

F – 2 Réimporter une sauvegarde du trousseau de clés publiques

- **Dans quel cas :**

Le trousseau de clés publiques doit être réimporté en cas de perte du trousseau de clés (vol de l'ordinateur, installation d'un nouvel ordinateur, …) ou de corruption des fichiers.

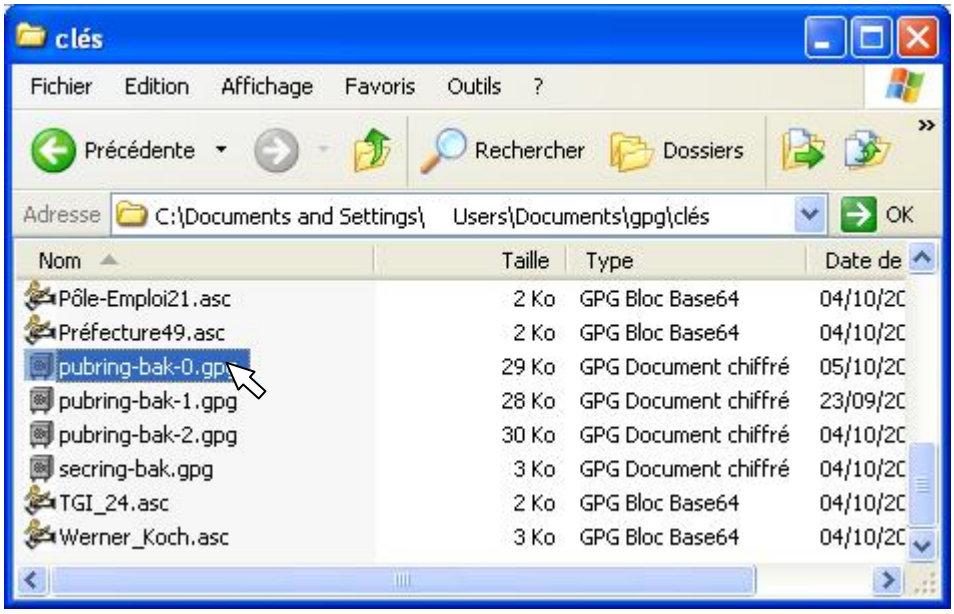
Message : Si l'ensemble des trousseaux de clés (privées et publiques) doit être réimporté, il est préférable de commencer par importer son bi-clé privé avant de réimporter le trousseau de clés publiques.

- **Déroulement**

Connectez votre support de sauvegarde.

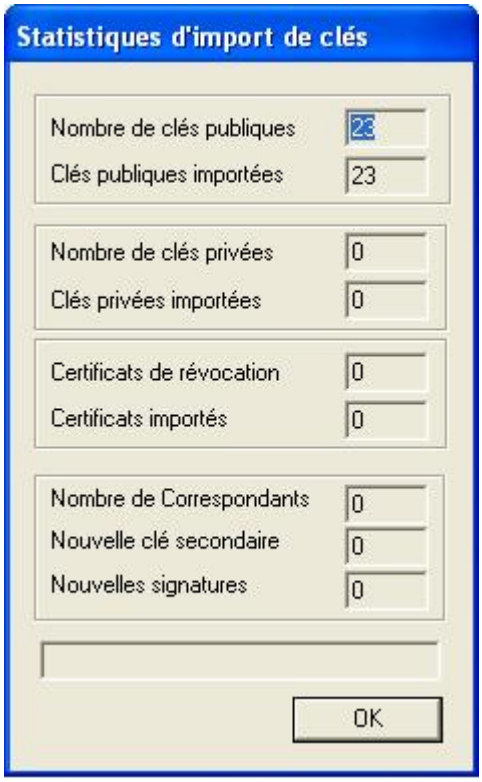
Ouvrir le dossier Mes documents/GPG/clés

Copier, depuis le support de sauvegarde, la sauvegarde du trousseau de clés publiques à importer (« pubring-back-x.gpg » ou x dépend du moment ou vous aurez fait cette sauvegarde) dans le dossier Mes documents/GPG/clés, en supprimant l'éventuel fichier du même nom qui s'y trouve.



Faites un double clic (gauche) sur le fichier « pubring-back-x.gpg » que vous venez d'importer (WinPT n'a pas besoin d'être démarré).

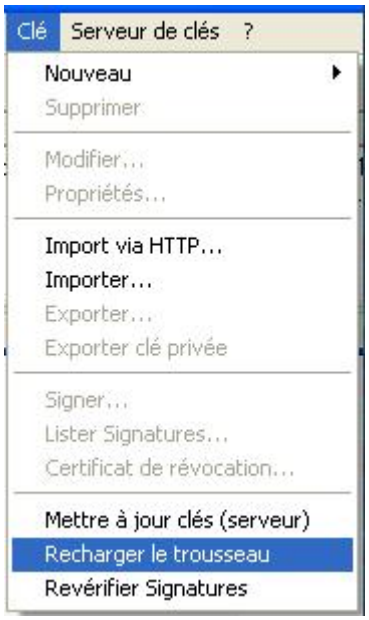
Un écran s'ouvre vous décrivant ce qui est importé. L'ensemble des clés publiques est importé en une fois (ici 23 clés publiques)



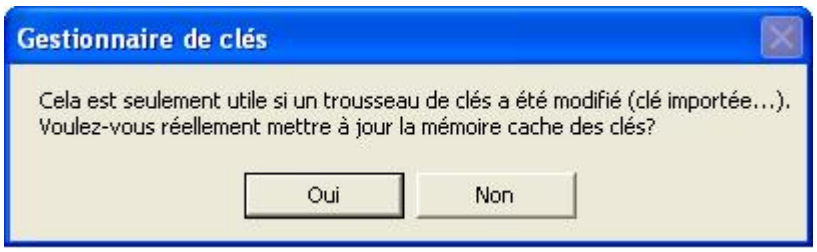
Cliquez sur le bouton « OK ».

WinPT étant en fonctionnement, démarrez le « Gestionnaire de clés ».

Si les clés publiques importées n'apparaissent pas dans le « Gestionnaire de clés », dans le menu « Clé » choisir la fonction « Recharger le trousseau »

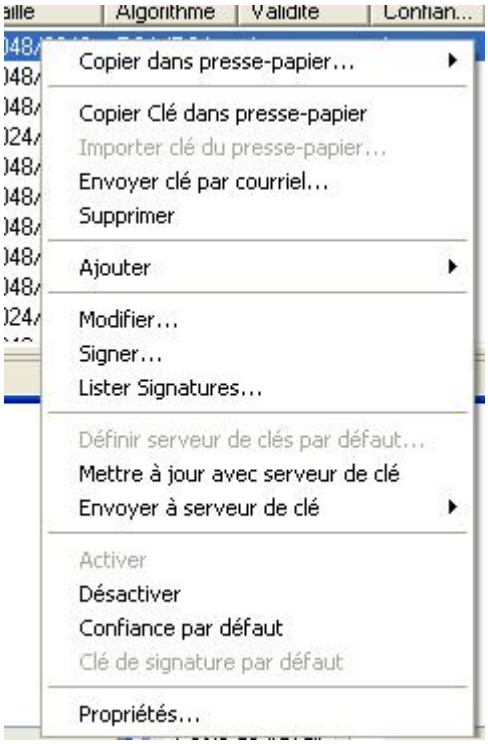


Cliquez sur « Oui » sur l'écran suivant qui apparaît.



Les clés publiques apparaissent alors dans le « Gestionnaire de clés ». Vérifier les informations présentes pour chacune des clé importées. Vous devriez au moins vérifier : Nom de structure et mel, Identifiant de la clé (l'information la plus difficile à usurper), la taille 2048/2048 et le procédé de chiffrement RSA/RSA.

Pour chaque clé, si les informations sont exactes, attribuez lui votre confiance en faisant : « Clic droit » sur la clé. Un menu contextuel apparaît.



Sélectionner la commande « Confiance par défaut ».

Sinon supprimer la clé de votre trousseau.

Puis passez à la clé suivante.

F – 3 Changer son mot de passe

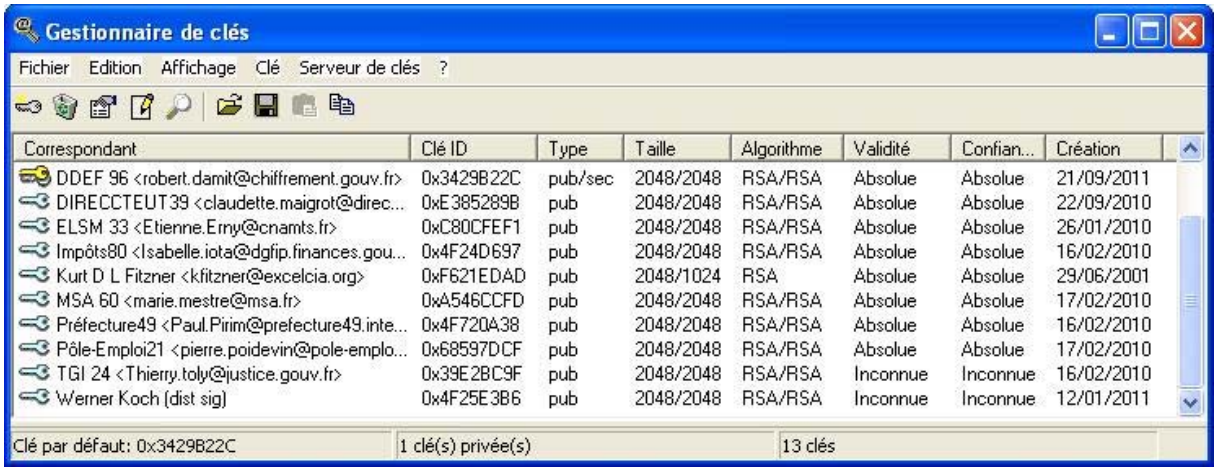
- **Dans quel cas :**

Vous pouvez avoir besoin de changer votre mot de passe car vous l'avez dévoilé par erreur ou parce qu'il vous faut le changer régulièrement par sécurité.

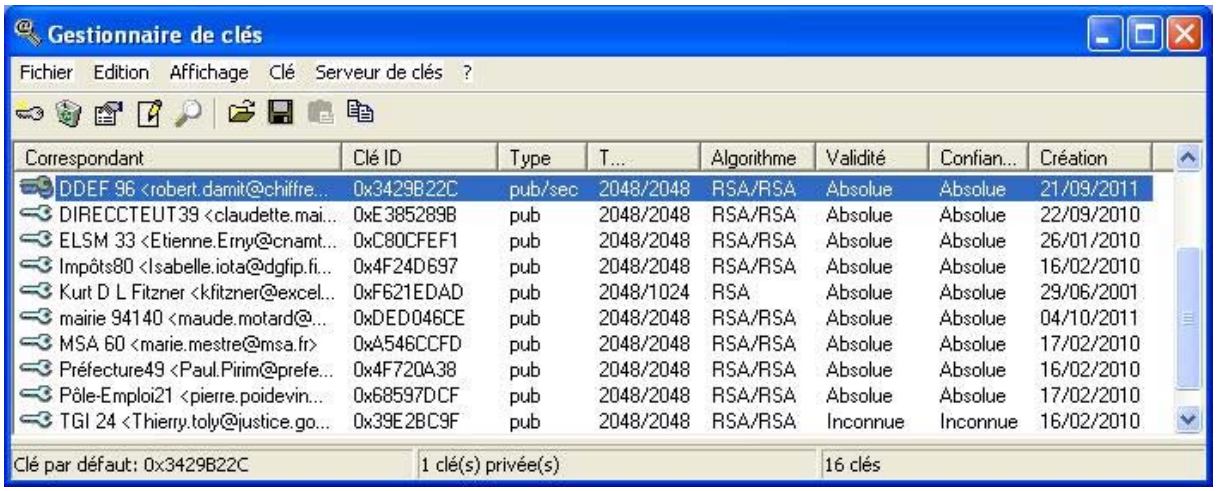
- **Déroulement**

Lancer le logiciel WinPT s'il n'est pas déjà en service. Dans le menu de WinPT,

sélectionnez le « Gestionnaire de clés ». Le « Gestionnaire de clés » s'ouvre alors



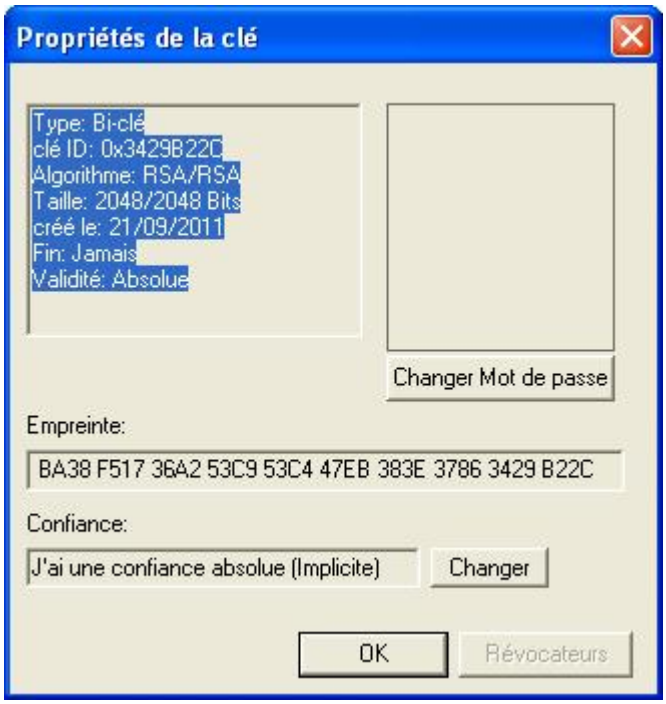
Sélectionner votre bi-clé (votre bi-clé (votre clé privée accolé avec sa clé publique) est celui comportant une clé jaune).



Une fois sélectionné, le fond de la ligne de votre bi-clé devient bleu.

Puis cliquez sur le bouton « Montrer propriétés de la clé » de la barre des boutons, qui représente une main tenant un document dans la barre des icônes au dessus du trousseau.

Un écran vous montrant les principales informations sur votre bi-clé apparaît alors.



Cliquer sur le bouton « Changer Mot de passe »

Saisir l'ancien mot de passe dans l'écran qui apparaît (décochez la case « Masquer saisie » si vous souhaitez voir votre saisie).

Puis cliquer sur le bouton « OK ». Un nouvel écran vous demande alors de saisir le nouveau mot de passe (décochez la case « Masquer saisie » si vous souhaitez voir votre saisie).

Le mot de passe doit comporter au minimum des chiffres et des lettres (ou des caractères spéciaux : ponctuation,%,$…) et comporter au moins 8 caractères (exemple : maison28). Sinon un écran d'alerte apparaîtra.

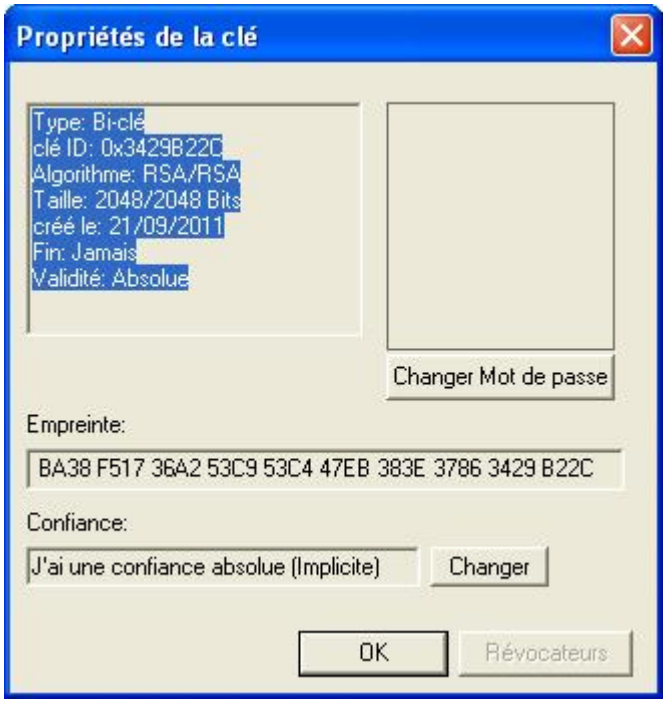
Ce mot de passe doit être facilement mémorisé par l'utilisateur car sa perte empêchera de chiffrer et déchiffrer les documents. Il est possible que l'utilisateur note son mot de passe sur un document qui doit alors être conservé à un emplacement sûr (par exemple un tiroir fermé à clé).

Une fois le nouveau mot de passe saisit cliquer sur le bouton « OK ». Il vous est alors demandé par l'écran suivant de saisir une seconde fois le nouveau mot de passe (décochez la case « Masquer saisie » si vous souhaitez voir votre saisie).

Une fois le nouveau mot de passe ressaisit cliquer sur le bouton « OK ».

Si il n'y a pas eu d'erreur vous êtes informé que le changement est réussi par l'écran suivant. Sinon il vous est demandé de recommencer.

Puis cliquez sur le bouton « OK »



Cliquez encore sur le bouton « OK ». Vous pouvez alors fermer le « Gestionnaire de clés ».

Il est alors recommandé d'arrêter WinPT pour générer une nouvelle sauvegarde avec ce nouveau mot de passe.

F – 4 Créer un nouveau bi-clé

- **Dans quel cas :**

Votre clé privée doit être changée suite à :

- L'oubli de votre mot de passe
- La divulgation de votre clé privée
- Le piratage de votre poste informatique
- Le vol de votre poste informatique

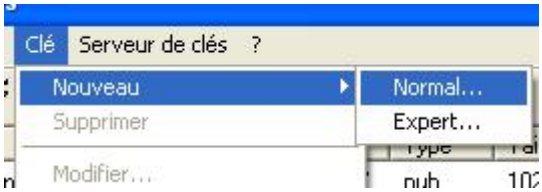
Dans ces situations, adressez un message d'alerte à vos interlocuteurs, puis créer votre nouveau bi-clé et transmettez votre nouvelle clé publique à tous vos correspondants.

- **Déroulement**

Lancer le logiciel WinPT s'il n'est pas déjà en service.

Dans le menu de WinPT sélectionnez le « Gestionnaire de clés »

Le « Gestionnaire de clés » s'ouvre alors. Y choisir le menu (Clé>Nouveau>Normal)



Vous obtenez maintenant un écran qui va vous permettre de créer votre bi-clé.

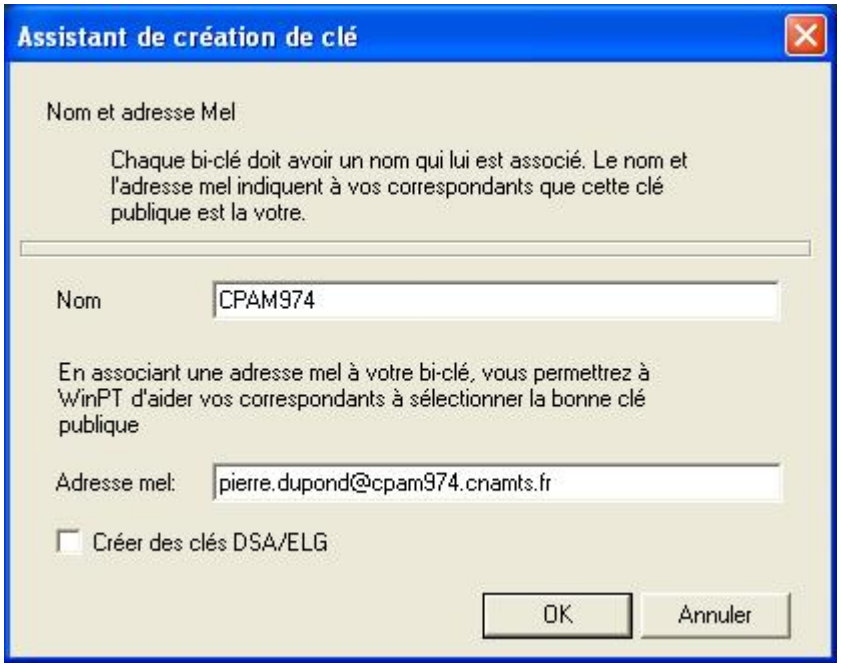
Aucune parenthèse ( ) ou crochet < > ne doit être utilisée lors de cette saisie, évitez également d'utiliser des lettres accentuées (é,â ù…).

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…). Attention à la saisie de cette adresse car elle peut être utilisée pour vous envoyer des mels.

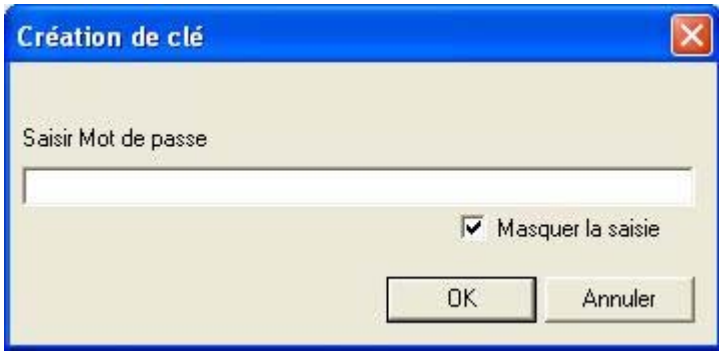
L'écran doit alors être ainsi renseigné (attention : ne pas cocher la case « Créer des clés DSA/ELG » car le niveau de sécurité de telles clés est insuffisant).



Cliquez maintenant sur le bouton « OK ».

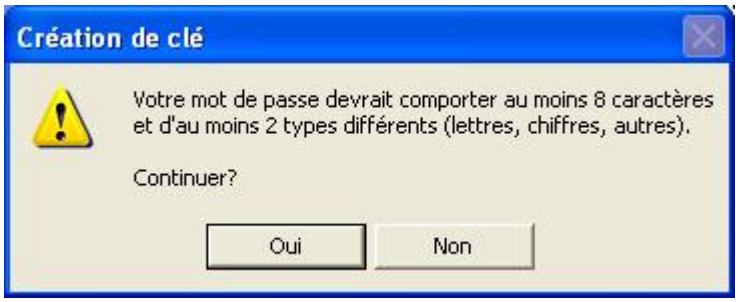
L'écran suivant apparaît vous demandant un mot de passe (« Saisir Mot de passe ») pour la clé privée. Décochez éventuellement la case « Masquer la saisie » pour pouvoir voir la saisie. L'utilisateur saisit son mot de passe qui doit comporter au minimum des chiffres et des lettres (ou des caractères spéciaux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

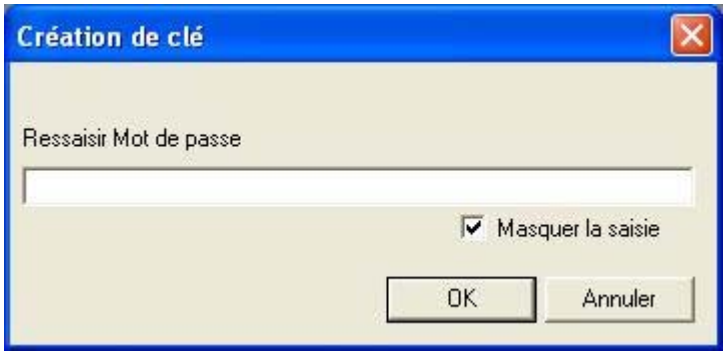


Si vous souhaitez quand même utiliser ce mot de passe cliquez sur le bouton « Oui » sinon cliquez sur le bouton « Non » pour revenir à l'écran précédent et recommencer.)

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

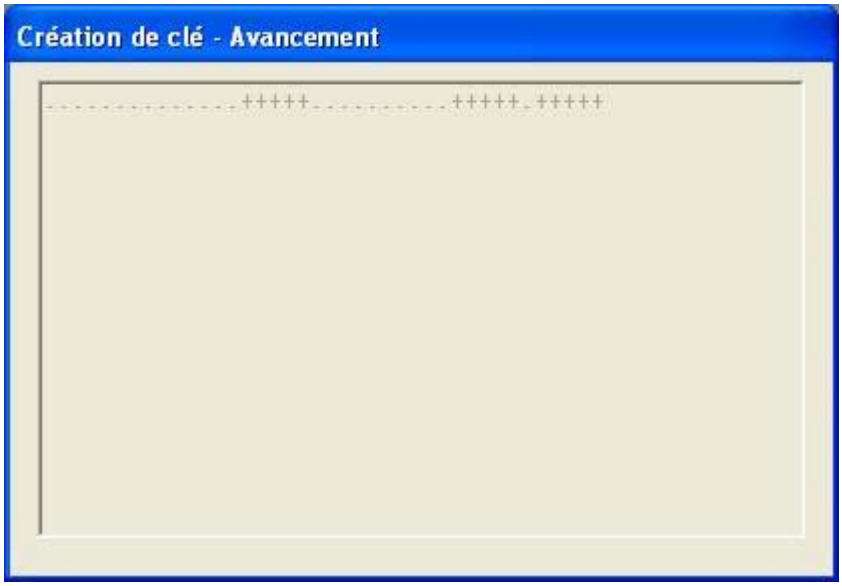
Si vous devez utiliser votre clé de chiffrement sur une autre machine installée différemment, cliquez sur le bouton « Non » pour revenir à l'écran précédent et recommencer, sinon cliquez sur le bouton « Oui ».)

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



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

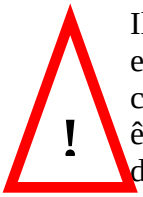
L'écran suivant apparaît pendant la génération des clés. Remuez votre souris, frappez des touches du clavier … pour augmenter le hasard dans la génération des clés (et passer le temps).



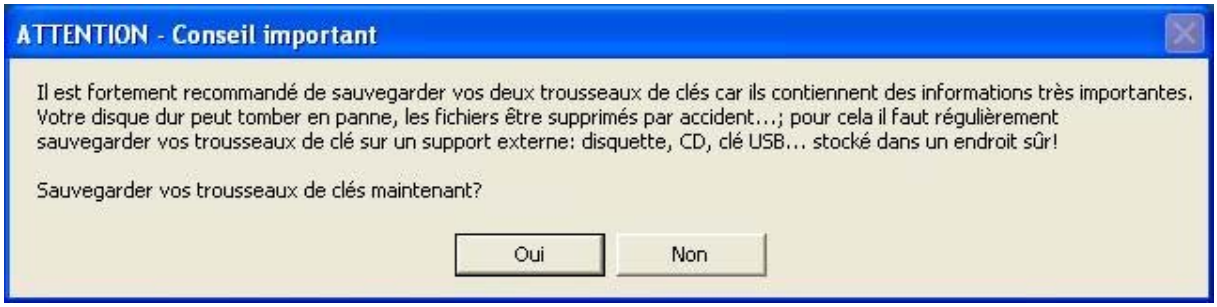
Lorsque la génération des clés est terminée, l'écran suivant d'avertissement apparaît pour vous le signaler.

Cliquez sur le bouton « OK ».

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

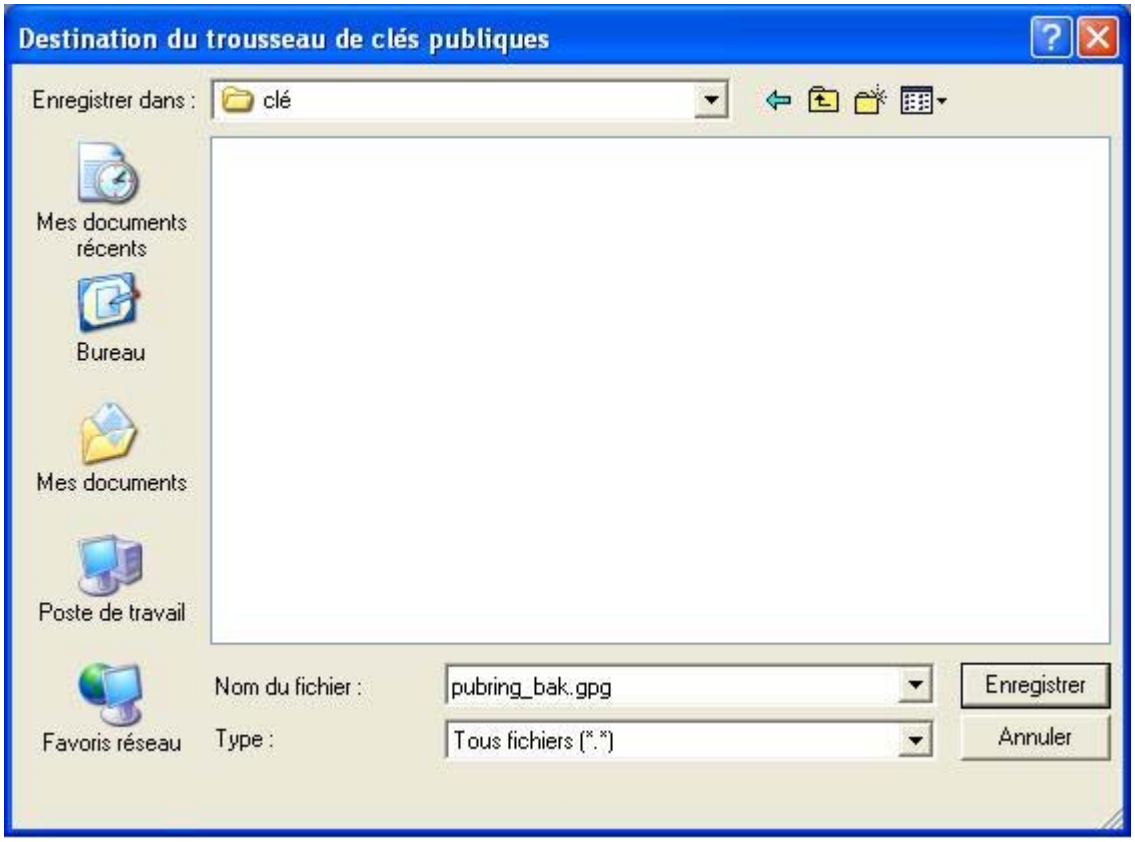


Il est indispensable d'effectuer une sauvegarde du bi-clé de chiffrement car sa perte empêchera tout déchiffrement des documents ayant été émis ou reçus. Le support comportant ce bi-clé doit également être conservé dans un emplacement sûr. Ce peut être un espace réservé à cet utilisateur sur un disque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



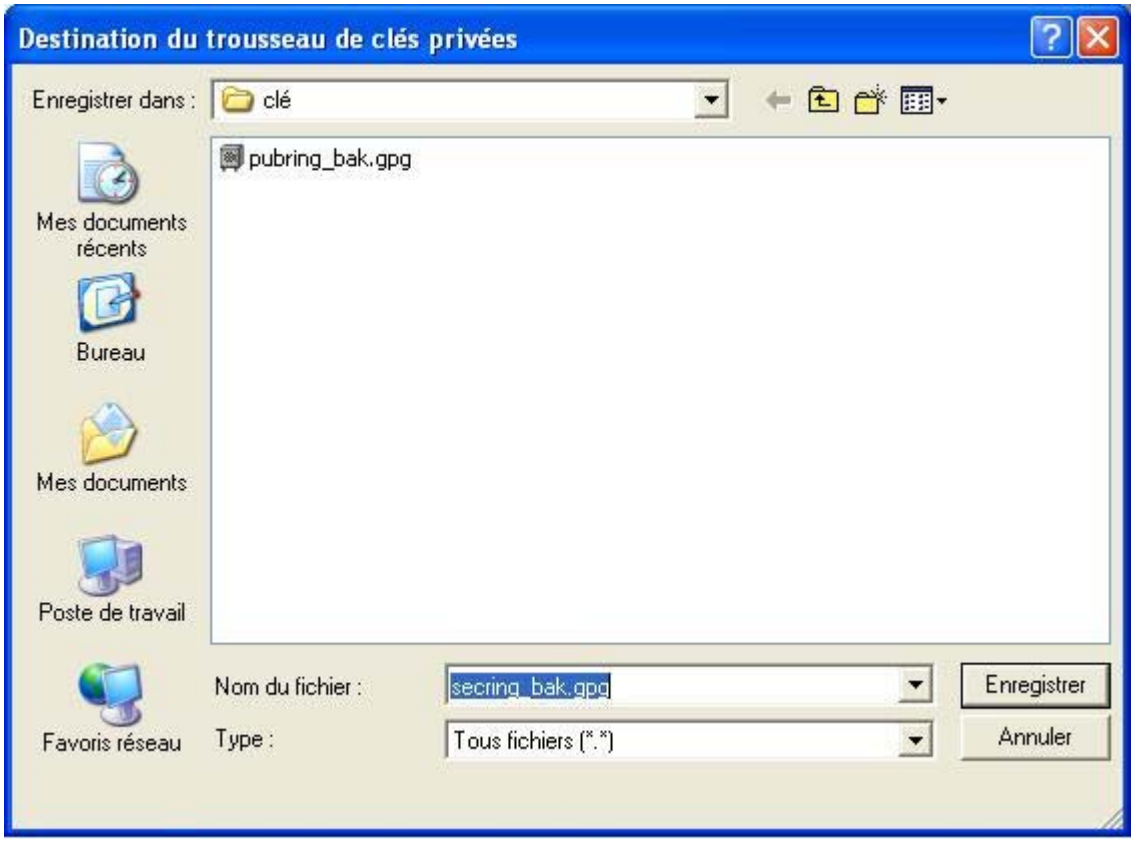
Cliquez sur le bouton « Oui ». Un écran apparaît pour vous permettre de choisir le nom et l'emplacement de sauvegarde de votre clé publique. Choisir de l'enregistrer sur un support externe à votre PC qui ne doit pas être accessible à tous (clé USB, disquette rangée sous clé, disque réseau réservé…) car il peut permettre de pirater plus facilement votre clef privée.

Deux fichiers vont être enregistrés : pubring_back.gpg pour la clé publique et secring_back.gpg pour vos bi-clés (clé publique et clé privée). Il est recommandé de ne pas modifier ces noms.



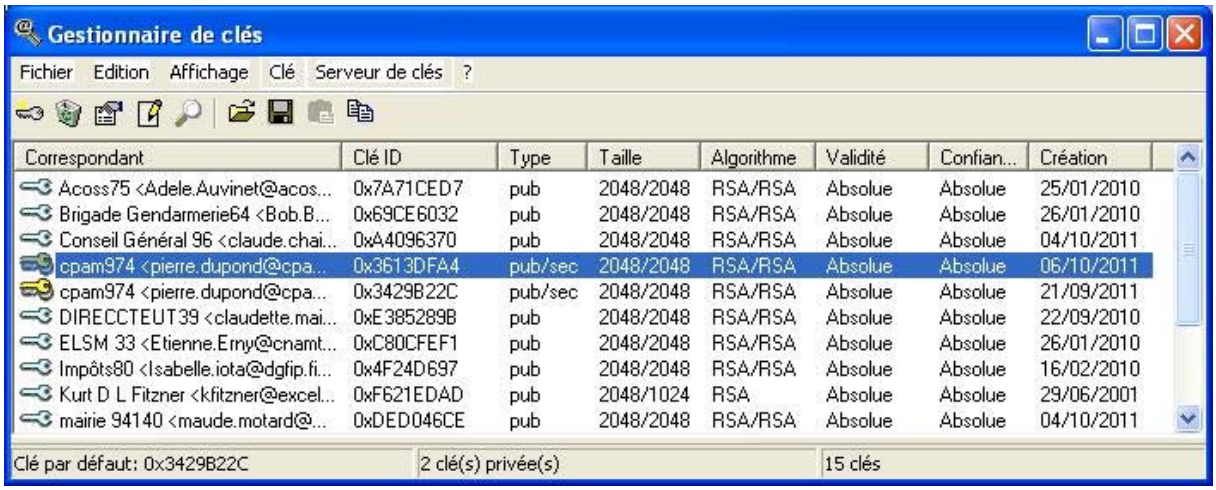
Puis cliquez sur le bouton « Enregistrer ».

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



Puis cliquez sur le bouton « Enregistrer ».

Le « Gestionnaire de clés » vous montre alors le résultat de la création du nouveau bi-clé



Identifiez la nouvelle clé avec sa date de création (qui est normalement celle du jour).

Faites un « Clic droit » sur la clé. Le menu contextuel suivant apparaît alors.

Choisir la commande « Clé signature par défaut ». Ca y est, votre nouvelle clé est active (N.B. Il conviendra également de la sélectionner dans GPGee lors de votre prochaine utilisation).

Les documents chiffrés avec votre ancienne clé publique ne pourront pas être déchiffrés avec le nouveau bi-clé. Il faut immédiatement envoyez votre nouvelle clé publique à vos interlocuteurs, comme cela est expliqué au paragraphe « D – 2. Transmission à vos partenaires de votre clé publique~~D – 2. Transmission aux partenaires de votre clé publique~~ ».

Il conviendra par la suite de supprimer de votre trousseau votre ancien bi-clé (car il en comporte maintenant deux).

F – 5 Supprimer une clé publique (ou un bi-clé)

- **Dans quel cas :**

Une clé publique doit être supprimée lorsque la nouvelle liste des clés transmise ne la comporte plus.

Ce qui peut être lié :

- ✓ au départ de l'agent
- ✓ au changement de bi-clé d'une personne

Les documents signés avec une clé publique supprimée continuent à être déchiffrés. Toutefois un message d'alerte s'affichera.

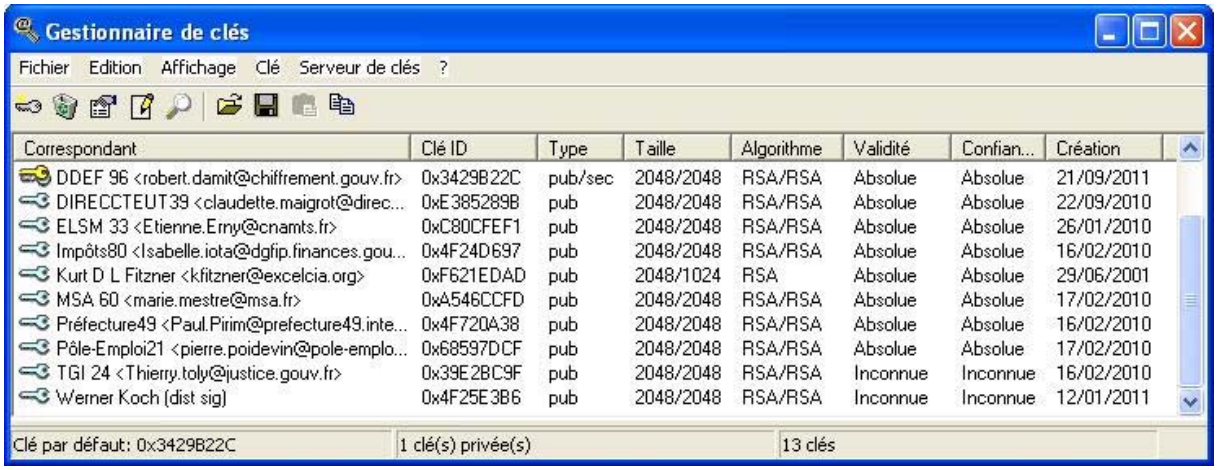
Un bi-clé ne doit être supprimé que si un nouveau bi-clé a être créé et que l'ancien ne doit plus pouvoir être utilisé). Si un bi-clé est supprimé, vous serez alors incapable de déchiffrer les documents chiffrés avec cette clé (par vous même ou reçu de vos correspondants).

- **Déroulement**

Lancer le logiciel WinPT s'il n'est pas déjà en service.

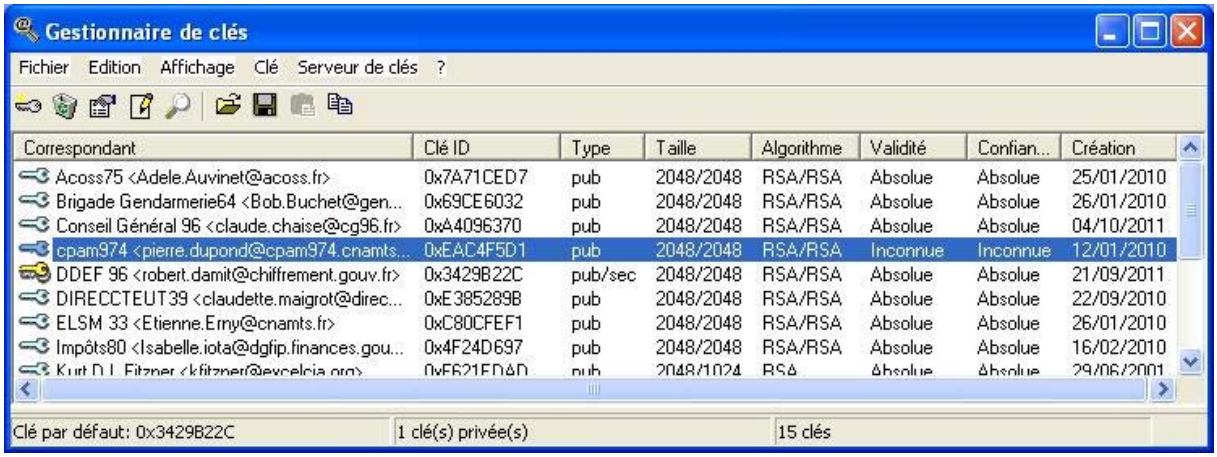
Dans le menu de WinPT sélectionnez le « Gestionnaire de clés ». Le « Gestionnaire de clés » s'ouvre alors.

Identifier la clé (ou le bi-clé) à supprimer et sélectionnez là avec un simple clic (gauche) sur sa ligne.



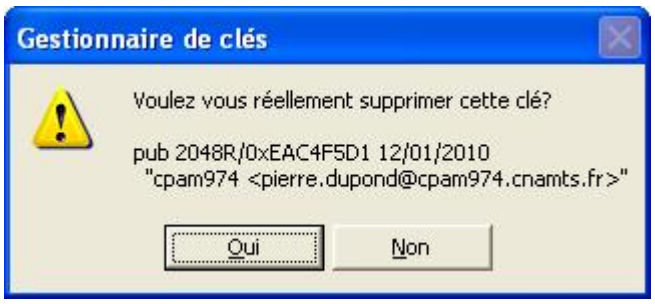
La clé à supprimer peut être repérée par son identifiant (2 clés pour le même correspondant pouvant se trouver dans votre trousseau). Si c'est un bi-clé repérez le avec sa date de création.

Une fois sélectionnée le fond de la ligne devient bleu.

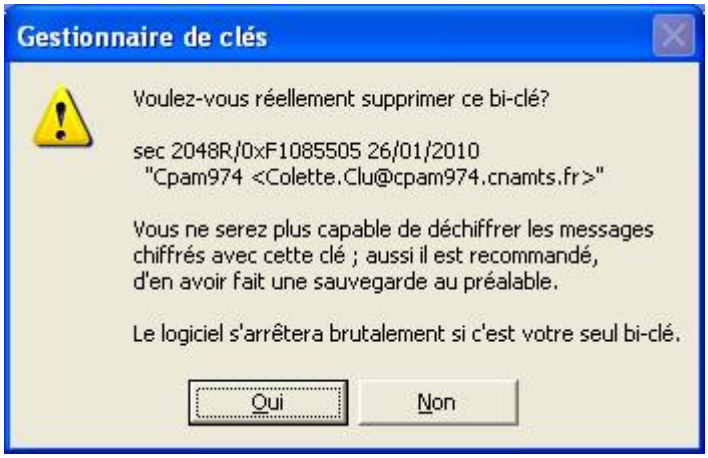


Appuyer sur la touche Suppr (ou Del) de votre clavier (vous pouvez également cliquer sur le bouton représentant une corbeille « Supprimer la clé du trousseau » dans la barre des boutons).

Un écran apparaît vous demandant de confirmer la demande de suppression de la clé



ou du bi-clé



Confirmez en cliquant sur « Oui ».

○○○

ANNEXES

Eléments supplémentaire sur le chiffrement asymétrique

Archive chiffrée pour de multiples destinataires

Lenteur du chiffrement asymétrique

Une des règles de la cryptologie moderne est que la confidentialité ne provient pas du procédé de chiffrement utilisé, celui-ci pouvant être divulgué, mais de la clé de chiffrement (ou mot de passe) qu'il utilise.

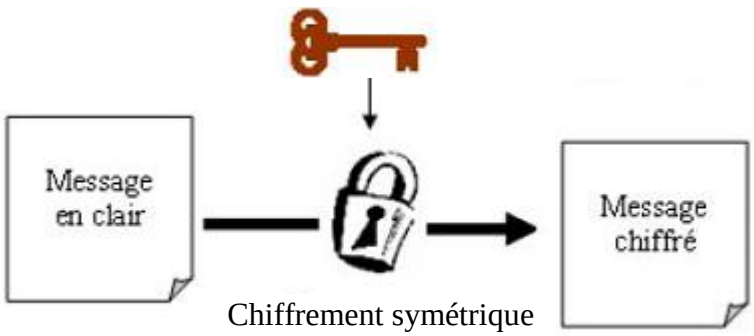
Un des principaux inconvénients du procédé de chiffrement asymétrique, qui a été sommairement décrit plus haut, est que pour ne pas pouvoir déduire la clé privée de la clé publique, il faut que celle-ci soit très longue (afin que le nombre de combinaisons possibles soit très long à tester pour ceux qui voudraient découvrir la clé privée). Les clés utilisées sont pour cela des clés de type RSA de 2048 bits de longueur.

Un autre inconvénient lié du chiffrement asymétrique est la lenteur du procédé de chiffrement et de déchiffrement.

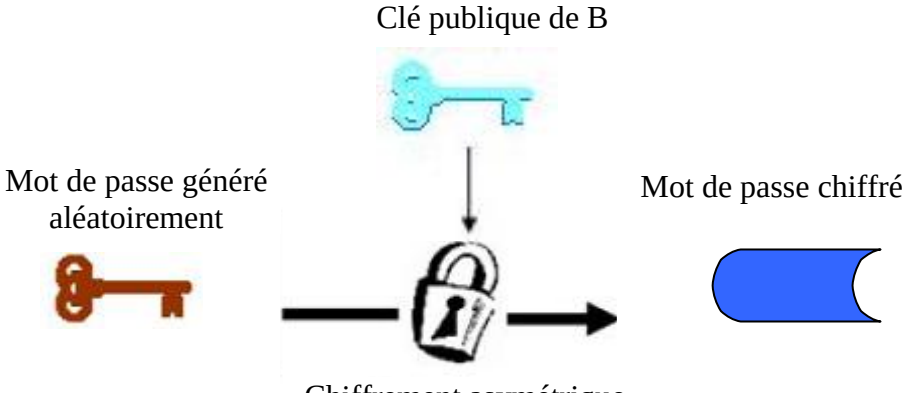
Combinaison avec le procédé de chiffrement symétrique

De ce fait, pour disposer d'un procédé commodément utilisable, la protection par chiffrement asymétrique utilise un chiffrement symétrique du document à protéger. Ce chiffrement symétrique est réalisé car il est beaucoup plus rapide (jusque 1 000 fois) et très résistant dès que le « mot de passe » (ou clé secrète) utilisé est suffisamment long.

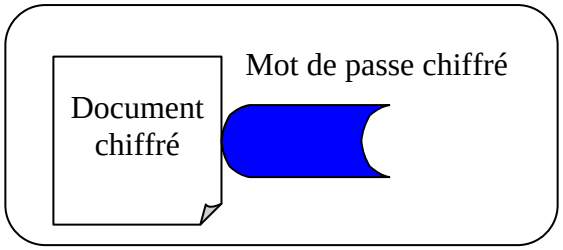
Le déroulement de l'opération de chiffrement est alors le suivant : un « mot de passe » de grande longueur (256 bits) est généré aléatoirement. Ce mot de passe est utilisé pour procéder au chiffrement symétrique du document et créer ainsi un document chiffré.



Le mot de passe, qui est beaucoup moins grand que le document, est lui alors chiffré de manière asymétrique avec la clé publique de B.

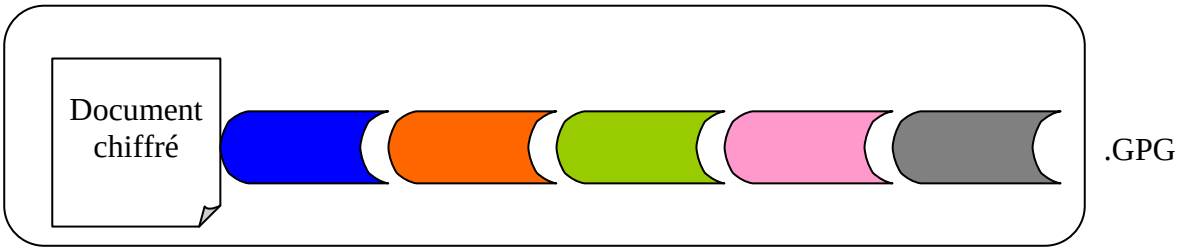


Ce mot de passe chiffré est alors ajouté au document chiffré pour composer une archive chiffrée :



Fichier chiffré pour plusieurs destinataires

Si cette archive est destinée à plusieurs destinataires, il est ajouté autant de fois le même mot de passe chiffré avec les clés publiques des différents destinataires. Le volume de cette archive augmente très peu avec le nombre de destinataires (quelques centaines d'octets par signature).



C'est cette archive qui est envoyée aux différents destinataires. Le logiciel GPG déchiffrera le mot de passe chiffré avec la clé privée du destinataire afin de pouvoir ensuite déchiffrer, avec le procédé symétrique, le document avec ce mot de passe.

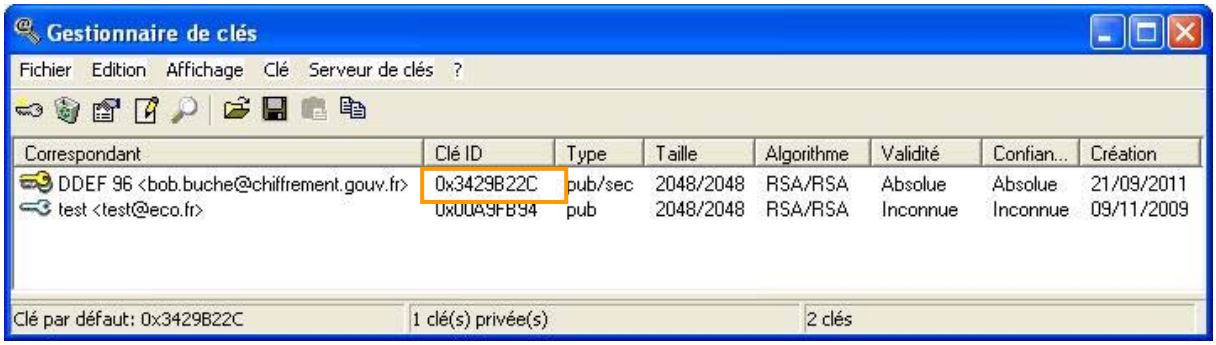
Clés de chiffrement et de signature

Il y a, pour la configuration retenue, en réalité 4 clés dans le bi-clé de l'utilisateur, 2 clés publiques et 2 clés privées, même si on n'en voit qu'une pour chaque. Il faut bien comprendre d'abord qu'une clé publique et sa clé privée constituent un couple de clé en théorie déductibles l'une de l'autre. Les 4 clés constituent en fait ici 2 bi-clés.

En fait par mesure de sécurité le chiffrement et la signature sont réalisés avec deux bi-clés différents pour permettre que si l'un des 2 bi-clés était compromis (cassé par un hackeur), le second bi-clé, lui, puisse avoir une certaine chance d'être intact et ainsi empêcher que le hackeur puisse complètement usurper votre bi-clé pour se faire passer pour vous.

Cette situation peut s'observer dans WinPT à différents endroits.

Au niveau du trousseau de clés :



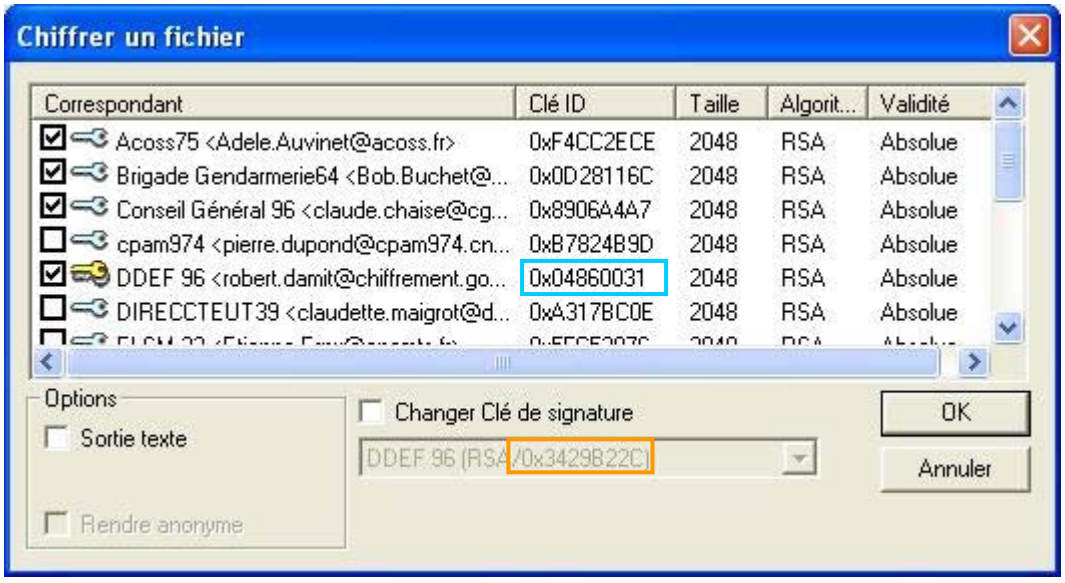
Vous pouvez observer que même pour la clé publique on voit apparaître deux tailles de clé (2048/2048) ainsi que le type de clé (RSA/RSA) qui est répété deux fois. C'est car en fait il y a 2 bi-clés différents.

En regardant le détail d'une clé au niveau de l'éditeur de clé, pour une clé publique comme pour un bi-clé entier (clé publique et clé privée) on observe cela :

Dans l'écran du haut on voit apparaître 2 lignes. Une ligne par bi-clé. L'identifiant du premier bi-clé est celui repris pour l'ensemble dans le gestionnaire de clés. Cependant, comme l'indique les croix dans les dernières colonnes :

- le premier bi-clé sert à certifier (C) et signer (S) ;
- le second bi-clé sert lui à chiffrer (E : Encrypt).

Dans l'écran de chiffrement suivant de WinPT, on peut noter que le Clé ID donné est celui de la clé de chiffrement et pas celui de la clé signature (contrairement au gestionnaire de clés). Cela peut se voir pour le bi-clé de « DDEF 96 » qui apparaît également comme Clé de signature avec un clé ID différent.



○○○

Foire aux questions

Questions :

- **Je n'y connais rien. Que dois-je faire ?**
- **Je n'ai pas de clé privée (secrète, bi-clé) ou de clés publiques que dois-je faire ?**
- **Je n'ai pas GPGee sur mon poste, est-ce normal ?**
- **Lorsque je clique droit sur un document et sur GPGee dans le menu contextuel il ne se passe rien ?**
- **WinPT s'est planté. Que faut il faire ?**
- **Sur mon poste la version de WinPT est la 1.4.3a et pas la 1.4.3d, est-ce normal ?**
- **GPGee me donne un message incompréhensible : Echec de l'opération : Internal GPG Problem … ?**
- **Avec GPGee j'obtiens un message d'erreur incompréhensible : EaccessViolation**
- **GPGee m'affiche un écran sans clés**
- **Il me manque une clé publique dans l'affichage de GPGee**
- **J'ai perdu ma clé de signature et mes groupes de clés dans GPGee**
- **J'obtiens une « coche » orange dans GPGee et un message d'alerte, pourquoi ?**
- **J'ai beau double-cliquer sur le document chiffré reçu il ne se passe rien ?**
- **J'obtiens un format de signature SHA 1 dans GPGee et pas SHA 256, pourquoi ?**
- **Comment être sûr que je transmets bien ma clé publique et pas ma clé privée ?**
- **Comment faire pour transmettre l'annuaire des clés publiques de mon poste à une autre personne ?**
- **Est-ce que je peux déchiffrer des documents chiffrés avec d'autres logiciels de chiffrement ?**
- **Est-ce que je peux déchiffrer un document .pgp (et pas .gpg) ?**
- **Comment déchiffrer un document qui comporte plusieurs extensions de chiffrement : exemple.doc.gpg.gpg ?**
- **J'ai changé d'adresse mel, comment modifier ma clé de chiffrement ?**
- **Je dois copier mon trousseau de clé sur une nouvelle machine. Comment faire ?**
- **Le fichier que j'obtiens après déchiffrement n'a pas un format reconnu par Windows ?**
- **J'ai déjà un fichier du même nom dans le dossier. Comment ne pas l'écraser en déchiffrant ou en chiffrant ?**
- **Le mel que j'ai reçu semble chiffré et n'a pas de pièce jointe ?**
- **Comment est-ce que je peux déchiffrer un « message PGP » inséré dans le corps du mel ?**
- **J'ai reçu une clé publique mais celle-ci n'est pas une pièce jointe du mel, elle semble insérée dedans. Comment la récupérer ?**
- **J'ai beau double cliquer sur la clé publique reçue il ne se passe rien ?**
- **Lorsque je double-clique sur la clé publique pourquoi ai-je un message d'erreur ?**
- **La clé publique que j'ai importée ne s'affiche pas dans WinPT ?**
- **WinPT m'indique un nombre de clés privées supérieur à celles qui apparaissent**
- **J'ai déjà importé des clés publiques. Si je réimporte les mêmes clés vont-elles se trouver en double dans le « Gestionnaire de clés » de WinPT ?**
- **J'obtiens des messages d'alerte que je ne connais pas, pourquoi ?**
- **Je n'arrive pas à déchiffrer le .gpg reçu. Pourquoi ?**

Réponses :

- **Je n'y connais rien. Que dois-je faire ?**

Il faut commencer par installer les logiciels de chiffrement prévus (ou faire installer). Ensuite regardez la plaquette « Logiciel de chiffrement GPG » et, pour approfondir, consultez le mode d'emploi (70 pages).

- **Je n'ai pas de clé privée (secrète, bi-clé) ou de clés publiques que dois-je faire ?**

Votre bi-clé (votre clé privée et sa clé publique) doit normalement être créé lors de l'installation des logiciels. Si cela n'a pas été fait recontactez la personne qui les a installés. Il y a des consignes à respecter lors de la création de votre bi-clé, pour son niveau de sécurité et pour qu'elle soit facilement repérable par son nom.
Concernant les clés publiques de vos correspondants, vous devez échanger avec eux vos clés publiques (mais cela peut être centralisé). Il est nécessaire de contrôler que les clés publiques importées dans le logiciel sont bien celles attendues et de leur « attribuer votre confiance » (cf chapitre D-3 de ce mode d'emploi).

- **Je n'ai pas GPGee sur mon poste, est-ce normal ?**

La présence de GPGee se voit dans le menu contextuel qui apparaît par un clic-droit sur un document. Si vous utilisez un OS 64 bits une installation spécifique était auparavant nécessaire pour utiliser GPGee. Maintenant un adaptateur GPGee64 doit être installé et apparaît dans le menu contextuel. Il est possible de n'utiliser que WinPT pour toutes les opérations. Les parties de ce mode d'emploi concernant GPGee ne sont dans ce cas pas pertinentes. La présentation des fonctions équivalentes de WinPT est faite pour cette situation.

- **Lorsque je clique droit sur un document et sur GPGee dans le menu contextuel il ne se passe rien ?**

Si GPGee est bien installé sur votre poste, il est possible que des opérations aient conduit à l'arrêt intempestif de ce logiciel (cet événement est normalement rare). Il faut fermer puis ré-ouvrir la fenêtre de l'explorateur ou alors redémarrer votre ordinateur pour relancer GPGee.
Si vous êtes sur un OS 64 bits, et qu'il s'agit de GPGee64, il convient de relever qu'actuellement, si vous traitez un document sur le bureau, la fonction apparaît mais ne fonctionne pas. Elle ne fonctionne pour l'instant que dans les dossiers de l'explorateur windows.

- **WinPT s'est planté. Que faut il faire ?**

Il est possible que des opérations aient conduit à l'arrêt intempestif de ce logiciel (cet événement est normalement rare). Il suffit de redémarrer WinPT, comme expliqué en E-3 dans ce mode d'emploi. Si cela ne suffit pas redémarrer alors l'ordinateur.

- **Sur mon poste la version de WinPT est la 1.4.3a et pas la 1.4.3d ?**

Les nouvelles versions corrigent des bugs et quelques failles de sécurité. Aussi il est préférable d'utiliser les nouvelles versions indiquées ici.

- **GPGee me donne un message incompréhensible : Echec de l'opération : Internal GPG Problem … ?**

Il n' a pas été possible de modifier ce message pour le rendre plus compréhensible :

En général, celui-ci apparaît car vous avez tenté de chiffrer un document alors que celui-ci est toujours ouvert sur votre poste de travail. Veuillez bien enregistrer et fermer le document avant d'essayer de le signer&chiffrer.

Il peut aussi apparaître lorsque vous tenter d'utiliser la clé d'un destinataire auquel vous n'avez pas accordé votre confiance au préalable (la « Validité » et la « Confiance » ne sont pas « Absolue »). L'étape de validation est décrite à la fin du chapitre D-3 de ce mode d'emploi.

Si ce n'est pas la cas signalez le problème. Eventuellement réessayez après avoir redémarré votre poste.

- **Avec GPGee j'obtiens un message d'erreur incompréhensible : EAccessViolation**

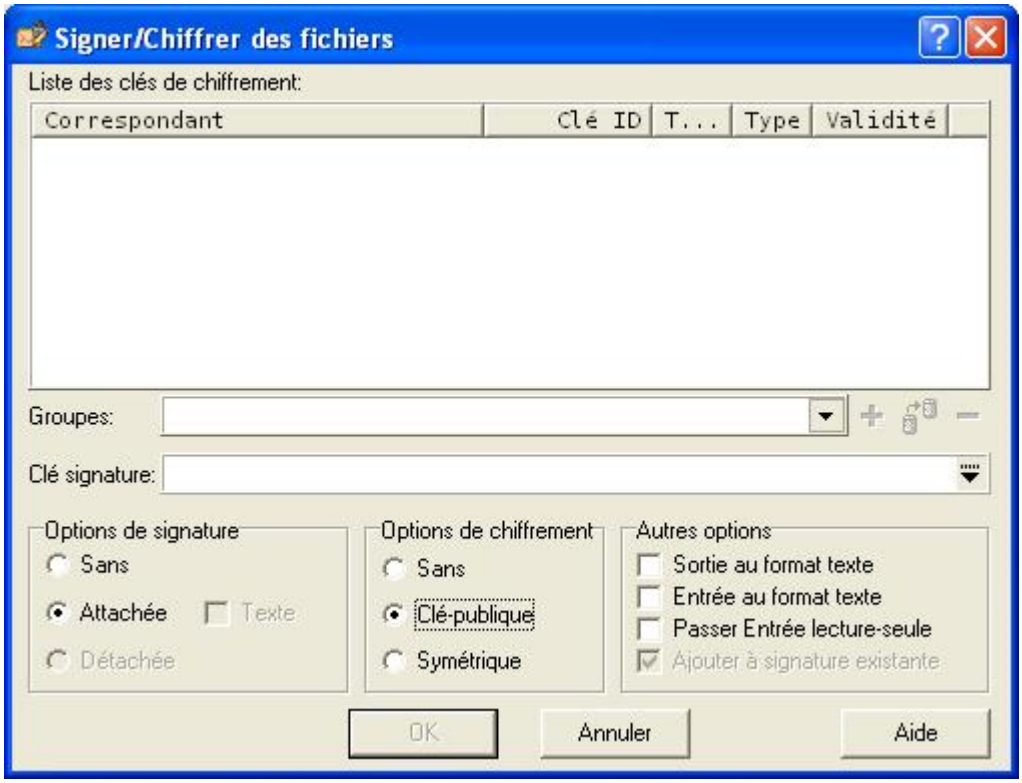
Les messages d'erreur suivants peuvent apparaître avec GPGee.

La seule cause connue est le fait d'avoir ouvert simultanément 2 sessions GPGee dans des fenêtres différentes de l'explorateur Windows. Ce logiciel ne permet pas de l'utiliser en même temps avec deux instances. Aussi veillez à n'en lancer qu'une seule instance.

Si ce n'est pas votre cas signalez le problème. Eventuellement réessayez après avoir redémarré votre poste.

- **GPGee m'affiche un écran sans clés**

Il peut arriver que GPGee rencontre une difficulté de lecture du trousseau de clé. Dans ce cas vous obtenez un écran sans aucune clé. Si vous fermez et ré-ouvrez GPGee le problème peut persister.



Essayez alors de fermer et rouvrir la fenêtre de l'explorateur windows dans laquelle se trouve le document à chiffrer avant de refaire un clic-droit sur le document pour lancer GPGee. Si cela ne résout pas la difficulté et que votre trousseau n'est pas vide, redémarrez l'ordinateur ou vérifiez l'emplacement par défaut du trousseau de clé (si nécessaire modifiez là avec le sous-menu « Configurer » de GPGee).

Si le problème persiste, il est peut être lié au fait que le logiciel GPGee n'est pas correctement installé (notamment, les liens vers les trousseaux de clés, l'application GPG.exe ou gpg.conf ne sont pas corrects en base de registre). Si c'est le lien vers GPG.exe aucun mode de (dé)chiffrement ne fonctionne même si les clés peuvent apparaître par moment. Vous pouvez inscrire en dur les bons liens dans le sous-menu « Configurer » de GPGee, mais il est recommandé de désinstaller les 3 logiciels, de bien nettoyer toutes les traces de « GPGee » dans la base de registre (de mauvais liens créent la perturbation) et de réinstaller les logiciels.

- **Il me manque une clé publique dans l'affichage de GPGee**

GPGee ne montre pas les clés révoquées, périmées ou désactivées, alors qu'elles sont visibles dans WinPT. Sinon, la version 1.4.2 de GPGee a été corrigée pour ne plus oublier d'afficher des clés valides. Si vous l'observiez encore alors que vous avez la version 1.4.2 (cliquez sur Aide pour voir la version installée), merci de nous le signaler pour déterminer quelles autres raisons de ce dysfonctionnement peuvent exister.

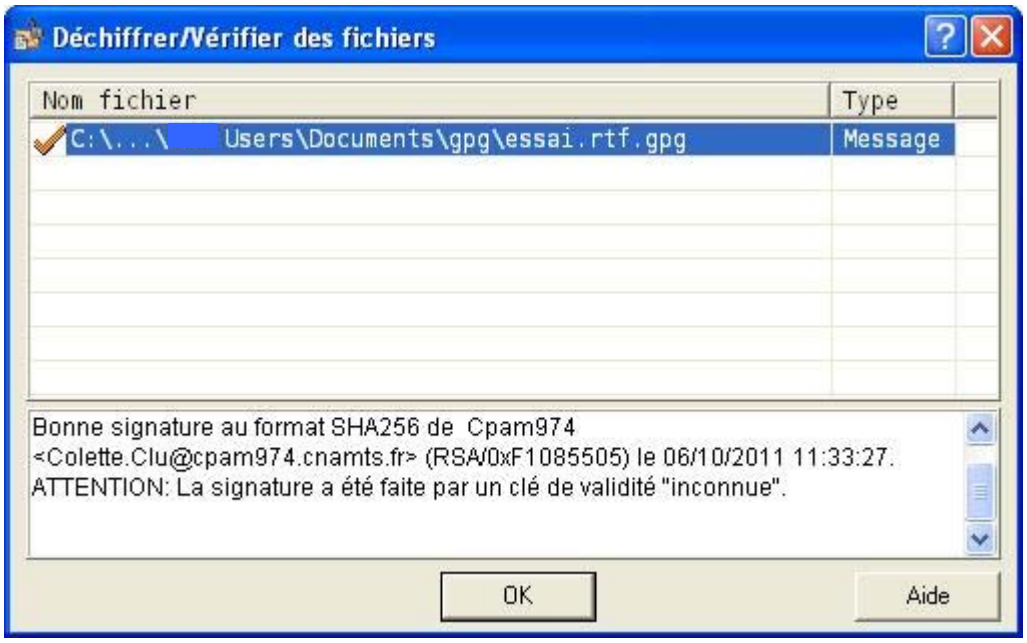
- **J'ai perdu ma clé de signature et mes groupes de clés dans GPGee**

Si vous êtes passé d'une version précédente à la version 1.4.2 de GPGee il est normal que ces informations aient disparues. La nouvelle version de GPGee identifie les clés avec une meilleure sécurité qui empêchait de conserver les éléments précédents. Vous devez recréer vos groupes suite à la migration. La clé de signature sera mémorisée dès que vous l'utiliserez.

- **J'obtiens une « coche » orange dans GPGee et un message d'alerte, pourquoi ?**

Si vous obtenez le résultat suivant dans GPGee, c'est que la clé publique de l'émetteur a bien été importée dans votre trousseau de clés, mais qu'il ne lui a pas été attribué de niveau de confiance (la vérification que la clé est bien celle du correspondant a-t'elle bien été

réalisée ?). Se référer au chapitre D-3 de ce mode d'emploi pour revoir les actions nécessaires lors de l'import d'une clé publique. Sinon c'est une clé qui ne devrait pas figurer dans votre trousseau de clés publiques.

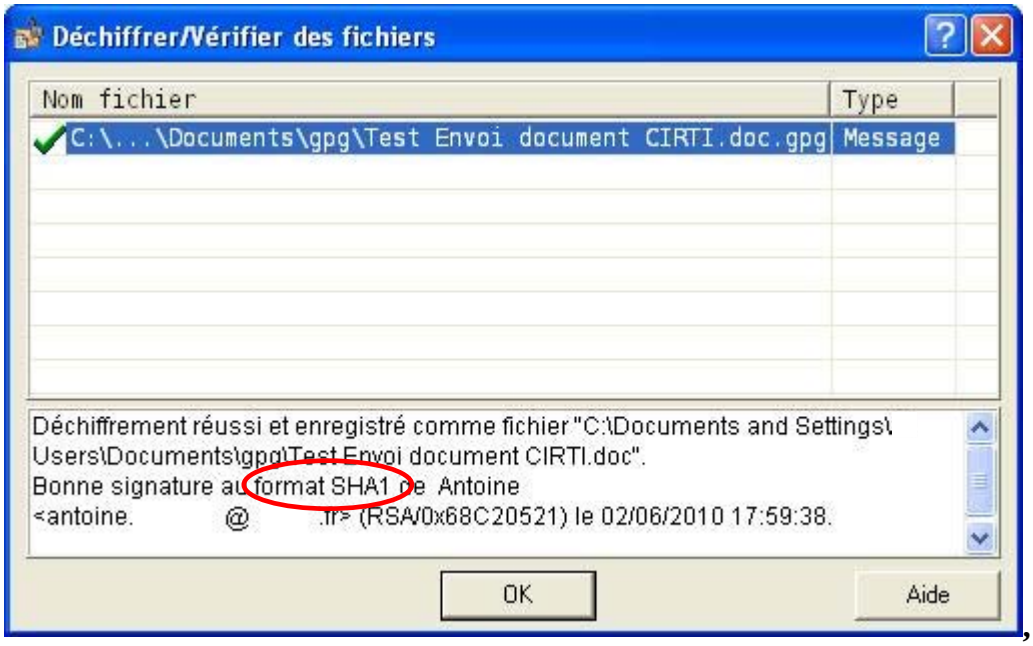


- **J'ai beau double-cliquer sur le document chiffré reçu il ne se passe rien ?**

Si le nom du ficher comporte deux tirets (signe moins, tiret de la touche 6) consécutifs « -- » il n'est pas ouvert directement par WinPT. Dans ce cas il suffit de renommer le fichier avec un nom plus court, en supprimant au moins l'un des deux tirets, pour qu'il soit bien traité (et sans enlever la double extension .xxx.gpg).

- **J'obtiens un format de signature SHA 1 dans GPGee et pas SHA 256 :**

Si vous obtenez le résultat suivant dans GPGee, avec un format de signature qui n'est pas SHA 256 :



, c'est que l'émetteur n'utilise pas le fichier de configuration prévu. Soit c'est une tentative d'usurpation, soit c'est une erreur dans la configuration installée sur son poste (dans ce cas le niveau de protection des documents envoyés par lui est insuffisant). Contactez l'émetteur pour déterminer la cause de cette situation et faire prendre les mesures nécessaires.

- **Comment être sûr que je transmets bien ma clé publique et pas ma clé privée ?**

Lorsque WinPT vous propose d'enregistrer votre clé privée, il met la terminaison _sec.asc (sec pour clé secrète). Si vous ne modifiez pas la dénomination standard proposée vos clés, sous forme d'un fichier informatique, se distinguent alors simplement par leur nom (et aussi par leur taille en octets) :

- nom.asc : clé publique (taille d'environ 2 Ko)
- nom_sec.asc : bi-clé (clé privée + clé publique, ce qui donne une taille d'environ 4 Ko)

- **Comment faire pour transmettre l'annuaire des clés publiques de mon poste à une autre personne ?**

Au moins deux méthodes différentes permettent de disposer d'un fichier comportant l'ensemble des clés publiques d'un trousseau, notamment pour le diffuser à d'autres utilisateurs.

- Une méthode consiste à récupérer l'archive de sauvegarde « pubring-bak-n.gpg » présentée dans le § D-4.

- Une autre méthode consiste, dans le gestionnaire de clé de WinPT, à sélectionner l'ensemble des clés (en enfonçant la touche « majuscule » :⇧ pour tout sélectionner) et à cliquer ensuite sur le bouton « Exporter clé publique » représenté par l'icône  . Il vous sera alors proposé d'enregistrer l'ensemble des clés publique dans un fichier : Exported_GPG_Keys.asc.

Vous pouvez ensuite envoyer ce fichier par mel. Dans les deux cas il suffit de double-cliquer sur ces fichiers pour importer les clés via WinPT.

- **Est-ce que je peux déchiffrer des document chiffrés avec d'autres logiciels de chiffrement ?**

Ces logiciels peuvent normalement déchiffrer tous les document chiffrés au format OpenPGP, ainsi que les documents .pgp (un paramétrage peut cependant être nécessaire pour cela). Il convient cependant que le document ait bien une provenance sûre avant d'essayer de le déchiffrer. D'autres formats de documents chiffrés existent qui ne peuvent pas être déchiffrés.

- **Est-ce que je peux déchiffrer un document .pgp (et pas .gpg) ?**

Si vous utilisez GPGee, même si ce fichier n'est pas représenté avec l'icône  , faite un clic-droit dessus comme avec un document .gpg. Le déchiffrement se déroulera de la même façon. Avec WinPT il faut le déchiffrer en l'ouvrant depuis le « gestionnaire de fichiers ».

- **Comment déchiffrer un document qui comporte plusieurs extensions de chiffrement : document.doc.gpg.gpg ?**

Un tel document **document.doc.gpg.gpg** a été chiffré plusieurs fois successivement (ici 2 fois). Chaque opération de chiffrement a ajouté une extension .gpg. Les modes opératoires qui vous ont été présentés ne vous permettent pas de réaliser un tel fichier. Pour le déchiffrer il vous faudra le déchiffrer successivement autant de fois (2 fois dans l'exemple indiqué) avec les méthodes normales. Une première fois pour obtenir **document.doc.gpg**, puis enfin **document.doc.**

- **J'ai changé d'adresse mel, comment modifier ma clé de chiffrement ?**

En cas de besoin de changement des informations indiquées dans votre clé, la meilleure solution est de vous créer un nouveau bi-clé de chiffrement, comme cela est expliqué au chapitre F4, en saisissant les bonnes informations. Vous diffuserez ensuite la nouvelle clé

publique à tous vos partenaires en les alertant du changement. Il conviendra, par la suite (pas immédiatement), de supprimer de votre trousseau votre ancien bi-clé.

- **Je dois copier mon trousseau de clé sur une nouvelle machine. Comment faire ?**

Dans cette situation, vous voulez tout recopier : votre bi-clé et les clés publiques. Si cela ne concerne que les clés publiques référez vous à la question : **Comment faire pour transmettre l'annuaire des clés publiques de mon poste à une autre personne ?**
Sinon, la méthode la plus simple consiste, après l'installation des logiciels et avant d'avoir démarrer WinPT (qui sinon va faire créer un nouveau bi-clé pour l'utilisateur), à faire une copie des fichiers :

trustdb.gpg
pubring.gpg
secring.gpg

Du dossier : C:\Documents and Settings\ "user" \Application Data\gnupg, vers le dossier équivalent de l'autre machine (« user » correspond à l'identification de l'utilisateur sur la machine).

- **Le fichier que j'obtiens après déchiffrement n'a pas un format reconnu par Windows ?**

Le format du fichier est reconnu par Windows avec l'extension du nom de fichier qui est constitué des 3 lettres (parfois plus), après le point à la fin du nom de fichier (ex : .doc ou .pdf). Le nom d'un document chiffré par GPG, est celui du document déchiffré auquel est rajouté l'extension .gpg après l'extension du document déchiffré. Document.doc devient ainsi Document.doc.gpg. Le déchiffrement produit normalement l'opération inverse. Si le format du fichier obtenu après déchiffrement n'est pas reconnu, c'est :

- soit que vous n'êtes pas équipé d'un logiciel capable de lire ce type de document ;
- soit que quelqu'un (vous ou l'expéditeur) à modifié l'extension qui figurait avant le .gpg. Il suffit généralement de la corriger sur le fichier déchiffré pour qu'il soit reconnu.

- **J'ai déjà un fichier du même nom dans le dossier. Comment ne pas l'écraser en déchiffrant ou en chiffrant ?**

En déchiffrant GPGee, comme WinPT vous avertiront et vous proposeront de donner un autre nom au fichier déchiffré.
Par contre lorsque vous chiffrez, si WinPT vous alertera dans une telle situation, GPGee ne le fera pas et remplacera d'office le .gpg existant. Avec GPGee il faut anticiper et si nécessire modifier les nom des documents au préalable.
Si vous modifiez le nom de fichier chiffré (ex. : Document**.doc.gpg)**, il ne faut pas modifier les 2 extensions (indiquées en gras) présentes à la fin du nom, mais uniquement le début (ex. : Nouveau_nom_de_document.doc.gpg).

- **Le mel que j'ai reçu semble chiffré et n'a pas de pièce jointe ?**

Dans certains cas le logiciel de chiffrement peut être interconnecté avec la messagerie et permet de chiffrer directement les messages et pas seulement un document informatique. Cette utilisation n'est cependant pas celle présentée ici. Il convient de demander à l'émetteur de vous retransmettre uniquement un pièce-jointe chiffrée et de ne pas chiffrer son mel.

- **J'ai reçu une clé publique mais celle-ci n'est pas une pièce jointe du mel, elle semble insérée dedans. Comment la récupérer ?**

Certaines configurations des messageries semblent parfois intégrer la pièce jointe (.asc ou .gpg), dans le corps du mel. Même si ce mode d'utilisation n'est pas celui normalement proposé, vous pouvez y récupérer la partie chiffrée et la traiter avec WinPT.
Ouvrez le message concerné et sélectionnez la partie chiffrée de :

- - - - - BEGIN PGP PUBLIC KEY BLOCK - - - - -

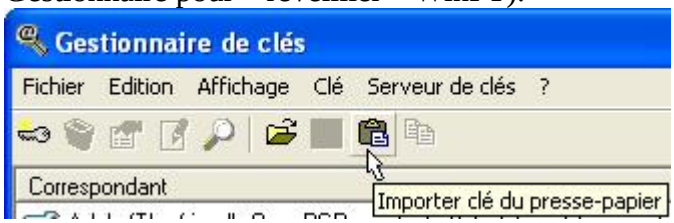
à

- - - - - END PGP PUBLIC KEY BLOCK - - - - -

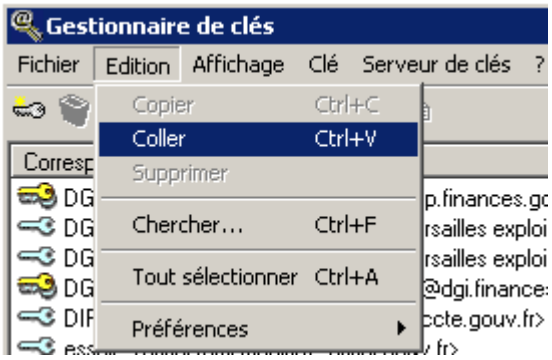
comme montré ci-dessous

Faites alors un « copier » (avec les touches « Ctrl » + « C »). La partie sélectionnée est alors ajoutée au presse papier Windows.

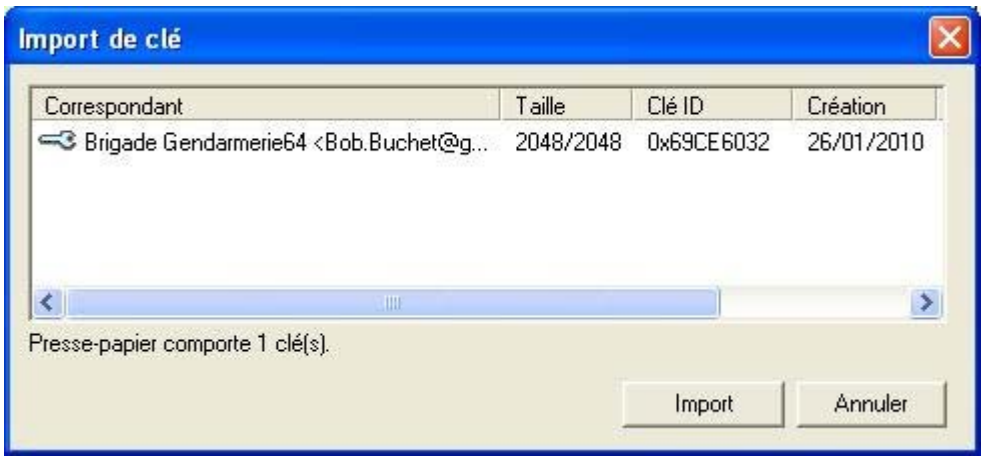
Cliquez alors sur l'icône de WinPT dans la barre des tâches (zone en bas à droite de l'écran comportant l'heure) pour ouvrir le Gestionnaire de clés. Cliquez alors sur le bouton « Importer clé du presse-papier » (si il n'est pas actif cliquez sur n'importe quelle clé du Gestionnaire pour « réveillller » WinPT).



Ou dans le menu « Edition » du Gestionnaire de clés choisissez la fonction « Coller » (ou en faisant « Ctrl » + « V »)



Vous obtenez alors la description de la clé reçue.



Et vous pouvez lancer son importation dans le « Gestionnaire de clés » en cliquant sur le bouton « Import ». Les opérations prévues pour un import de clé publique doivent ensuite être réalisées.

- **Comment est-ce que je peux déchiffrer un « message PGP » inséré dans le corps du mel ?**

Vous pouvez déchiffrer un **« message PGP »** qui se trouve dans le corps d'un mel avec la même méthode que celle indiquée pour une clé à la question : **J'ai reçu une clé publique mais celle-ci n'est pas une pièce jointe du mel, elle semble insérée dedans. Comment la récupérer ?**

Ouvrez le message concerné et sélectionnez le message chiffré de :

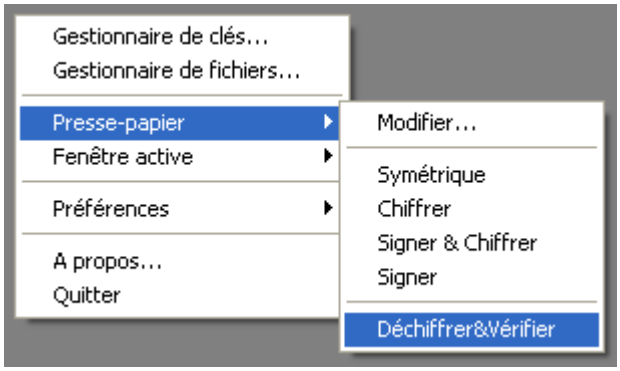
- - - - - BEGIN PGP MESSAGE - - - - -

à

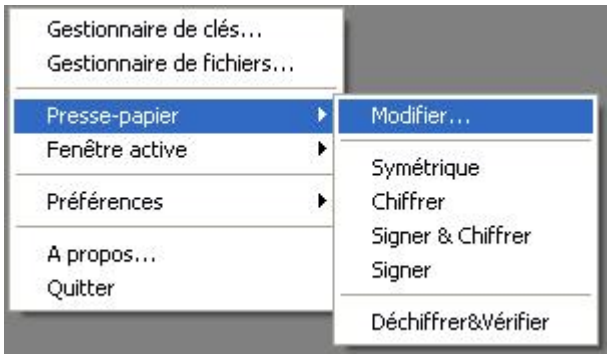
- - - - - END PGP MESSAGE - - - - -

Faites alors un « copier » (avec les touches « Ctrl » + « C »). La partie sélectionnée est alors ajoutée au presse papier.

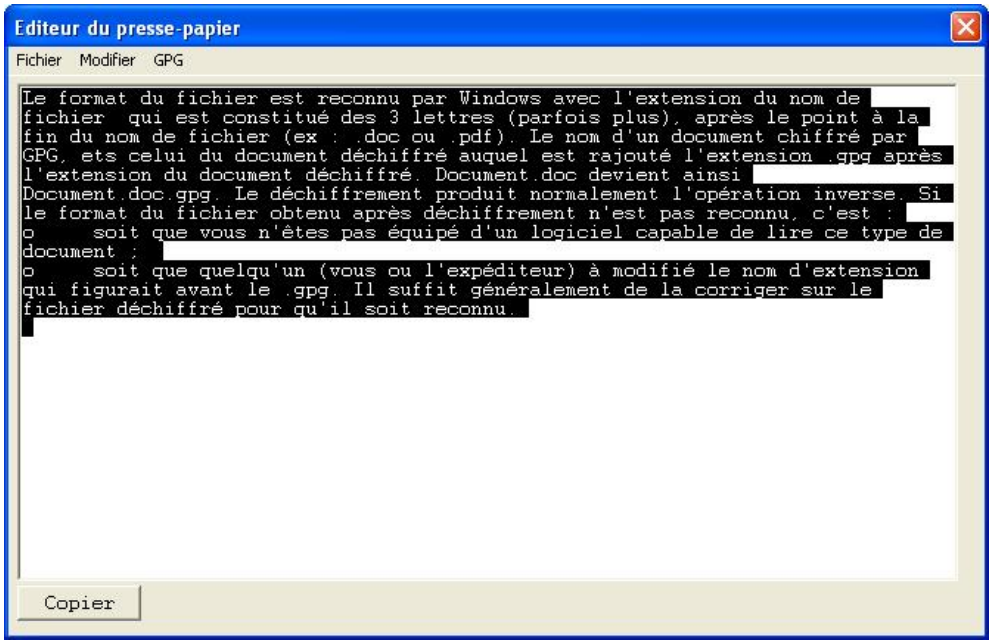
Cliquez alors sur l'icône de WinPT dans la barre des tâches (zone en bas à droite de l'écran comportant l'heure) pour ouvrir le sous-menu « Presse papier », puis la sous-fonction « déchiffrerVérifier ».



Vous obtenez les écrans habituels de WinPT pour saisir votre mot de passe. Collez le contenu déchiffré dans un éditeur de texte (Word…) pour le lire (« Ctrl » + « V ») ou lisez-le directement dans WinPT. Pour cela, cliquez sur l'icône de WinPT dans la barre des tâches (zone en bas à droite de l'écran comportant l'heure) pour ouvrir son menu et choisissez la fonction « Presse papier », puis la sous-fonction « Modifier ».



Vous accédez alors à « l'éditeur du presse-papier » qui vous montre le texte déchiffré présent dans le presse papier.



- **J'ai beau double-cliquer sur la clé publique reçue il ne se passe rien ?**

Si le nom du ficher comporte deux tirets (signe moins, tiret de la touche 6) consécutifs « -- » il n'est pas ouvert directement par WinPT. Dans ce cas il suffit de renommer le fichier avec un nom plus court, en supprimant au moins l'un des deux tirets, pour qu'il soit bien traité.

- **Lorsque je double-clique sur la clé publique pourquoi ai-je un message d'erreur ?**

Lors de l'import d'une clé, WinPT peut vous afficher le message d'erreur suivant et la clé n'est pas importée.

Si une clé publique à une date de création postérieure à la date système de votre ordinateur, vous obtiendrez ce message. La modification de votre date système pour qu'elle soit postérieure à celle de création de la clé peut permettre de l'importer.

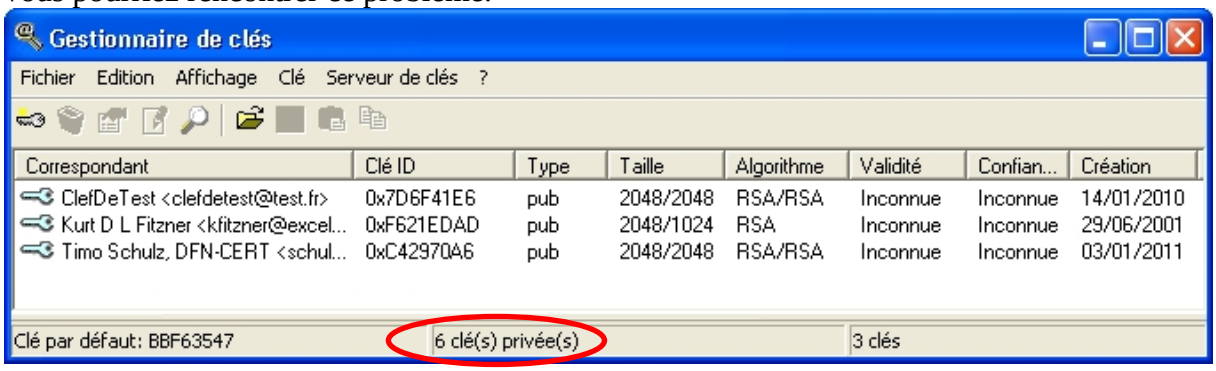
Ce message peut aussi être causé par une modification de la clé (par une erreur informatique ou par un pirate). Demandez alors à votre correspondant de vous retransmettre sa clé.

- **La clé publique que j'ai importée ne s'affiche pas dans WinPT ?**

Après l'import d'une clé dans WinPT il est nécessaire de recharger le trousseau (avec le menu « Clé/Recharger le trousseau » du gestionnaire de clés) pour l'afficher. Sinon elle n'apparaîtra qu'au démarrage suivant de WinPT.

- **WinPT m'indique un nombre de clés privées supérieur à celles qui apparaissent**

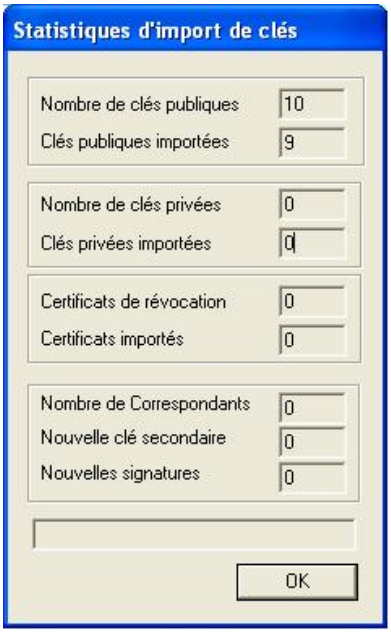
Si vous avez importé une clé privée ayant une date de création postérieure à celle de votre système, ou si vous avez reculé la date de votre OS avant celle de création d'une clé présente, vous pourriez rencontrer ce problème.



Vous devez soit corriger la date de votre système, soit supprimer votre trousseau de clés privées (dans C:\Documents and Settings\ "user" \Application Data\gnupg) puis réimporter les seuls bi-clés ayant des dates correctes.

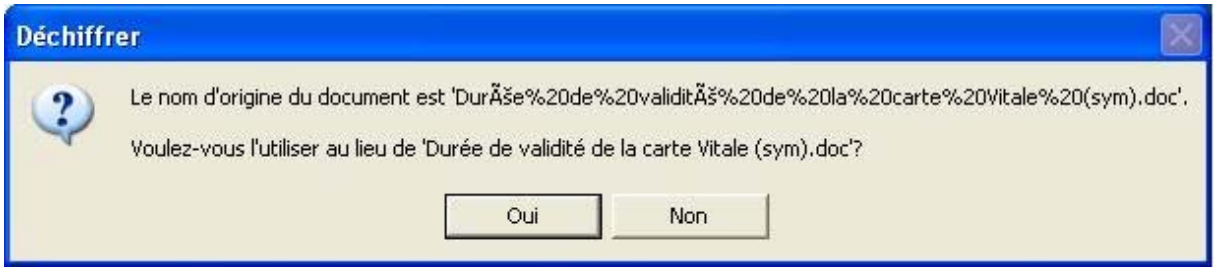
- **J'ai déjà importé des clés publiques. Si je réimporte les mêmes clés vont-elles se trouver en double dans le « Gestionnaire de clés » de WinPT ?**

Vous pouvez demander d'importer plusieurs fois la même clé. WinPT vérifie si la clé est déjà présente et n'importera pas une deuxième fois une clé déjà présente. Dans l'exemple ci-dessous, le fichier sélectionné comportait 10 clés publiques mais seulement 9 sont importées car l'une des 10 est déjà présente dans le trousseau.



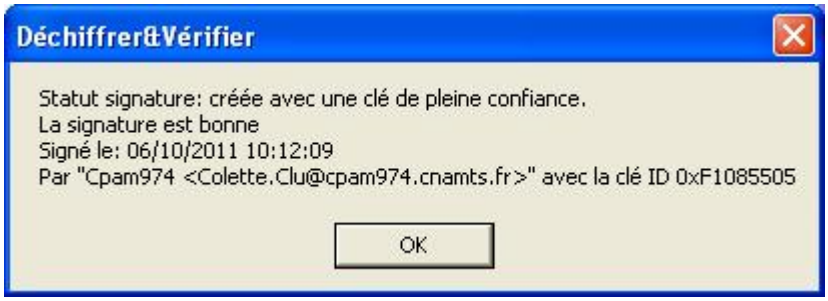
- **J'obtiens des messages d'alerte que je ne connais pas, pourquoi ?**

Si vous obtenez l'un des écrans suivant :



ou

ou



c'est que vous avez utilisé WinPT et pas GPGee pour déchiffrer le document. Soit c'est volontaire, reportez vous alors aux chapitres sur l'utilisation de WinPT pour savoir comment interpréter ces écrans. Si c'est involontaire c'est que vous avez réalisé un double-clic (avec le bouton gauche de votre souris) sur le fichier, ce qui a lancé WinPT, au lieu d'un simple clic-

droit qui permet d'accéder à GPGee. Les écrans de WinPT étant plus complexes à interpréter que ceux de GPGee, pensez bien à réaliser des clics-droits.

- **Je n'arrive pas à déchiffrer le .gpg reçu. Pourquoi ?**

Lors du chiffrement, la liste des destinataires du document chiffré est définie (en les sélectionnant individuellement ou en sélectionnant un groupe de destinataires). Si un document ainsi chiffré est envoyé par mel à une personne qui n'avait pas été sélectionnée à l'étape précédente, elle ne pourra pas le déchiffrer. C'est la cause la plus courante de ce type de problèmes. Demandez qu'on vous renvoie le document chiffré à votre attention.

Il est nécessaire d'être vigilant, lors de l'envoi du mel, de ne pas ajouter comme destinataire des personnes non choisies lors de la première étape du chiffrement. En pratique, il est moins perturbant de réduire la population des destinataires lors de l'envoi du mel, que de l'augmenter.

○○○