PGP 6.5.8

Olivier Hoarau (olivier.hoarau@fnac.net)

V1.1 du 1.10.00

1 Préambule

Ce document présente PGP qui vous permet d'échanger des données en toute confidentialité sur internet et de vous identifier et d'authentifier des personnes sur internet sans aucune ambiguïté.
La dernière version de ce document est téléchargeable à l'URL http://funix.free.fr. Ce document peut être reproduit et distribué librement dès lors qu'il n'est pas modifié et qu'il soit toujours fait mention de son origine et de son auteur, si vous avez l'intention de le modifier ou d'y apporter des rajouts, contactez l'auteur pour en faire profiter tout le monde.
Ce document ne peut pas être utilisé dans un but commercial sans le consentement de son auteur. Ce document vous est fourni "dans l'état" sans aucune garantie de toute sorte, l'auteur ne saurait être tenu responsable des quelconques misères qui pourraient vous arriver lors des manipulations décrites dans ce document.

2 Historique du document

10.9.00 Création du document
1.10.0 Rajout du paragraphe sur la fonction Wipe
Rajout d'un mot sur le patch corrigeant le bug ADK de la version française

3 Présentation

Vous pouvez utiliser **PGP** (Pretty Good Privacy, qu'on peut traduire par plutôt bonne confidentialité) pour protéger vos emails, vos fichiers, il apporte un niveau supplémentaire de confidentialité dans votre utilisation quotidienne de l'ordinateur et dans les communications avec d'autres personnes. Accessoirement **PGP** permet de vous authentifier aux yeux de vos interlocuteurs, ou d'authentifier d'autres personnes. Cette version **PGP** corrige le **ADK bug** (Additional Decryption Key) qui a défrayé la chronique dans le domaine , il y a encore peu. Les fonctionnalités de **PGP** sont les suivants:
- **PGPnet** qui permet de sécuriser les communications basées sur TCP/IP (pour l'instant ça ne marche que pour Win 95b (OSR2), win98 et winNT4.0 mais pas pour Win95a (première édition) et Win2000)
- On peut encrypter des fichiers et des répertoires sous forme d'un gros fichier, cet archive est autoextractible, c'est à dire que quelqu'un ne possédant pas PGP, peut la décompresser et la décrypter, dès lors bien sûr qu'on lui en ait donné les droits.
- pour les inconditionnels de la ligne de commande, la commande peut aussi être lancé d'une fenêtre DOS
- il s'intègre à Outlook 2000 et Outlook Express 5.0

Pour ce qui concerne la licence, le logiciel est libre d'utilisation pour une utilisation non commerciale de type perso, écoles et autres universités, et organisations à but non lucratif.

NOTES :

- Il existe une version traduite en français que vous trouverez à l'URL http://www.geocities.com/SiliconValley/Bay/9648/pgp651fr.htm, sur cette page vous y trouverez un patch pour corriger le but ADK.
- Si vous avez encore des doutes sur la légalité de PGP, allez jeter un coup d'oeil à l'URL www.mtic.pm.gouv.fr/dossiers/documents/lat/pgp.shtml.

4 Comment ça marche

PGP repose sur le principe de l'algorithme asymétrique à base de clé publique et privée. La clé publique comme son nom l'indique est publique et peut être largement diffusée sur le net, l'autre clé est privée, elle ne doit en aucun cas être communiquée à quelqu'un et doit rester secrète, elle est uniquement disponible pour son propriétaire et seulement. L'émetteur va chiffrer son message au moyen de la clé publique qui appartient au destinataire, ce dernier déchiffrera son message avec sa clé privée, et le tour est joué.

Par conséquent le point crucial du système est que vous ne communiquiez en aucun cas votre clé privée, vous devez faire en sorte que le fichier et répertoire contenant votre clé privée soient d'accès hautement restrictifs.

Le risque maintenant du système est que la clé publique du destinataire que vous détenez ne soit pas la bonne mais appartienne à quelqu'un d'autre, ou que quelqu'un se soit fait passer pour votre destinataire (ce qui revient au même) et ait donné sa clé publique.

Pour parer à cela, il faut ABSOLUMENT être sûr sans la moindre ambiguïté que la clé publique que vous receviez soit bien celle de votre destinataire, pour cela vous devez certifier la clé publique, vous ne devez en aucun cas certifiez une clé publique si vous avez des doutes sur son origine.

PGP utilise plusieurs algo, voici le détail des différents appels aux algos, lors du chiffrement d'un message :

- création d'une clé de session spécifique au message
- utilisation de **IDEA**, **CAST** ou **TripleDES** pour chiffrer le message en utilisant la clé de session
- utilisation de **RSA** ou **DH/DSS** pour chiffrer la clé de session avec la clé publique du destinataire
- le message est chiffré paré à être envoyé

Côté destinataire, on aura :
- appel à **IDEA** pour déchiffrer la clé secrète du destinataire à partir du pass-phrase
- appel à **RSA** ou **DH/DSS** pour déchiffrer la clé de session avec la clé secrète
- appel à **IDEA**, **CAST** ou **TripleDES** pour déchiffrer le message avec la clé de session

NOTE La limitation en France porte sur la taille de la clé de session qui sert à chiffrer le message.

Pour s'authentifier, vous aller crypter un fichier avec votre clé privée, seule la clé publique pourra le décrypter, où est donc l'intérêt puisque par définition celle-ci est publique et que n'importe qui peut y avoir accès ? Très simple, ça permettra à celui qui possède votre clé publique et qui décrypte le message de penser que vous seul pouvez en être à l'origine, puisque vous êtes le seul à avoir l'autre clé (la clé privée). Ce mécanisme permet d'une part de créer un système de signatures électroniques, d'assurer qu'un fichier est resté intègre (qu'il n'a pas été bidouillé par des personnes tierces). Beaucoup de personnes utilise **PGP** essentiellement pour s'authentifier plutôt que pour crypter les données.

PGP repose sur le principe du "trousseau de clé" (keyring en anglais), chaque utilisateur va se constituer un catalogue de clés publiques, celles-ci pourront être signées ou pas suivant le niveau de confiance qu'on a en elle. On dispose d'outils pour gérer ce trousseau de clé qui sont principalement:

-l'importation d' une clé publique, qui permet ensuite d'envoyer des messages chiffrés au propriétaire de la clé publique, pour cela on rajoute sa clé publique dans le trousseau
-ensuite on doit donner un degré de confiance à la clé, par défaut on a aucune confiance en la clé, pour authentifier la clé, on va signer la clé.
-une fois signée, on peut éventuellement envoyer cette clé signée sur un serveur de clé,

comme ça les autres pourront juger de la confiance à accorder à la dite clé. C'est l'étape d'exportation.

Les versions 2.X de **PGP** utilisaient une gestion de clés de type **RSA**, les versions ultérieures ont utilisé des clés de type **Diffie-Hellman**, ce qui fait qu'on n'avait pas forcément la compatibilité entre les différentes versions de **PGP**. Les versions plus récentes gèrent à la fois les types **RSA** et **DH**.

5 Installation

Vous devez récupérer l'archive **PGPFW658Win32.zip** à l'URL www.pgpi.org que vous dézipperez dans un répertoire temporaire, à créer préalablement, dans ce répertoire lancez **setup.exe**. Lisez attentivement les fenêtres d'information, notamment celle concernant la licence puis celle sur les fonctionnalités plus particulièrement au niveau des restrictions d'emploi (**PGP Issues**). Par défaut le programme est installé sous **c:\Program Files\Network Associates\PGP**. Vous avez le choix ensuite d'installer :
- les programmes esssentiels à PGP (**Core PGP**)
- **PGPnet Virtual Private Networking**
- **PGP Qualcomm Eudora Plugin** (plugin à **Eudora**, non validé par défaut)
- **PGP Microsoft Exchange/Outlook Plugin** (comme son nom l'indique, sélectionné par défaut)
- **PGP Microsoft Outlook Express Plugin** (comme son nom l'indique, sélectionné par défaut)

Le total par défaut fait 11Mo.

A un moment de l'install on vous demande quelle interface réseau vous voulez sécurisé par **PGPnet**, j'ai eu le choix entre:

- la carte d'accès à distance (le modem pour aller sur le net)
- la carte réseau

Vous ne pouvez sélectionner qu'une interface, j'ai choisi l'interface carte réseau pour mes essais. **PGPnet** n'est pas abordé dans cette page pour l'instant.

Il demande ensuite si on possède déjà un jeu de clés (**Keyrings**), répondez par oui (par défaut) ou par non. L'ordinateur doit être ensuite rebooté.

6 Gestion des clés

6.1 Création des clés

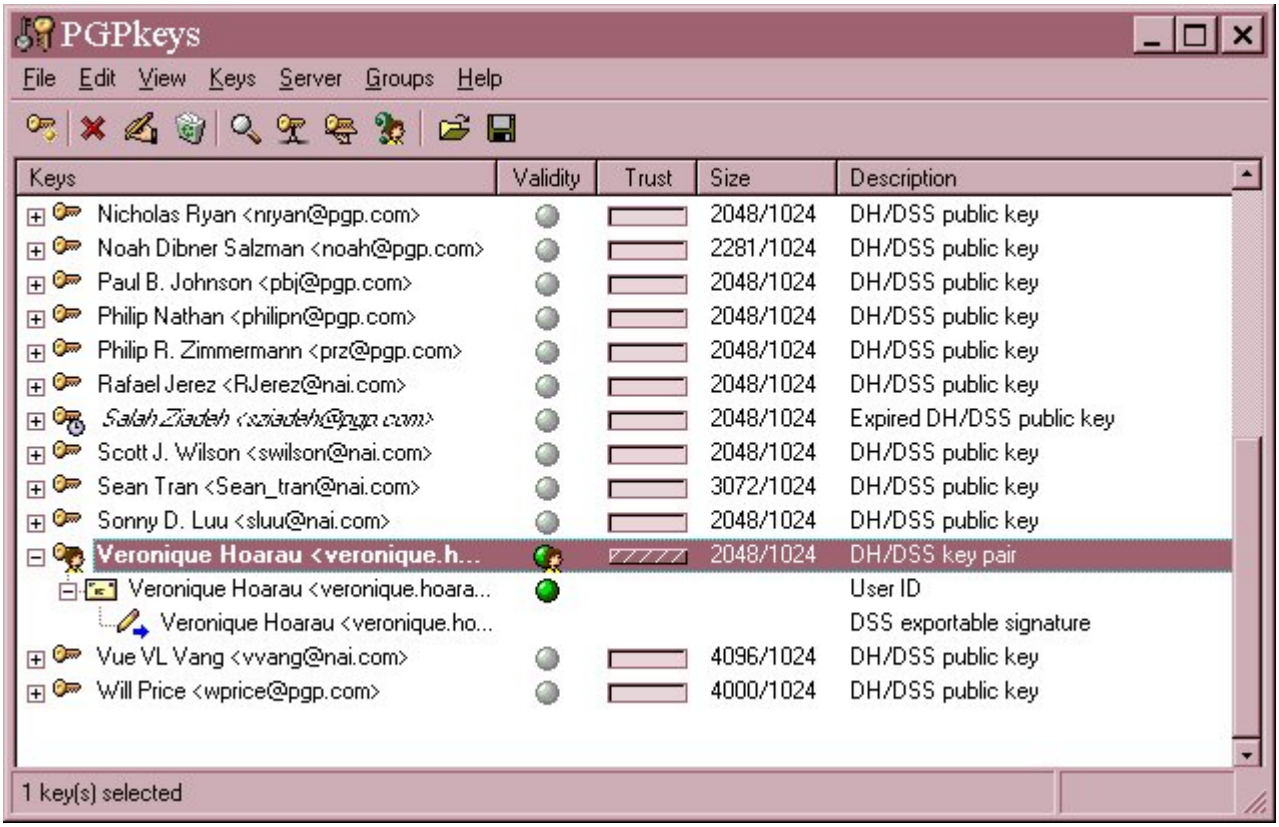
Au reboot de la machine, vous allez retrouver maintenant une petite icône au niveau de la barre de tâches, quand vous cliquez dessus avec le bouton droit de la souris, le menu suivant apparaît.

Pour l'instant ce qui nous intéresse c'est la création des clés publique et privée, sélectionnez donc **PGPKeys**. La première qu'on lance le programme, celui-ci demande si vous voulez générer votre paire de clés, cliquez sur suivant, saisissez votre nom et votre email, il sera attaché à votre clé publique pour qu'on puisse vous reconnaître. Ensuite il vous demande quel type de clé, vous voulez générer, vous avez le choix entre:

- Diffie Hellman/DSS (par défaut)
- RSA

Choisissez plutôt le premier type qui est le plus usité. On vous donne ensuite le choix pour la longueur des clés (1024bits, 1536bits, 2048bits, 3072bits, et personnalisé), on choisit la valeur par défaut à savoir 1024 bits. Vous pouvez ensuite faire en sorte que vos clés soient valides uniquement pendant une certaine période, ou alors qu'elles n'expirent jamais, par défaut elles n'expirent jamais (**Key pair never expires**). Tapez ensuite une phrase mot de passe (deux fois, la deuxième fois pour confirmer la frappe), cette phrase peut être relativement longue et comporter des espaces. Si ça vous gène de taper et de ne rien voir, cliquez sur **Hide Typing**. La génération des clés peut commencer alors. Vous pouvez ensuite envoyer votre clé publique vers un serveur de clé se trouvant sur internet, vous pouvez passer cette étape. La création des clés est terminée.

La fenêtre **PGPKeys** apparaît, on y retrouve votre clé (sur le screenshot Veronique Hoarau) et les clés de vos correspondants (par défaut un tas de personnes de **pgp.com**).



Pour y voir plus clair, on va supprimer de votre "trousseau" de clés toutes ces personnes que vous ne connaissez pas. Pour cela sélectionnez les clés non désirées, puis **Edit** et **Delete**.

6.2 Exporter la clé publique

Sélectionnez votre clé, puis dans la barre de menu, sélectionnez **Keys** et **Export**, vous vous retrouvez avec une fenêtre pour se balader dans l'arborescence, par défaut dans mon cas le fichier va s'appeler **Veronique Hoarau.asc**, si vous voulez filer la clé publique à quelqu'un se trouvant sous Unix, je vous conseille de supprimer l'espace dans le nom du fichier. Dans cette même fenêtre faites attention de ne pas cocher "**Include Private Key(s)**".

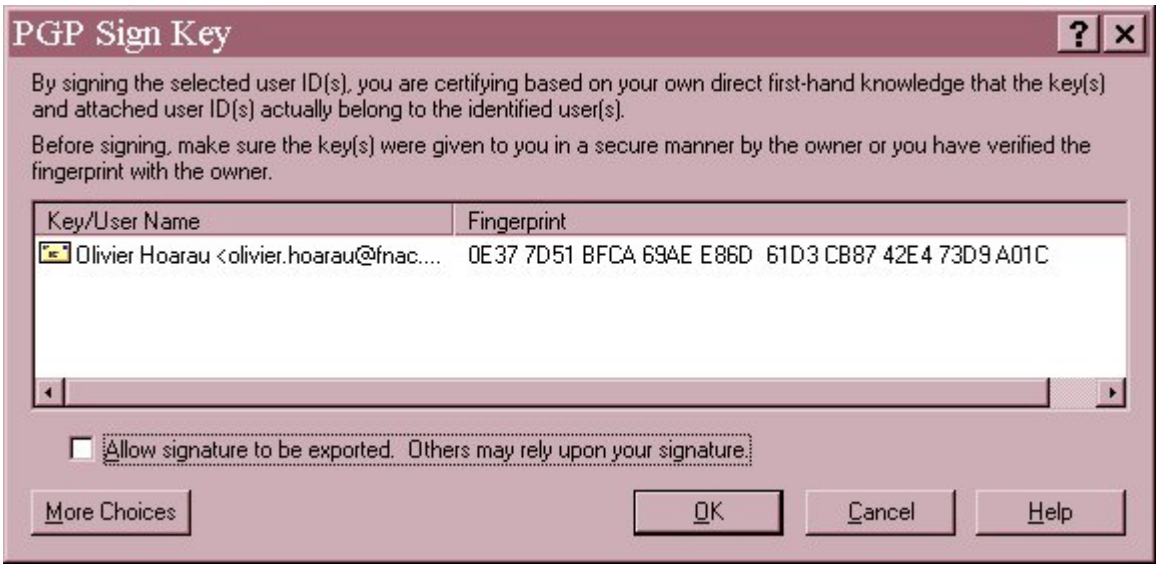
6.3 Importer une clé publique

Votre correspondant doit vous filer sa clé publique au format qui va bien, pour la mettre dans votre "trousseau" de clés, au niveau de la même fenêtre, sélectionnez **Keys** et **Import**, la clé publique doit être contenue dans un fichier **.txt** ou **.asc**.
Une fois le fichier sélectionné :

Cliquez sur Import. L'interlocuteur concerné va apparaître alors dans la fenêtre principale.

6.4 Certifier une clé

Vous remarquerez que pour chaque correspondant vous avez un champ "**Trust**" c'est une marque de confiance dans la clé, ou de certification, si vous êtes absolument sûr que la clé publique que vous venez de recevoir appartient bien au destinataire et seulement dans ce cas là, vous pouvez certifier sa clé. Pour cela sélectionner la clé puis dans le menu **Keys** et **Sign** :



En signant (certificant) la clé de l'utilisateur concerné, vous avez la certitude que la clé publique en votre possession est bien la sienne. Cliquez sur OK, vous devez alors ressaisir votre phrase password.

7 Chiffrer des données

7.1 Présentation

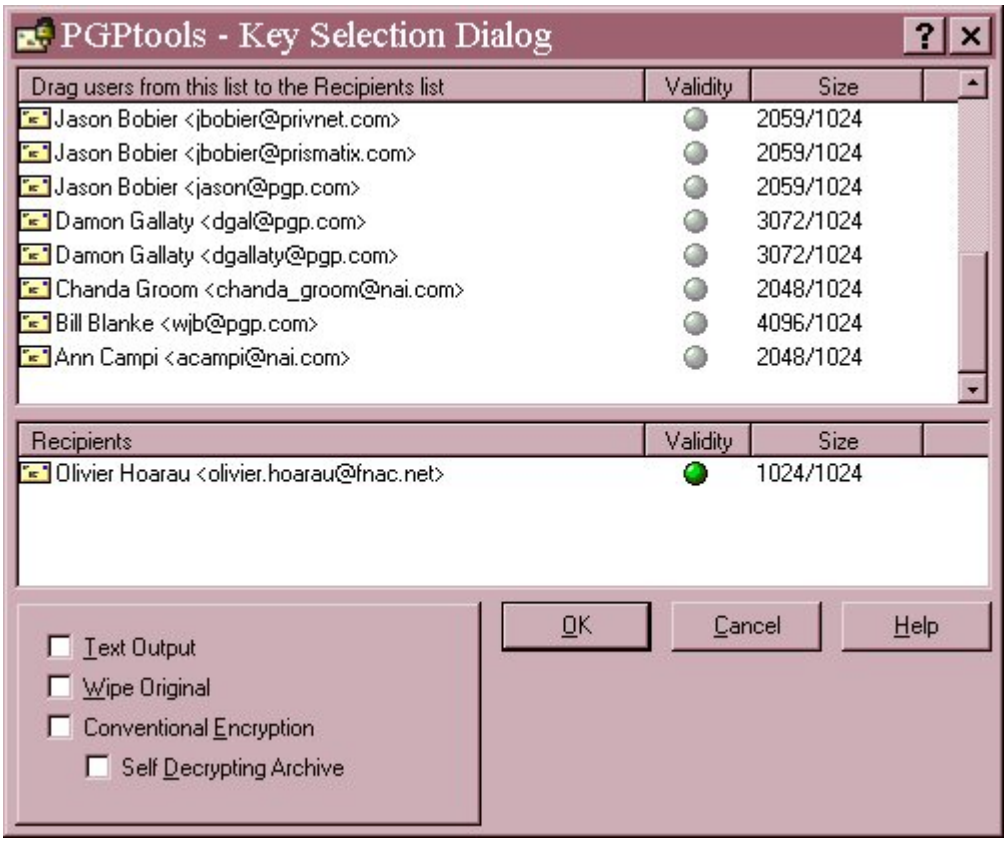
Au niveau de l'icône **PGP**, on va sélectionner maintenant **PGPtools**:

De gauche à droite:

- La première icône rappelle l'utilitaire **PGPKeys** qu'on a vu précédemment
- La deuxième icône permet de crypter un fichier
- La troisième pour signer un fichier
- La 4eme pour encrypter et signer
- La 5eme pour décrypter et vérifier

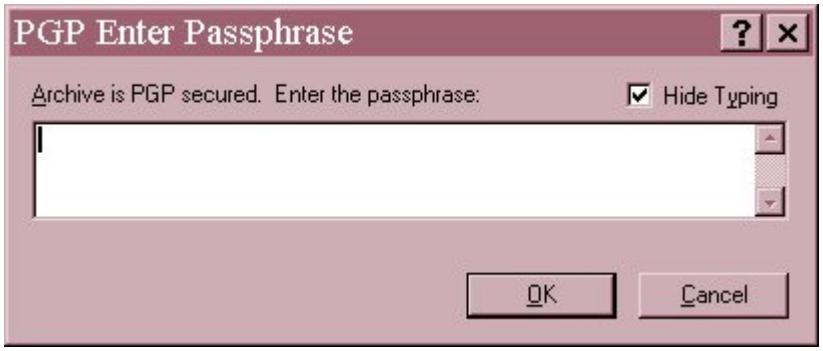
7.2 Crypter un fichier

Cliquez sur l'icône correspondante, sélectionnez le fichier correspondant, puis le destinataire dans la liste qui vous ont fourni leur clé publique :



Vous pouvez sélectionner le destinataire (**Recipient**) par drag and drop ou en double cliquant dessus. A noter que vous pouvez supprimer le fichier d'origine en cliquant sur **Wipe Original**. Le fichier sera sauvegardé avec l'extension **.pgp**.

A noter que vous pouvez créer ici un fichier crypté qui pourra être autoextractible en cliquant sur **Self Decrypting Archive**, vous devez saisir ensuite une phrase mot de passe qui sera ensuite au destinataire à décrypter le fichier, le fichier obtenu prend l'extension **.sda.exe**. A l'exécution de ce programme, la fenêtre suivante apparaît :



Il suffit de rentrer la phrase mot de passe pour que le fichier soit décrypté, à noter que ce mécanisme ne fait appel aux clés, mais uniquement à un mot de passe.

7.3 Décrypter des données

Au niveau de **PGPtools**, cliquer sur la cinquième icône en partant de la gauche, choisissez ensuite le fichier à décrypter et qui a du être crypter avec votre clé publique puisque vous en êtes destinataire.

On doit voir que le message a bien crypté avec votre clé publique, saisissez ensuite la phrase mot de passe de votre clé privée. Le fichier est alors décrypté, dans le répertoire où se trouve le fichier crypté.

8 Authentifier et s'authentifier

8.1 S'authentifier

La signature permet à ce que vos interlocuteurs vous authentifient parfaitement, pour cela on prend un fichier, on le signe avec la clé privée, n'importe qui en possession de la clé publique pourra le déchiffrer et donc vous identifier car vous êtes le seul capable de générer le texte. Pour cela cliquer sur la troisième icône (**sign**) en partant de la gauche de **PGPtools**, sélectionner le fichier en question puis votre phrase mot de passe.

Le fichier obtenu porte l'extension **.sig**.

ATTENTION Le but de la signature n'est pas de crypter un fichier, puisque n'importe qui en possession de votre clé publique pourra le décrypter, mais bien de vous authentifier.

8.2 Authentifier

Cliquer sur l'icône **Decrypt/Verify**, choisissez le fichier crypté, la fenêtre suivante apparaît :

Vous avez pu décrypter le message car vous avez la clé publique de l'envoyeur ce qui identifie bien ce dernier. Ceci n'authentifie pas complètement l'expéditeur, en effet quelqu'un pourrait très bien pu piquer la clé privée de l'envoyeur, vous n'est pas assuré à 100% que ce soit encore lui.

D'une autre manière quand vous récupérerez des fichiers sous internet, on trouve de plus en plus de fichiers signatures, ils permettent de voir que vous récupérer bien la bonne archive du bon auteur et non pas une archive détournée avec des backdoors à l'intérieur.

9 Supprimer définitivement des fichiers

Quand vous effacez un fichier avec le gestionnaire de fichiers par exemple, celui-ci n'est pas vraiment effacé, les blocs qu'il occupe, ne sont pas effacés immédiatement, ils seront réutilisés dans un temps plus ou moins long par le système de fichiers, il est donc toujours possible de pouvoir récupérer un fichier. **PGP** offre la possibilité de supprimer immédiatement et définitivement un fichier avec la fonction **Wipe**.

Au niveau de la barre d'outils **PGPTools**, sélectionnez l'icône **Wipe** (6eme à partir de la gauche). Vous devez sélectionner le fichier que vous voulez supprimer, une demande de confirmation de suppression vous est demandée, puis le fichier est définitivement supprimé avec aucune possibilité de régénération.

PGP dispose aussi d'un outil pour supprimer tous les blocs des fichiers que vous avez supprimés, dans la barre **PGPTools**, c'est la dernière icône à droite **Freespace Wipe**. Vous devez sélectionner le disque à nettoyer et le nombre de passe, plus ce nombre est élevé meilleur est le "nettoyage" (3 passes par défaut). Voici un screenshot pendant le nettoyage :