Projet Epibac - Chiffrement de fichiers avant envoi à Santé publique France

Installation de l'outil de chiffrement

Vous venez de recevoir par mail un fichier *Install.ivs* ainsi que cette documentation au format PDF nommée *Notice d'utilisation.pdf*.
Le fichier *Install.ivs* est un programme d'installation qui doit être enregistré sur votre disque dur et renommé en *Install.exe* avant d'être exécuté. Ce programme installe tous les composants nécessaires pour réaliser le chiffrement de fichiers.

L'outil utilisé pour le chiffrement des fichiers est le logiciel GPG dans sa dernière version stable 1.2.5. Ce logiciel est la version gratuite et libre du standard de cryptographie forte OpenPGP. Il utilise dans son fonctionnement deux clés aux rôles bien distincts :
- La première clé est dite clé publique puisqu'elle est connue de tout un chacun. C'est la clé publique du destinataire d'un message qui est utilisée pour chiffrer un message à son intention.
- La seconde clé, dite clé privée, est connue seulement de son propriétaire et sert à déchiffrer les messages chiffrés avec la clé publique correspondante.

Nous avons intégré au préalable la clé publique du projet Epibac dans le package fourni.
A l'issue de l'installation, GPG est donc directement utilisable.

GPG est un programme en « ligne de commandes », c'est-à-dire sans interface graphique.
Nous avons également intégré un outil supplémentaire, du nom de WinPT, qui permet de manipuler l'outil de chiffrement de manière plus conviviale. Nous détaillerons l'utilisation de ces outils dans la suite du document.

Remarque : Le programme d'installation ne nécessite pas de droits particuliers pour s'installer. Ainsi, un utilisateur sans privilège particulier, notamment qui n'est pas administrateur de sa machine, pourra procéder à cette installation. Toutefois, lors des étapes de sélection de répertoires, il faudra veiller à choisir des répertoires sur lesquels vous avez les droits d'écriture.

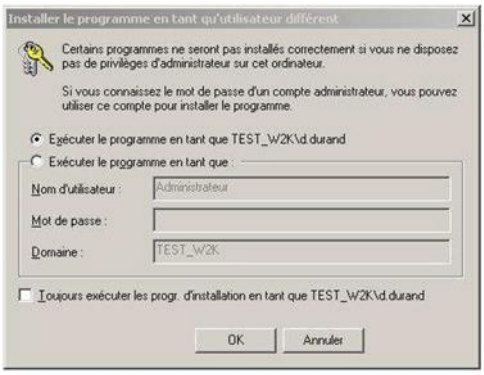
Afin de procéder à l'installation, suivez ces quelques étapes :
- enregistrez la pièce jointe au mail, nommée *Install.ivs,* sur votre disque dur à l'endroit de votre choix[1], en la renommant *Install.exe*

Pour se faire, sous Outlook
- faites un clic droit sur la pièce jointe
- choisissez *Enregistrer sous*
- sélectionnez un répertoire où vous avez le droit d'enregistrer des fichiers
- changez l'extension du fichier en *Install.exe* puis cliquez sur *Enregistrer*
- placez-vous dans le répertoire dans lequel vous avez enregistré et renommé la pièce jointe.

Double-cliquez sur le fichier *Install.exe* pour lancer l'installation. La fenêtre suivante apparaît :

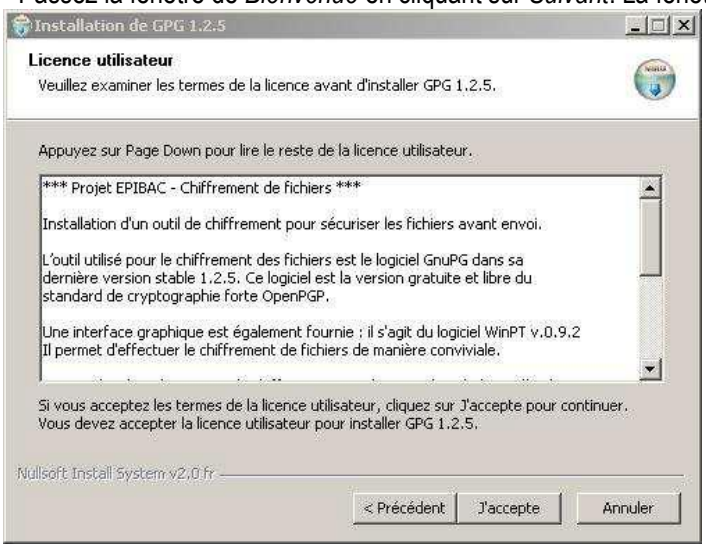
[1] Vous devez avoir le droit d'écriture dans le répertoire choisi pour pouvoir enregistrer le fichier ; généralement, votre bureau ou un sous-dossier du répertoire \Mes Documents devrait convenir.

Remarque : Si vous êtes un utilisateur sans droit particulier, une fenêtre de dialogue comme celle-ci-dessous peut s'afficher avant la fenêtre d'accueil du programme d'installation :



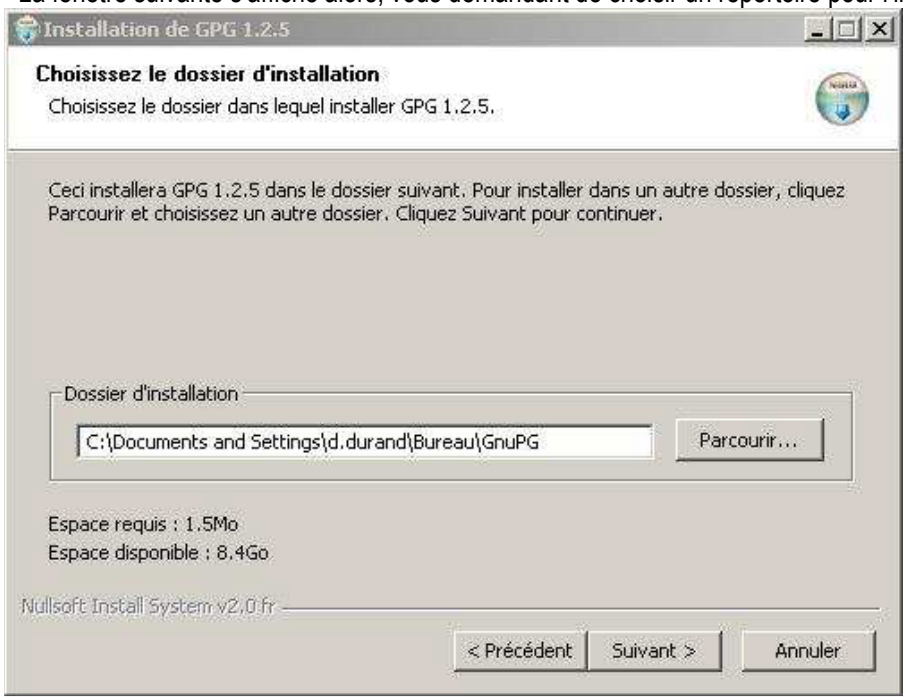
Dans ce cas vous pouvez choisir d'exécuter le programme sous votre compte utilisateur (ici celui de l'utilisateur procédant à l'installation, d.durand), car encore une fois le programme d'installation ne nécessite pas de droits privilégiés.

- Passez la fenêtre de *Bienvenue* en cliquant sur *Suivant*. La fenêtre suivante apparaît :



Quelques explications sur les outils installés et sur les principes de chiffrement sont données au travers de cette fenêtre. Après les avoir lues, vous pouvez cliquer sur *J'accepte.*

- La fenêtre suivante s'affiche alors, vous demandant de choisir un répertoire pour l'installation :



Par défaut il vous est proposé de copier les fichiers dans un dossier créé pour l'occasion sur le *Bureau* Windows. Vous pouvez si vous le souhaitez choisir un autre répertoire pour l'installation[2]. Cliquez ensuite sur *Suivant*.

- Une fenêtre vous demandant de choisir un nom de dossier s'affiche alors :

Il s'agit ici d'indiquer un nom pour le dossier qui sera créé dans le sous-menu *Programmes* du menu *Démarrer* de Windows. Vous pouvez laisser le nom proposé par défaut ou le modifier, puis cliquer sur *Installer* pour procéder à l'installation proprement dite.

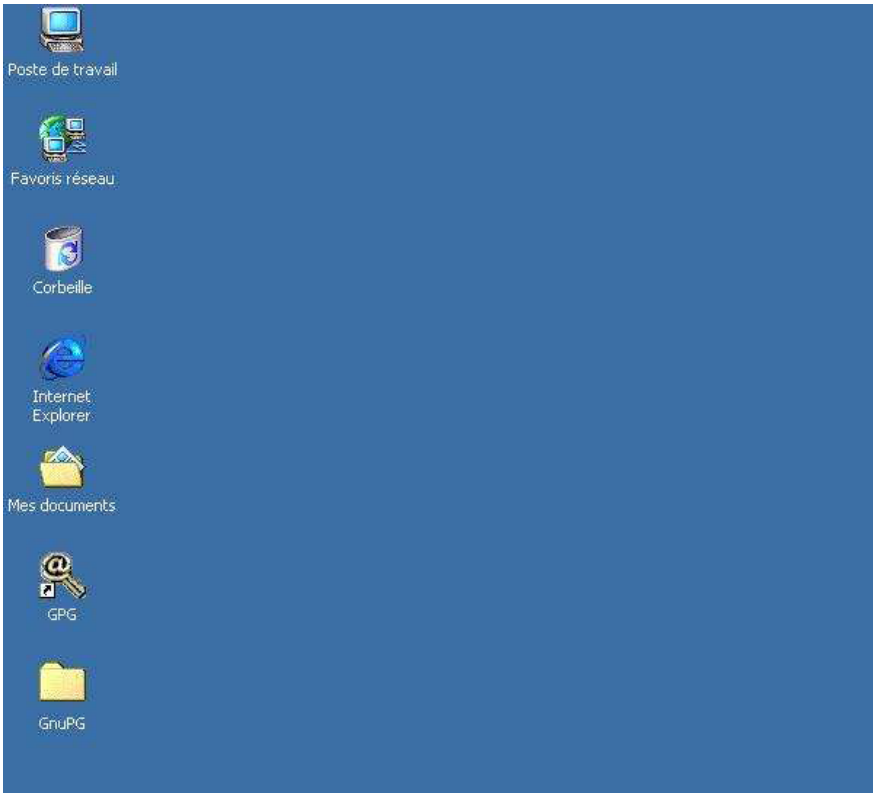
---

[2] Vous devez avoir le droit d'écriture dans le répertoire choisi pour que le programme d'installation puisse y copier le fichier ; typiquement, votre bureau (par défaut) ou un sous-dossier du répertoire \Mes Documents devrait convenir.

- Les fichiers nécessaires sont alors installés dans le répertoire choisi préalablement. A l'issue de cette installation, la fenêtre suivante apparaît :

Ceci vous indique que l'installation s'est bien déroulée. Vous pouvez sortir en cliquant sur le bouton *Fermer*.

L'installation est terminée, tout est prêt pour chiffrer vos premiers fichiers.



Si vous avez conservé les choix par défaut, vous devez avoir deux nouveaux éléments sur votre *Bureau* :
- un raccourci vers l'interface graphique WinPT (cf. plus loin dans ce document pour son utilisation) N.B. : ce raccourci doit être présent sur le *Bureau* même si vous avez choisi un autre répertoire pour l'installation
- un dossier GnuPG contenant les programmes GPG et WinPT ainsi que les différents fichiers utilisés par ces deux programmes.

Chiffrement d'un fichier
1ère méthode : Utilisation de l'interface graphique WinPT

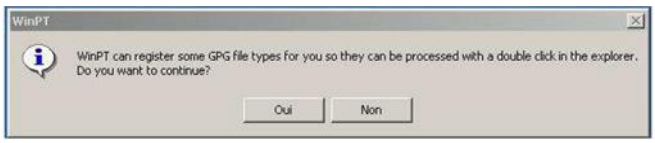
Cette méthode, plus conviviale, est à privilégier. En cas de problème, une seconde méthode est proposée à la suite.

Nous allons décrire la procédure pour chiffrer un fichier nommé ici pour l'exemple *Resultats.doc*.

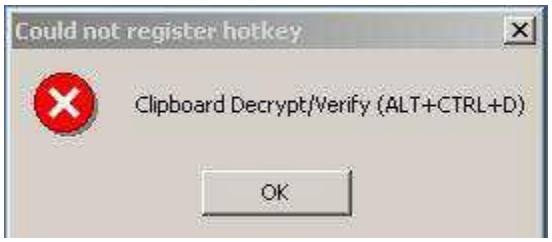
1) Lancer le programme WinPT par en double-cliquant sur le raccourci sur le bureau

ou bien en l'appelant par l'intermédiaire du menu ajouté dans le menu Démarrer : *Démarrer* \ *Programmes* \ *GPG* \ *WinPT*

2) Lors de la première exécution, la fenêtre suivante peut apparaître, vous proposant d'associer WinPT aux extensions particulières créées par GPG. Vous pouvez cliquer sur *Oui*. La question ne vous sera plus posée par la suite.

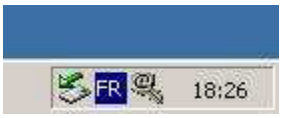


3) Au lancement de WinPT, une fenêtre d'erreur peut également apparaître : le programme essaie d'associer des combinaisons de touches/raccourcis claviers : si ces combinaisons de touches sont déjà utilisées par d'autres programmes, un message comme celui ci-dessous peut apparaître :



Il suffit de cliquer sur *OK*, cela ne gêne en rien le bon fonctionnement du programme.

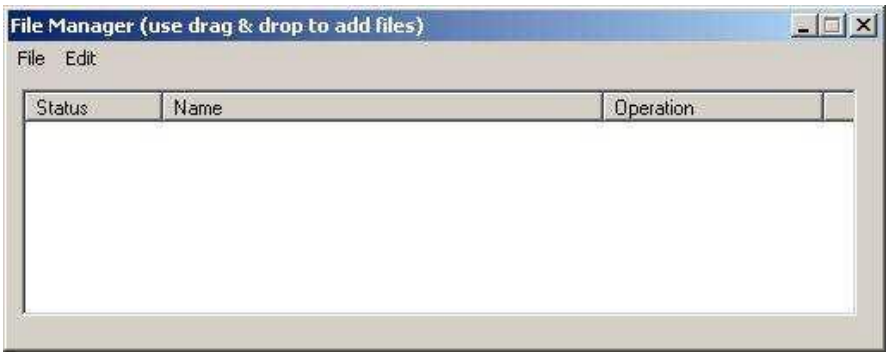
4) Lorsque le programme est lancé, vous pouvez le voir dans la barre des tâches à côté de l'horloge : il s'agit de la petite icône constituée d'une clé avec un @



5) Vous accédez aux fonctions du programme par un clic droit sur cette icône. A ce moment-là, le menu suivant s'affiche :

Il convient de toujours appeler le gestionnaire de fichiers (File Manager) ; sélectionnez donc cette option et cliquez sur *File Manager.*

6) La fenêtre suivante apparaît :

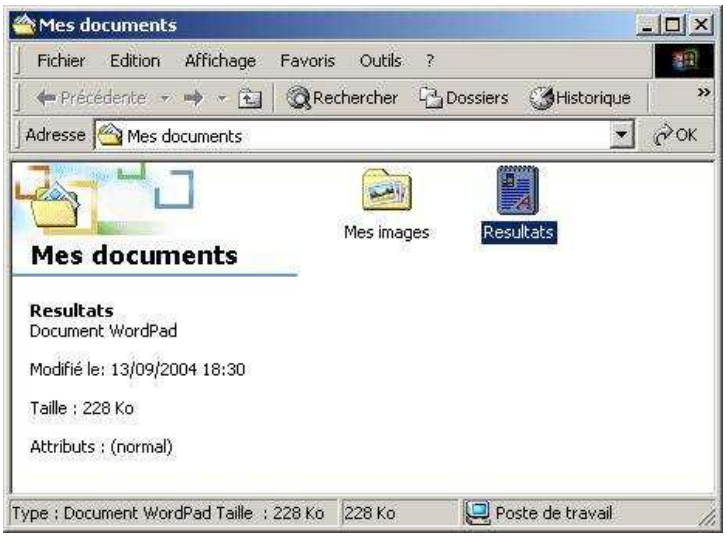


Il suffit de glisser le fichier que vous souhaitez chiffrer dans cette fenêtre.

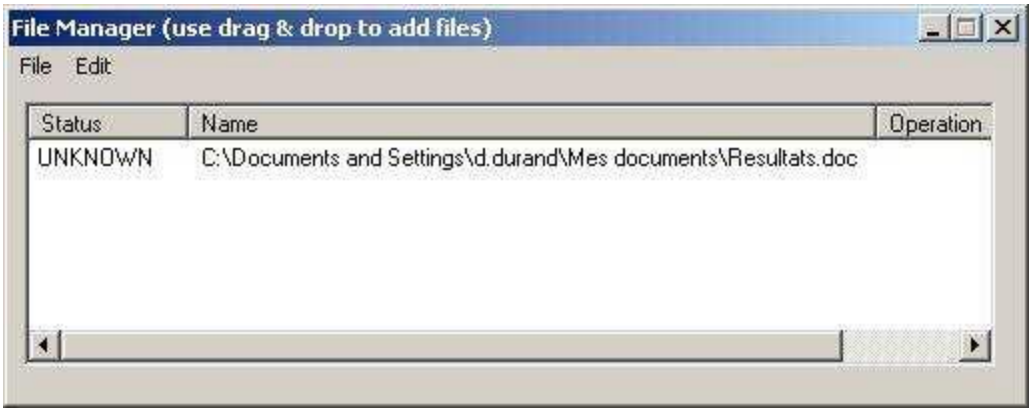
7) Le plus simple pour y parvenir est d'ouvrir en même temps une fenêtre sur le dossier contenant le fichier que vous souhaitez chiffrer (en ouvrant l'Explorateur de fichiers par exemple).

Ici nous souhaitons chiffrer le fichier Resultats.doc[3] et avons donc ouvert le dossier qui contient ce fichier.

[3] Les extensions de fichiers « connues » peuvent être masquées sous Windows en fonction du paramétrage de la machine. Pour cette raison, ici, le document.DOC, apparaît seulement par une icône caractéristique, sans l'extension.

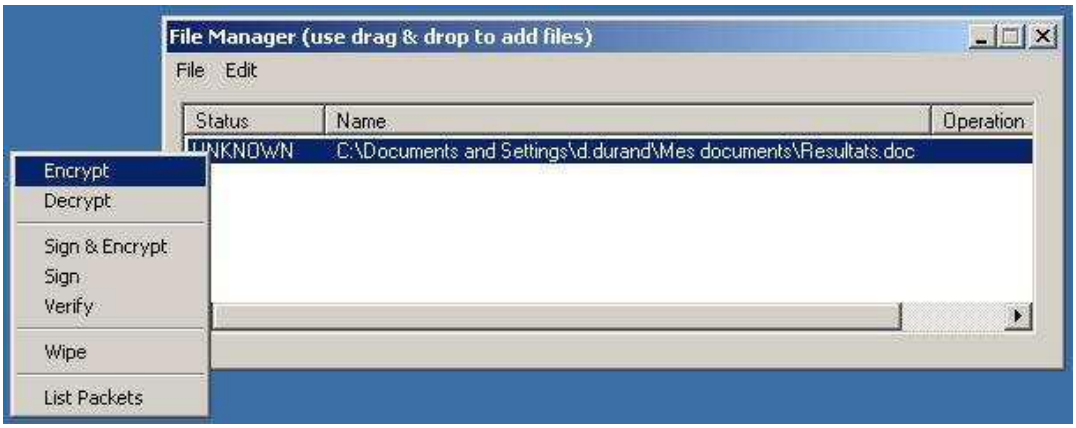


8) Nous faisons glisser l'icône du fichier vers la fenêtre *File Manager* et relâchons la souris (glisser-déposer ou drag&drop).



Le chemin du fichier s'affiche alors dans le *File Manager* avec un statut *UNKNOWN*, puisque le fichier n'est pas chiffré pour l'instant.

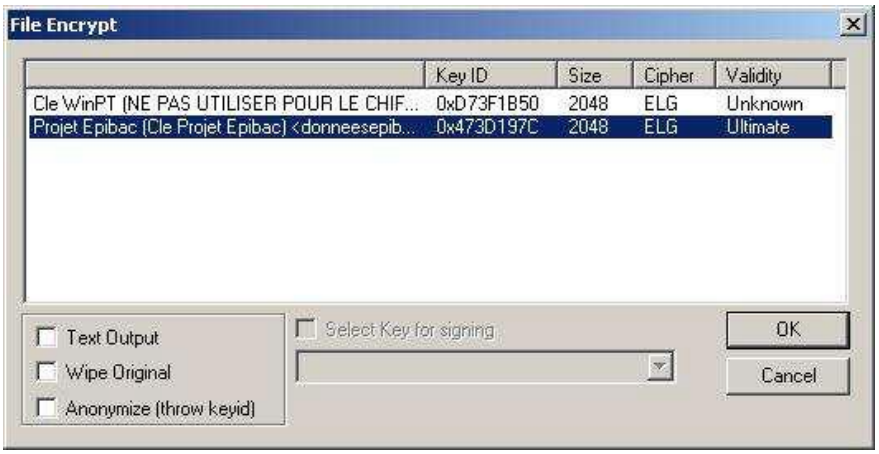
9) Sélectionnez le fichier (clic sur la ligne) puis faites un clic droit ; le menu suivant apparaît :



Choisir *Encrypt* pour procéder au chiffrement du fichier.

Remarque : on peut également obtenir le chiffrement en cliquant sur *File* puis *Encrypt*.

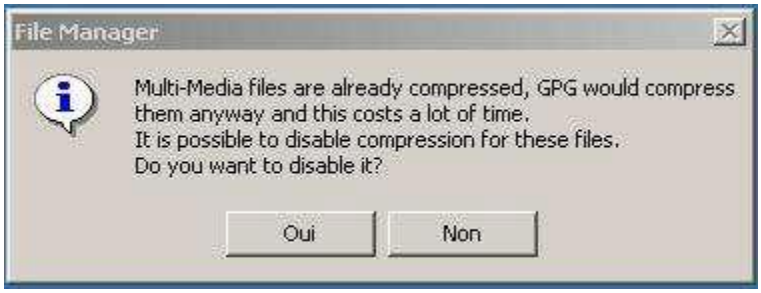
10) Une nouvelle fenêtre apparaît vous demandant de préciser avec quelle clé vous voulez chiffrer le fichier :



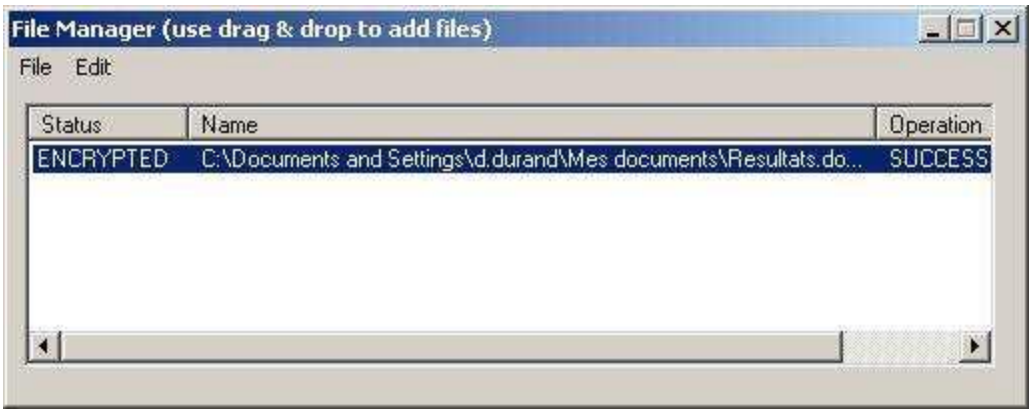
Il faut sélectionner la clé « Projet Epibac » et valider par *OK*.

Attention : ne pas utiliser la première clé (Cle WinPT) qui n'apparaît que pour le bon fonctionnement du logiciel.

11) La première fois le message suivant peut éventuellement apparaître : valider par *Oui*.



12) Lorsque le chiffrement est réalisé, le statut du fichier devient *ENCRYPTED* :



13) Le fichier chiffré est disponible dans le même répertoire que celui du fichier d'origine. Le fichier chiffré porte une double extension. Ici, il s'agit de la double extension .doc.gpg.

La première extension est celle du fichier d'origine, la seconde (.gpg) indique que le fichier est chiffré. C'est ce fichier, chiffré et portant la double extension, que vous pouvez transmettre par email à l'adresse : donneesepibac@santepubliquefrance.fr


Mes documents
Fichier Edition Affichage Favoris Outils ?
Précédente
Rechercher
Dossiers
Adresse
Mes documents
OK
Mes images
Resultats
Resultats.doc.gpg
Mes documents
Sélectionnez un élément pour obtenir une description.
Stocke et gère des documents
Voir aussi :
Favoris réseau
Poste de travail
3 objet(s)
258 Ko
Poste de travail

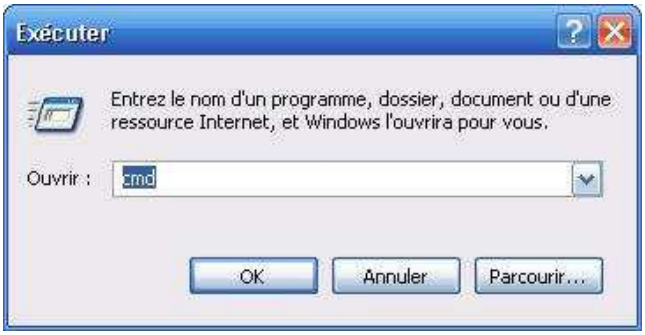
2ème méthode : Utilisation de la ligne de commande

Les manipulations décrites sont, après la première utilisation, très rapides à effectuer et toujours identiques, seul le nom du fichier à chiffrer changera.

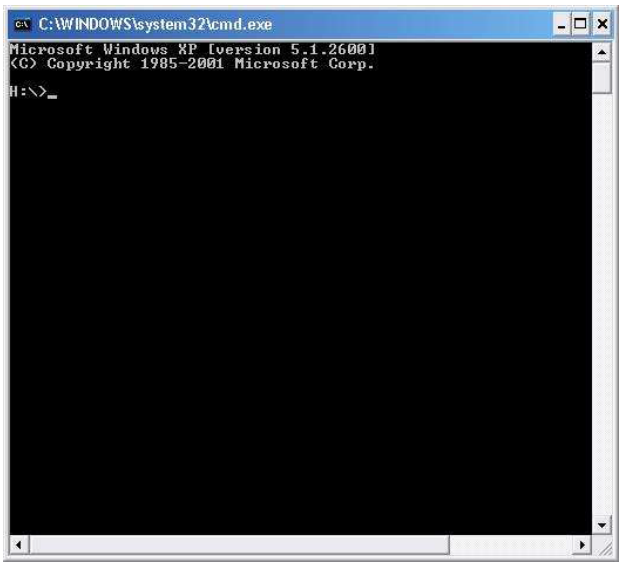
1) À l'aide de l'Explorateur de fichiers, copiez le fichier que vous voulez chiffrer, par exemple ici *monfichier.ext,* dans le répertoire d'installation du logiciel de chiffrement.

2) Ouvrir une « fenêtre de commandes » : la fenêtre de commandes, ou invite de commandes, est une interface en mode texte qui permet d'exécuter le logiciel de chiffrement en lui précisant quel fichier chiffrer.

Pour ouvrir cette « fenêtre de commandes », cliquez sur *Démarrer* dans le coin inférieur gauche de l'écran, puis choisissez *Exécuter…* La fenêtre suivante apparaît :



Tapez le mot *cmd* comme sur la capture ci-dessus en face de *Ouvrir*, puis cliquez sur *OK*. La fenêtre de commandes suivante apparaît à l'écran :



3) Cliquez sur cette fenêtre, un curseur clignote. Les caractères devant le curseur désignent le lecteur et le répertoire dans lequel s'est ouverte par défaut la fenêtre de commandes. Ici, elle s'est ouverte sur un lecteur H.

Vous devez tout d'abord aller dans le répertoire où est stocké le fichier à chiffrer (ainsi que l'outil de chiffrement). Dans notre cas, il s'agit du répertoire \gnupg qui se trouve sur le lecteur C[4].

[4] Si l'outil de chiffrement a été installé dans le répertoire proposé par défaut, il s'agira d'un répertoire GnuPG contenu dans une arborescence du type C:\Documents and Settings\nom_d_utilisateur\Bureau\GnuPG. La commande serait alors :

cd \Documents and Settings\ nom_d_utilisateur \Bureau\GnuPG

Pour cela, tapez simplement :
C : puis *Entrée*

Nous sommes désormais positionnés sur le lecteur C : Une commande simple permet de changer de répertoire : il s'agit de la commande *cd* pour C*hange* D*irectory*.
Nous devons taper cette commande en précisant vers quel répertoire nous souhaitons aller, ici :

cd \gnupg

Remarque : Le caractère « \ » est obtenu par la combinaison de touches « AltGR » + « 8 » et il doit être spécifié car ce caractère désigne le début d'un répertoire.

4) Nous sommes alors dans le bon répertoire, celui dans lequel se trouve l'outil de chiffrement et le fichier à chiffrer. Nous avons simplement à taper la commande suivante, toujours dans la fenêtre de commandes :

gpg -r epibac -e ".\monfichier.ext"

N.B. : Vous devez entourer le nom du fichier par des guillemets comme mentionné ici et le faire précéder de **.**
Cette séquence permet de spécifier complètement le fichier et d'avoir le fichier chiffré résultant avec une double extension, à savoir l'extension d'origine + l'extension gpg.
Ainsi, quelques secondes après avoir validé cette commande par *Entrée*, vous récupérez le fichier *monfichier.ext.gpg*, dans le même répertoire.

Vous pouvez alors transmettre ce fichier, chiffré et portant la double extension, par email à l'adresse :
donneesepibac@santepubliquefrance.fr