

Dans la série
LES TUTORIELS LIBRES
présentés par le site FRAMASOFT

Premiers pas avec WinPT (cryptographie sous Win)

EITIC

Logiciel : WinPT
site : <http://www.winpt.org/>

Niveau : Débutant

Auteur : [EITIC](#)

date de mise en ligne : 21 01 2003

Licence du document : licence libre GNU/FDL

FRAMASOFT

« Partir de Windows pour découvrir le libre... »

www.framasoft.net

WinPT : premiers pas ...

WinPT, logiciel de crypto assure la confidentialité de vos échanges.

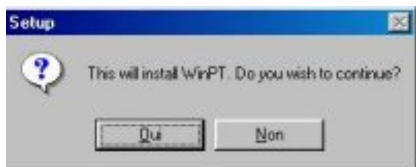
Attention : l'installation et surtout l'utilisation de ce logiciel requièrent une connexion internet.

Installation

Après avoir lu le fichier installation.txt cliquer sur l'icône



cliquer sur oui



Cliquer sur next ...
... et suivez le guide d'installation.



Quand l'installation est terminée, un raccourci s'affiche sur le bureau



Génération d'une paire de clés (clé privée et clé publique)

En fait le logiciel fonctionne de la manière suivante :
Il génère une paire de clés :

- la clé privée qui sert à lire les documents cryptés
- la clé publique que les correspondants utilisent pour crypter les documents envoyés au titulaire de la clé privée

A la fin de l'installation cette fenêtre s'ouvre
Cliquer sur oui pour générer une clé



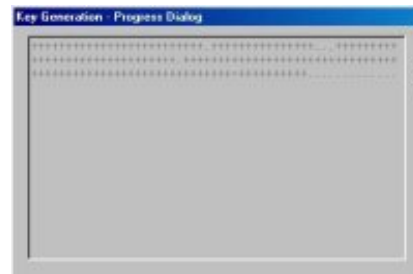
Remplissez soigneusement les champs requis comme ci-contre

Choisissez un mot de passe qui ne soit pas un mot existant (mélanger lettres et chiffres)
et **MEMORISEZ-LE** soigneusement vous ne pourrez pas le récupérer en cas d'oubli

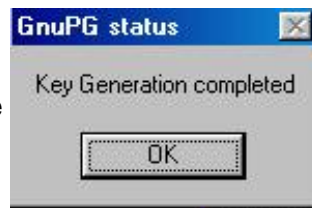
Attention, si vous choisissez une date d'expiration votre clé aura une durée limitée

Le logiciel génère votre clé.

Cela peut prendre un peu de temps



La clé est générée



Cliquer sur OK

Il est important de sauvegarder les deux clés générées (publique et privée) sur un autre support que le disque dur, pour prévenir tout risque de crash du disque dur par exemple (vos clés seraient alors irrémédiablement perdues).

Attention : il ne sert à rien d'imprimer ;o)



Cliquer sur "oui" et choisissez votre destination de sauvegarde (disquette, cdrom, ...) Ici sauvegarde sur une disquette (à archiver soigneusement !)



Utilisation du logiciel

Une icône est installée en bas à droite de la barre d'état du bureau

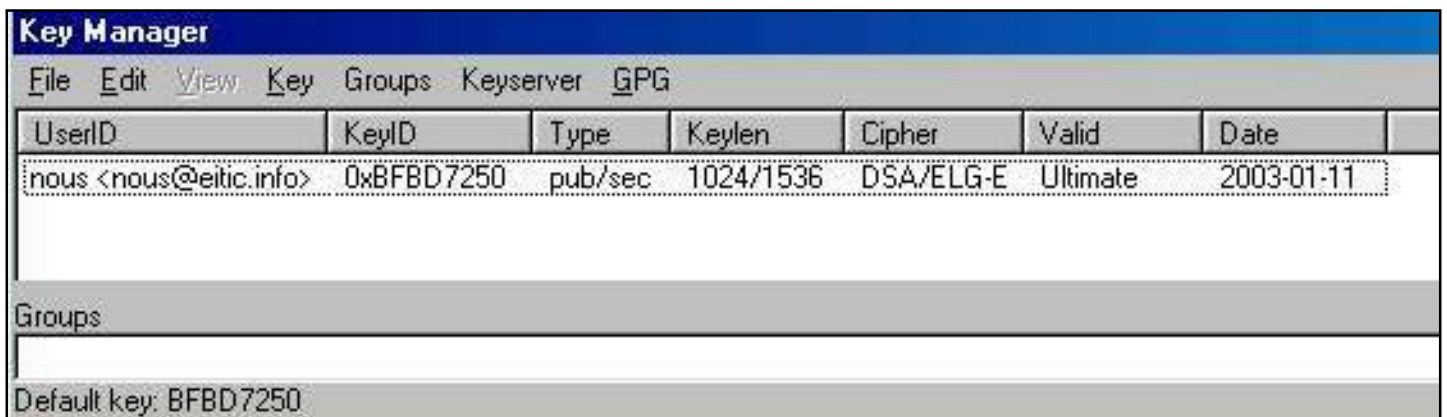


Cliquer avec le bouton droit de la souris sur cette icône en forme de clé

Un menu contextuel s'ouvre

C'est depuis ce menu que le logiciel se pilote

Selectionner "Key manager" avant de relacher le bouton de la souris



L'adresse nous@eitic.info est associée à une paire de clés (publique et privée : pub/sec) créée le 11/01/2003. Sa validité n'est pas limitée dans le temps (ultimate)

Envoi de la clé publique sur un serveur de clés (nécessite d'être connecté à internet)

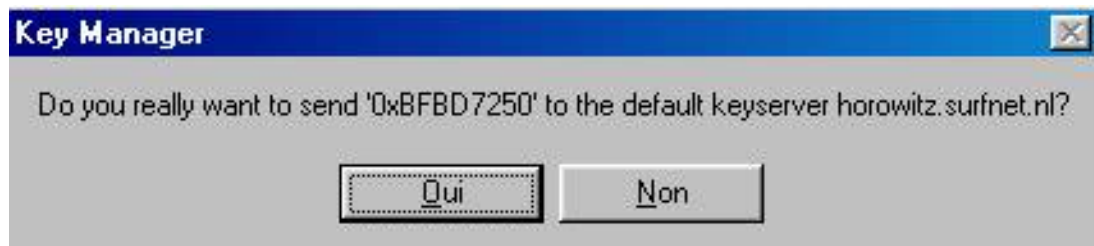
Pour que les correspondants éventuels puissent envoyer des documents cryptés, il faut qu'ils possèdent la clé publique de leur interlocuteur. D'où l'intérêt des serveurs de clés qui stockent les clés publiques

Il existe deux manières de procéder.

- Méthode directe
- Méthode manuelle

Méthode directe

Sélectionner l'adresse mail concernant la clé, cliquer sur le bouton droit de la souris et choisir "Send to keyserver"



Cliquer sur "oui". Un message d'alerte vous prévient de la bonne réalisation de la procédure...

Méthode manuelle

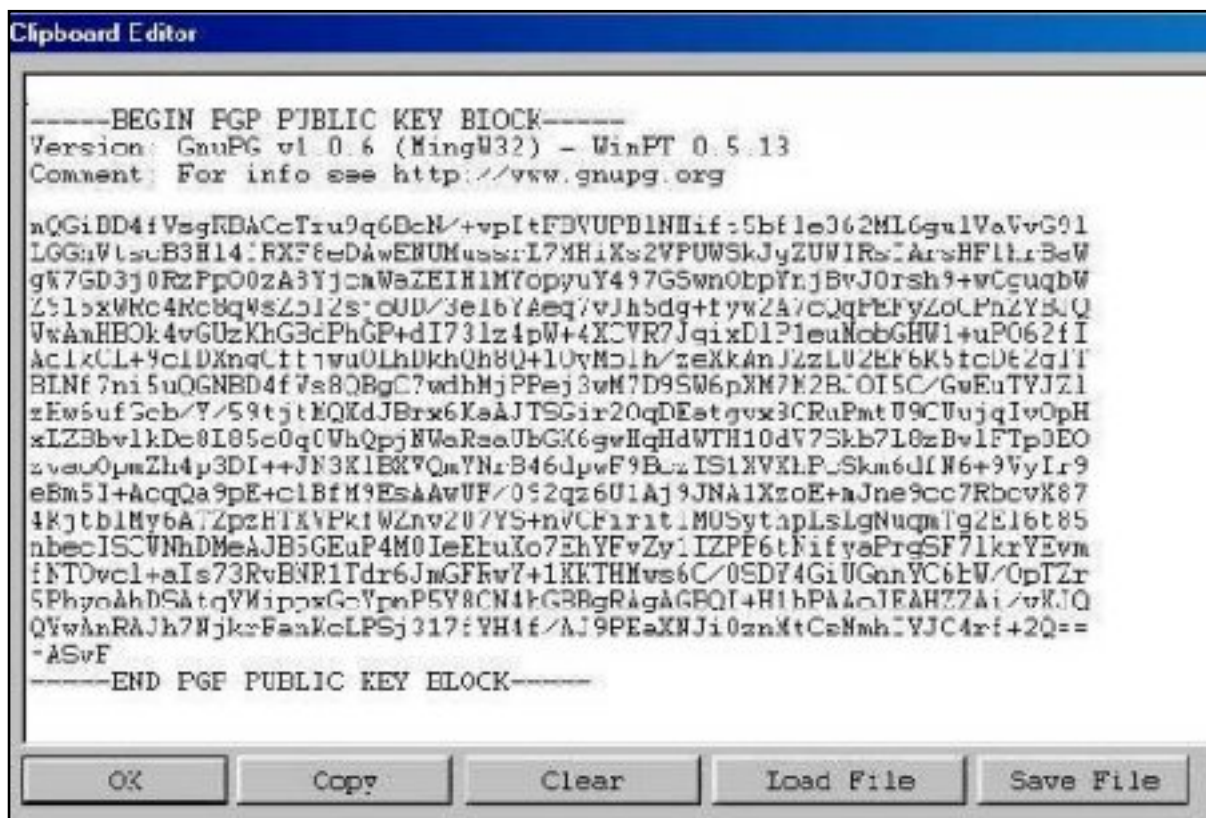
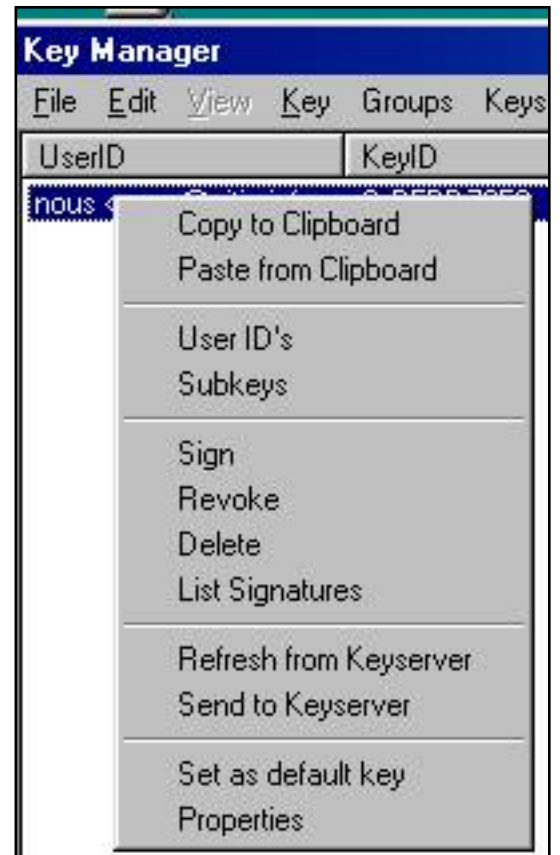
Il faut tout d'abord éditer la clé publique

- sélectionner la clé concernée dans le key manager
- cliquer (toujours avec le bouton droit de la souris) sur cette clé et choisir "copy to clipboard"

Un message d'alerte informe de la fin de l'action

Cliquer alors (toujours bouton droit) sur l'icône de la clé en bas à droite du bureau

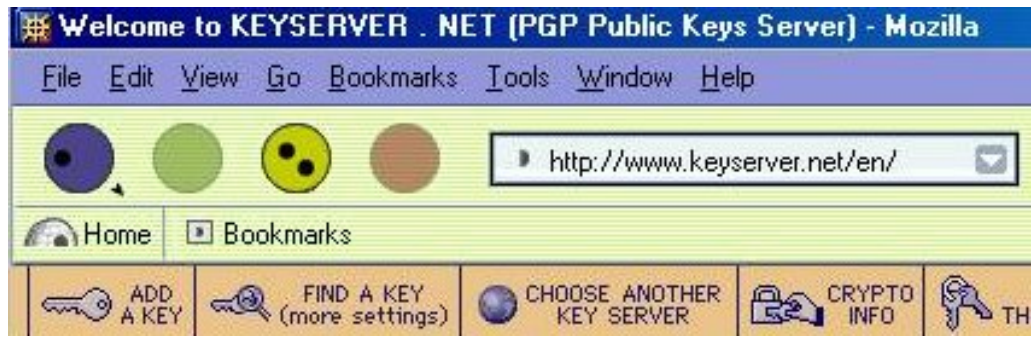
Le "clipboard" s'ouvre avec la clé sélectionnée



Il faut alors envoyer cette clé sur le serveur

Se connecter à [Serveur de clés](http://www.keyserver.net)

La fenêtre de keyserver.net s'ouvre



Cliquer sur "Add a key" et coller dans la zone de texte la clé publique sélectionnée dans le clipboard

Attention pour copier cette clé il faut bien veiller à ce que la sélection couvre tout le bloc de texte et rien que le bloc de texte, pas une ligne vide

Cliquer alors sur le bouton "submit this key to the keyserver"

La réception de la clé est confirmée



Chercher une clé publique sur un serveur de clé

Connecté au même serveur : [Serveur de clés](#)

Cliquer sur "find a key"

Entrer l'adresse concernée

Plusieurs options sont proposées

- Short list (liste des clés)
- List with Certificates (liste des clés et adresse des personnes les ayant signées, c'est à dire attestant que la clé présentée appartient bien à l'adresse citée. C'est ce que l'on nomme "un réseau de confiance", nous en parlerons par ailleurs.
- Show the key "Fingerprint" (le "Fingerprint" c'est l'immatriculation de la clé qui identifie précisément cette clé.

Choisir "Short List" et "Show the key "Fingerprint"".

Cliquer sur "Get List"

ADD A KEY FIND A KEY (more settings)

FIND A KEY

Type here to get the res Keys

Search for:
nous@eitic.info

Short List
 List with Certificates
 Show the key "Fingerprint"

Get List

Voici le résultat de la recherche

Notre clé publique est donc bien enregistrée sur le serveur de clés

Search Results		belgium.keyserv		
Your query on: "nous@eitic.info"				
To get a key, click on its Key Id.		Primary Name or Identifier		
Click on Search to make another query.		Secondary Name or Identifier		
Type	Key ID	Name	Size	Created
	BFBD7250	nous <nous@eitic.info>	1024	2003/01/10
Fingerprint = 1D5A 9225 3EAC E344 351E 79F1 01D9 6408 BFBD 7250				

Acquérir la clé publique d'un correspondant

Se connecter au même [serveur de clés](#)


Cliquer sur "find a key"

Entrer l'adresse concernée

Choisir "List with Certificates" et "Show the key Fingerprint".

Cliquer sur "Get List"



Type	Key ID	Name	Size	Created
	A1DBE7CE	eux <eux@eitic.info>	1024	2003/01/11
	Fingerprint = D981 75B0 F348 F28F 9CA1 B564 07A8 6FE9 A1DB E7CE			

Cliquer sur le lien bleu souligné (id de la clé)

La clé publique s'affiche.

Sélectionner soigneusement tout le bloc avec le bouton droit de la souris

Choisir copier.

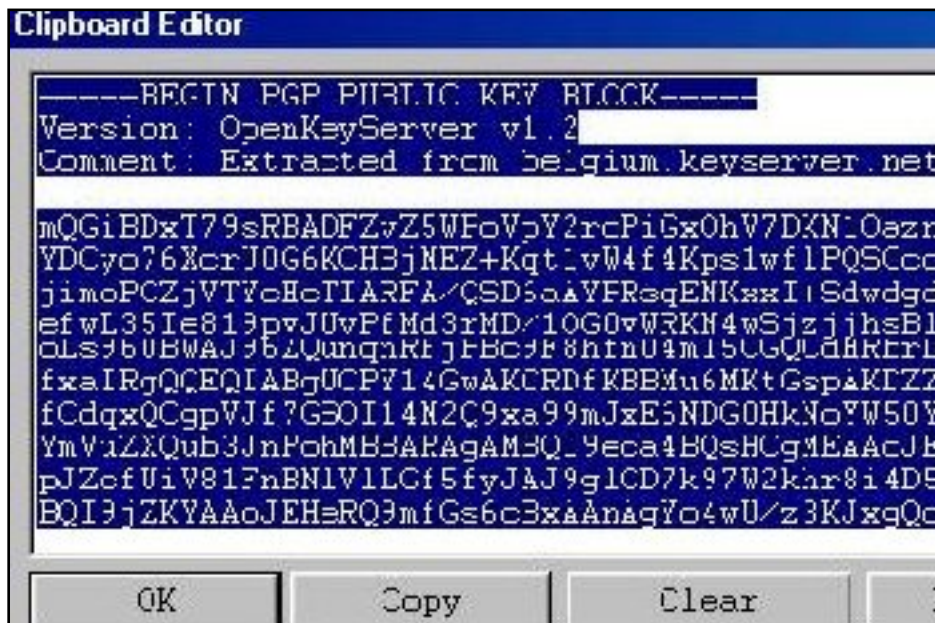


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: OpenKeyServer v1.2
Comment: Extracted from belg

mQGIBD4fYAkRBAD1jET6rpcMFTzR
twhsaP1/e60iAAZvcNuGO+xopxW9
m6fX8dM6Ag/xa4VqVWOLNxStSTvz
RnfJOgdkOnR1GOatczYLtJOD/OT6
UQqGpKKirdZQ1UEXubGUiQ4qx0Zv
```



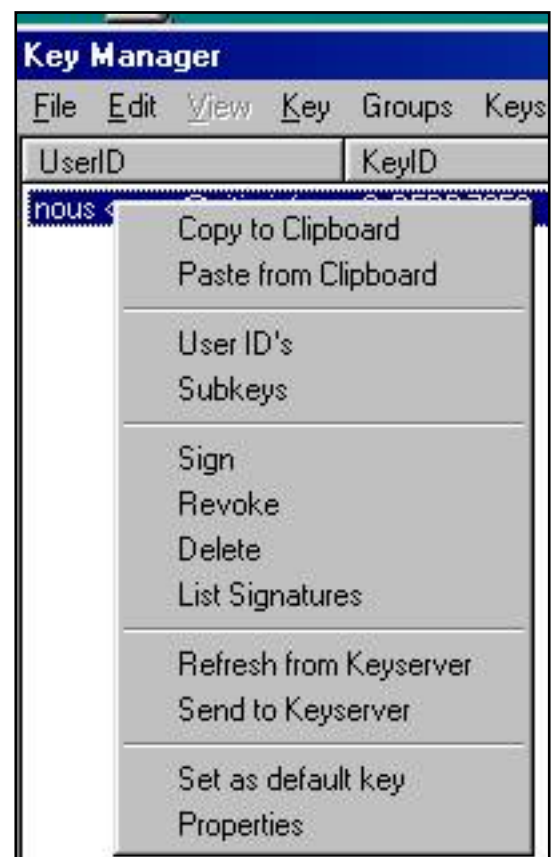
Cliquer (toujours bouton droit) sur l'icône de la clé (en bas à gauche du bureau) et choisir "edit clipboard"

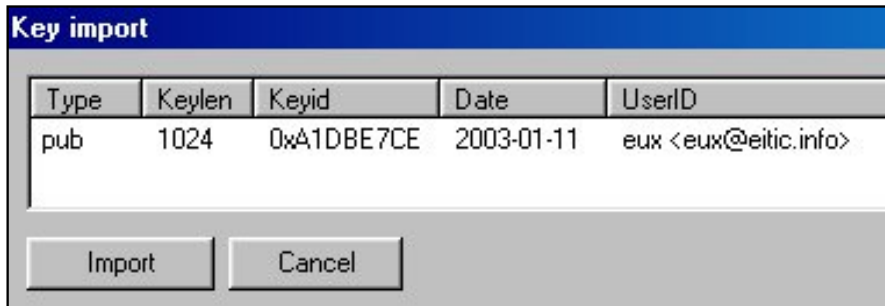


Sélectionner tout le bloc

Cliquer (toujours bouton droit) sur le "Key Manager" (en bas à gauche du bureau) et choisir "paste from clipboard"

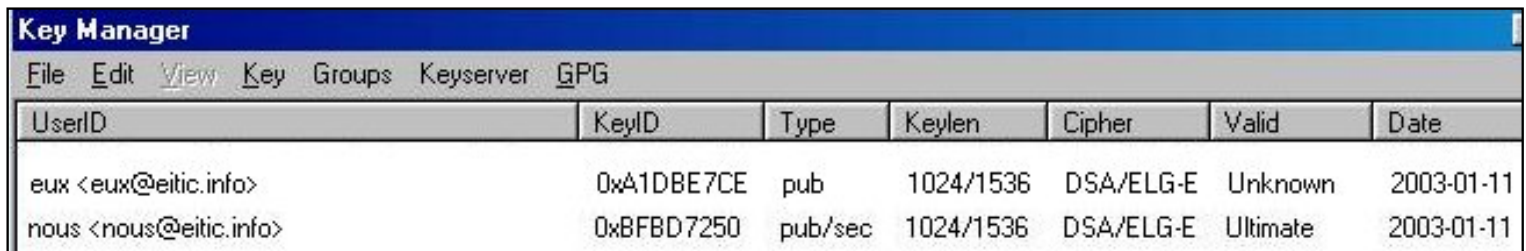
La fenêtre "key import" s'ouvre, elle indique les références de la clé à importer





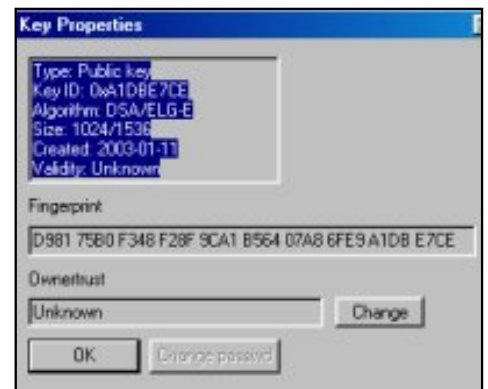
Cliquer sur le bouton "import", puis sur "ok" dans le message d'alerte annonçant la fin de la procédure d'importation.

Dans le menu "key" du "Key Management" choisir "Reload key cache", la clé importée apparaît dans la liste des clés (publiques bien évidemment !)



Pour connaître les propriétés de la clé importée et vérifier qu'elle appartient bien au correspondant, faire un clic droit sur la clé et choisir "Propriétés"

Comparer notamment le "Finger Print" de la clé, avec celui qui a été adressé par le correspondant.



Si tel est le cas, changer le degré de confiance accordé à la clé en cliquant sur le bouton "change" Choisir le degré de confiance souhaité (traduit en français dans l'ordre d'affichage)

- ne sais pas
- pas confiance
- confiance partielle
- confiance totale

Cliquer sur OK et valider le choix dans le message d'alerte

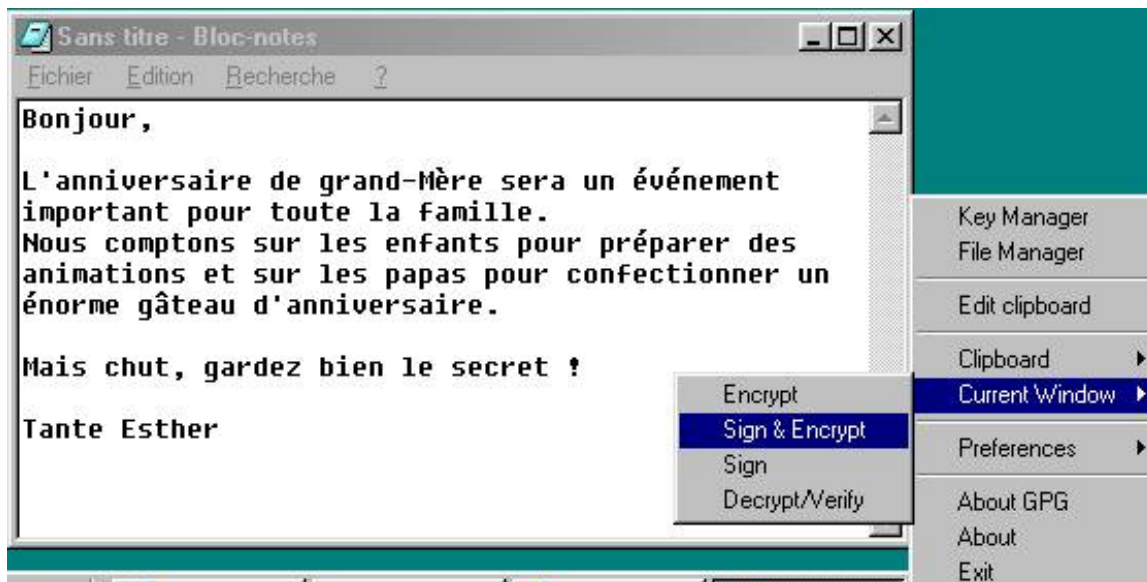


Crypter un document

Ouvrir un éditeur de texte, par exemple "note pad" (alias le bloc note de windows)

Ecrire le texte souhaité

Avec le bouton droit de la souris, cliquer sur l'icône de la clé (en bas à droite du bureau) et choisir "Current Windows" (fenêtre sélectionnée) et "Sign & Encrypt" (signer et crypter)



Dans la fenêtre "Sign & Encrypt" qui s'ouvre, choisir la clé du DESTINATAIRE du message crypté

Une fenêtre s'ouvre elle indique l'adresse lié à la clé PRIVEE avec laquelle le message sera signée (donc celle de l'EXPEDITEUR et demande la phrase clé (le mot de passe) pour cette clé.




```
Sans titre - Bloc-notes
Fichier  Edition  Recherche  ?

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.0.6 (MingW:
Comment: For info see http://

hQG0A4mWcGFP154yEAYAruxE09Ihl
Epj3ocU/JFFD11k0sMwmXEzJ1CHPI
/mAo86ecuECH6qfGik2bnLJdT3UPI
QD0ngI96S9TU/utjy70Wm1yLssdhl
NGLaDKG3ASf6CQWcNJWqBgCzKi92I
3U/ypCF94gEeBGI/UH20DPAJctiJI
Edt4kcMjr/D81bwtXFiiIuM0UyFql
JynIG/dZVdt00IY8V8BZnsKKF7gGi
AViJEopy4S+HP6FUz93WogFSwKQBI
PBmYWZrnnvadK1UF/CBwEAa0mrnk:
wFuNHCxxpuSkc/nPv1dNISjyBKLjl
kn9dAEirxKFNDywoFkjKUUGXH1SNl
1twj/eUQ+TtAET+ghBy5U6vksXgNl
+YDnSJ6PPBDqbC24r00w04YU4DuIi
xOKsb22u/vUq35wnCYwCi0miRMvkl
ZmM1M25xQ/v3Zk+YYnzeOKsUuFWBt
=FDIF
-----END PGP MESSAGE-----
```

Le message s'affiche maintenant crypté



Il suffit de l'enregistrer dans le répertoire de son choix pour l'envoyer par mail en pièce jointe (attention comme il a été crypté avec la clé du destinataire il ne pourra pas être décrypté par l'expéditeur ! Ceci dit, vous pouvez également le crypter avec votre propre clé afin d'en garder une copie cryptée)

Il est possible de le coller directement dans le corps d'un mail (attention de bien sélectionner tout le bloc avant de copier).

Décrypter un document

Ouvrir le document dans un éditeur de texte (ici "note pad")

Choisir "Decrypt/Verify" en cliquant avec le bouton droit sur l'icône de la clé (en bas à droite du bureau)

Si le message est dans le corps du mail, utiliser directement la fonction "Current Window" - "Decrypt/Verify" avec la fenêtre du mail.

Le plugin (petit module qui apporte des fonctions supplémentaires) Enigmail permet l'envoi de mails cryptés directement depuis mozilla.



Le "réseau de confiance"

De même que, sur notre ordinateur, nous pouvons accorder (ou non) notre confiance à la clé publique d'un correspondant, il est possible de porter cette information sur un serveur de clé. Signer la clé d'un correspondant c'est dire "j'atteste que cette adresse mail appartient bien à la personne dont le nom est indiqué". "J'atteste également du sérieux de cette personne dans l'usage qu'elle fait de sa clé.

C'est pour cela qu'il ne faut pas "signer" la clé de tout interlocuteur sans le connaître vraiment. Ainsi se crée un "réseau de confiance" d'interlocuteurs potentiels.

Il est par ailleurs très facile d'envoyer un mail avec l'adresse d'un autre internaute ... Un mail, signé par clé GPG est garanti envoyé par le propriétaire de l'adresse, sous réserve que le "fingerprint" de la clé signataire corresponde à celui indiqué par le correspondant ... ou, si vous ne connaissez pas ce correspondant, que cette clé soit signée par des personnes de confiance... A vérifier facilement sur le serveur.

Prochain épisode : intégrer Enigmail dans Mozilla et signer la clé publique d'un correspondant sur un serveur