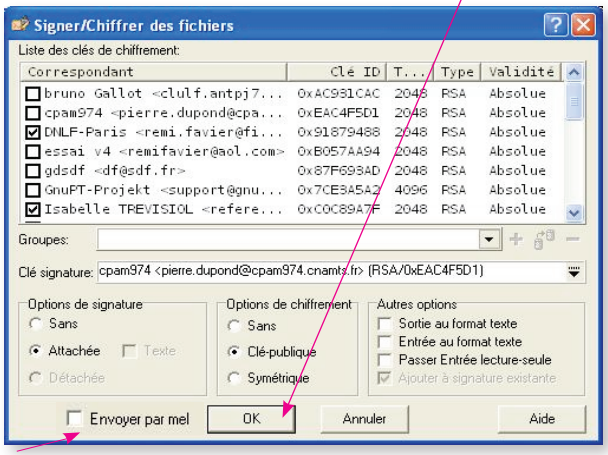
Signer&Chiffrer

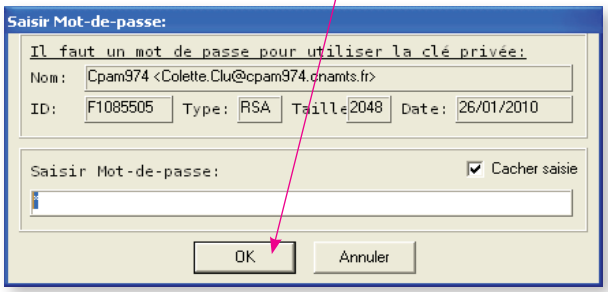
1) Faites un clic-droit sur le document à chiffrer. **GPGee** apparaît dans le menu contextuel. Choisissez **Signer&Chiffrer**

2) Un écran permet de choisir les destinataires du document chiffré. Votre clé de signature doit apparaître. Les options ne doivent pas être changées. Puis cliquez sur **OK**.



Cocher la case "Envoyer par mel", crée un courriel d'envoi du document chiffré aux correspondants.

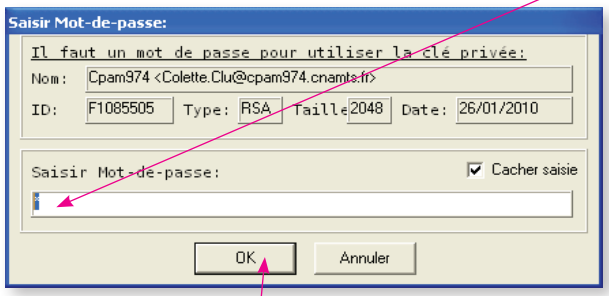
3) Un nouvel écran demande le mot de passe de votre clé privée. Après avoir cliqué sur **OK**, le document chiffré est créé à côté de l'original. Transmettez ce document chiffré à vos destinataires.



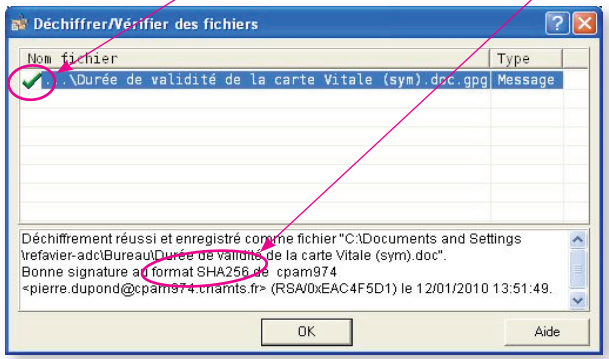
Déchiffrer

1) Enregistrer le document reçu dans votre répertoire de travail. Faire un clic-droit sur le document à déchiffrer. **GPGee** apparaît dans le menu contextuel. Choisissez **Déchiffrer&Vérifier**.

2) Un écran demande le mot de passe de votre clé privée.



3) Après avoir cliqué sur **OK** un nouvel écran vous indique le résultat du déchiffrement et de la vérification de la signature de l'émetteur. Si vous n'obtenez pas la coche ✔ ou le bon format de signature, une vigilance s'impose.



Le document déchiffré est créé à côté de l'original.

4) Supprimer après utilisation les documents informatiques reçus.

Logiciel de chiffrement GPG

Le logiciel de chiffrement GPG, avec ses deux extensions WinPT et GPGee, vous permet de protéger les documents informatiques, notamment pour des échanges par mél avec vos correspondants.

Approfondir

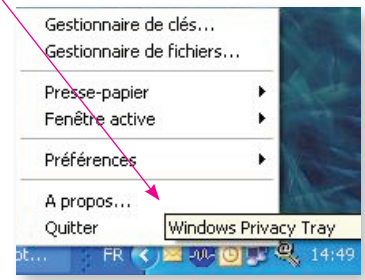
Pour approfondir l'utilisation de cet outil, consultez le mode d'emploi.

GPGee

Un clic-droit sur le document à chiffrer ou à déchiffrer, et **GPGee** apparaît, dans le menu contextuel, pour réaliser l'opération désirée.

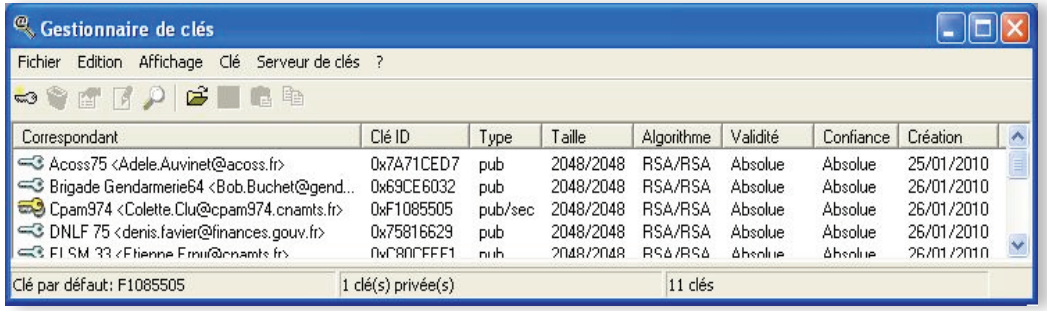
WinPT

Dans votre barre de tâches (en bas à droite de l'écran, avec l'horloge), se trouve l'icône de **WinPT** (Windows Privacy Tray) : une fois celui-ci démarré, cliquer sur cette icône affiche le menu de WinPT.



Le Gestionnaire de clés de WinPT permet de gérer votre trousseau de clés :

– les clés publiques de chacun de vos correspondants
– votre bi-clé (clé privée et sa clé publique) qui doit toujours être gardé en sécurité (pas envoyé par mel…).



À faire au démarrage

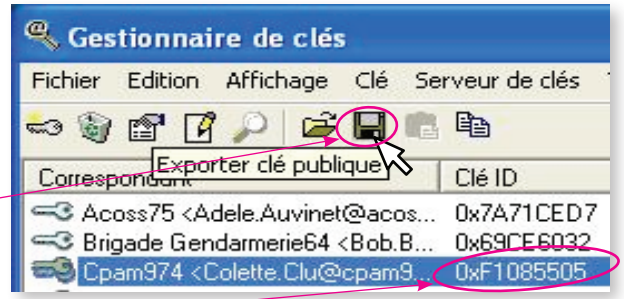
Transmettez votre clé publique à vos correspondants

(elle doit avoir été préalablement créée)

1) Dans le Gestionnaire de clés de WinPT, sélectionnez votre bi-clé dont la ligne devient alors bleue.

2) Cliquez sur le bouton **Exporter clé publique,** pour l'enregistrer.

3) Puis transmettez (par mél…) cette clé (.asc) à vos correspondants. Indiquez (par un autre moyen : téléphone…) votre **Clé ID**.



Ne transmettez jamais votre clé privée (ou secrète).

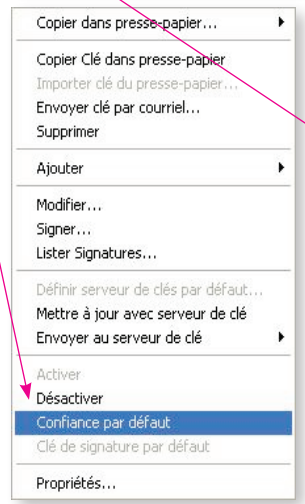
Importez et contrôlez les clés publiques reçues de vos correspondants

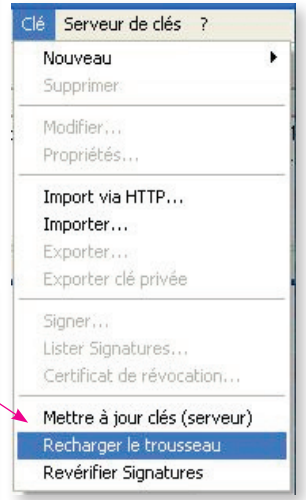
1) Pour importer une clé publique, il suffit de double-cliquer dessus. Cliquez ensuite sur **OK** sur l'écran de statistiques d'import.

2) Ouvrez ensuite le Gestionnaire de clés pour contrôler que la clé publique reçue est bien celle prévue. Dans le menu **Clé** sélectionnez **Recharger le trousseau** pour afficher la nouvelle clé.

3) Si le **Clé ID** est le bon, faites un clic-droit sur la clé et, dans le menu affiché, cliquez sur **Confiance par défaut**. Sa confiance devient alors « Absolue ».

4) Supprimez du Gestionnaire de clés les clés publiques inutiles (pas celles prévues, remplacées).





Dans windows

un **coffre-fort** est un document chiffré **.gpg**

une **main qui signe** est une clé de chiffrement **.asc**