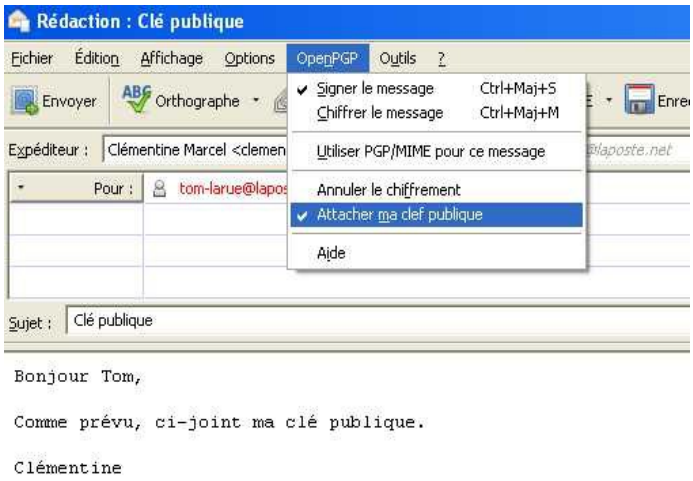
Annexe 4 : Gestion des clés publiques

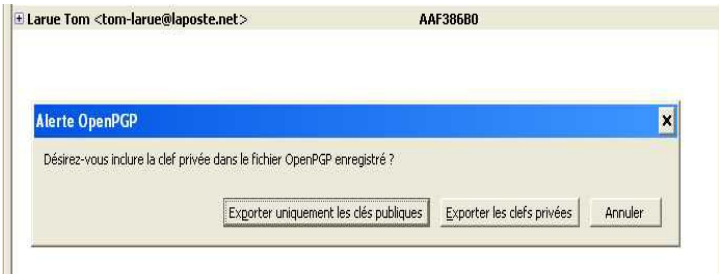
1. Envoi de sa clé publique à un destinataire

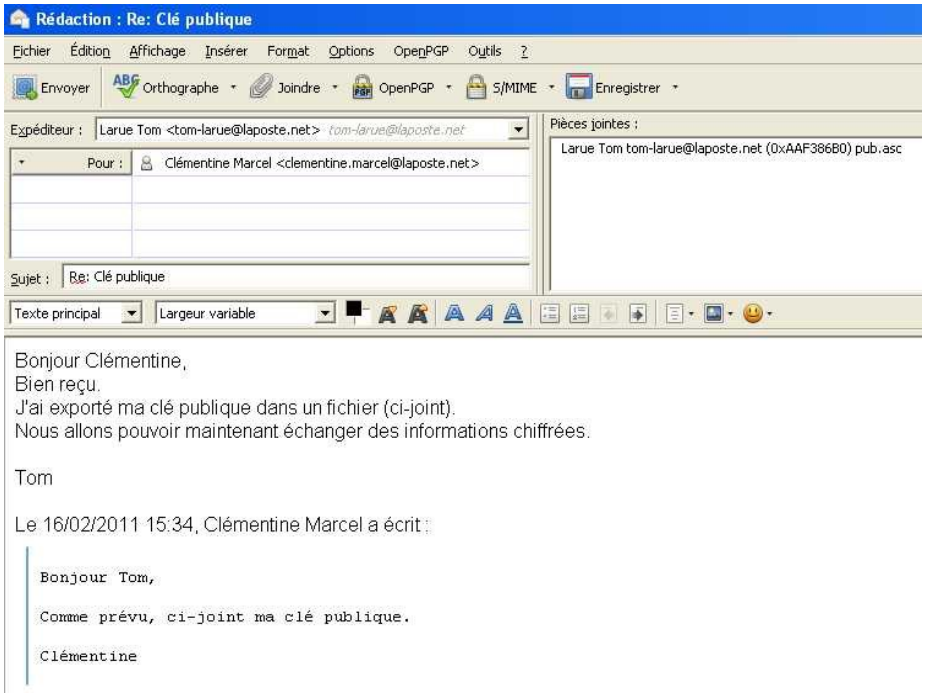
Deux possibilités :

- Soit, attacher sa clé publique à un message :



- Soit, exporter sa clé publique dans un fichier, puis le joindre à un message :

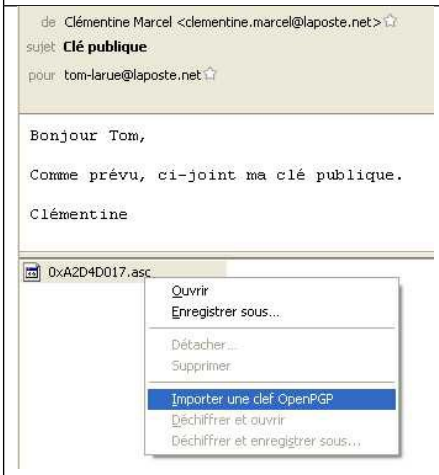




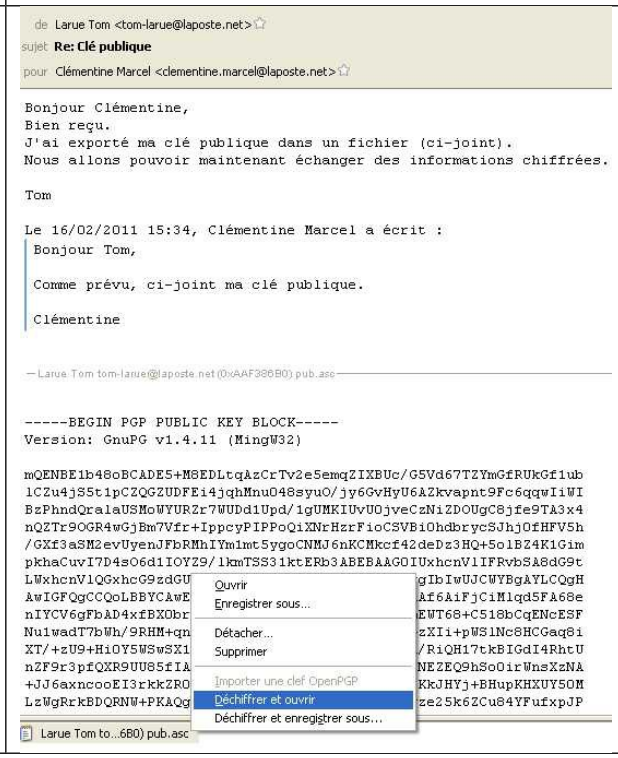
2. Réception de la clé publique d'un correspondant

➢ Dès réception de la clé publique de votre correspondant, l'importer sous Enigmail.
Plusieurs solutions sont possibles selon le contexte :

➢ Clic droit sur le fichier attaché, Importer une clé OpenPGP.



➢ Clic droit sur le fichier joint, Déchiffrer et ouvrir.



➢ Autres possibilités selon le contexte :
Menu OpenPgP, Déchiffrer/vérifier,
OU
Menu OpenPgP, Gestion des clés, puis Menu Fichier, Importer des clés depuis un fichier...

3. Vérification d'une clé publique reçue

➢ Vérifier et signer la clé publique reçue.
Contacter son correspondant et vérifier avec lui l'empreinte de la clé reçue :

- menu OpenPGP, Gestion de clés,
- clic droit sur la clé reçue, Signer la clé,

le propriétaire de la clé visualise l'empreinte de sa clé dans le menu Gestion des clés, clic droit, Propriétés de la clé.

- Si l'identité du propriétaire est certaine et si sa manière de <u>vérifier lui même les clés de ses correspondants</u> est valide, cocher "J'ai fait une vérification très poussée".

<u>Remarque sur les serveurs de clés</u>

Il est conseillé d'exporter votre clé publique sur un serveur de clés, tel que "pgp.mit.edu" par exemple afin que vos correspondants puissent la récupérer.
Il est également conseillé d'importer les clés de vos correspondants.
- Menu OpenPGP, Gestion de clés, Serveur de clés.