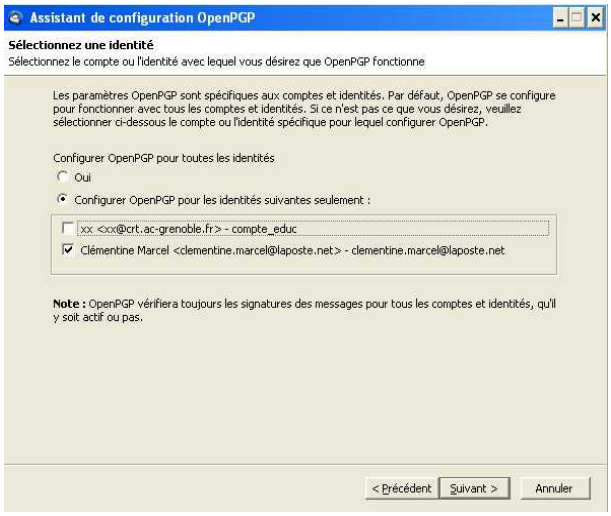
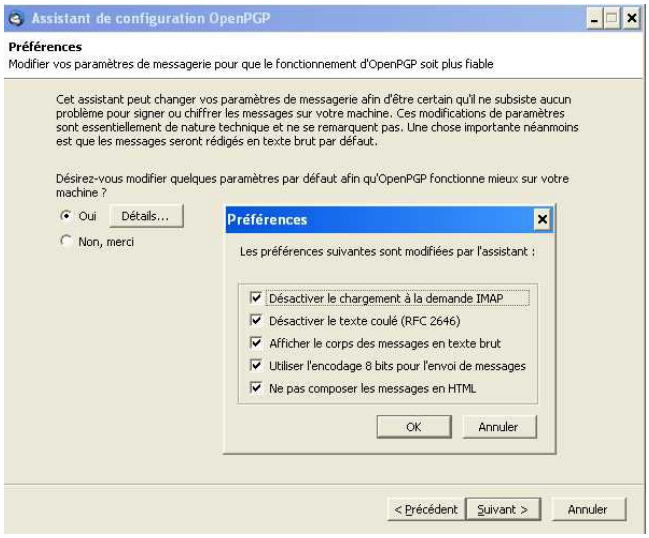
Annexe 3 - Gestion initiale des clés sous Enigmail

Cette gestion consiste à générer la ou les paires de clés asymétriques ainsi que les certificats de révocation correspondant. Un assistant permet de démarrer simplement avec ce module. Il est possible également de générer des clés sans l'assistant (cf. compléments).
Attention, lire attentivement les explications fournies par l'assistant dans la suite de la procédure.

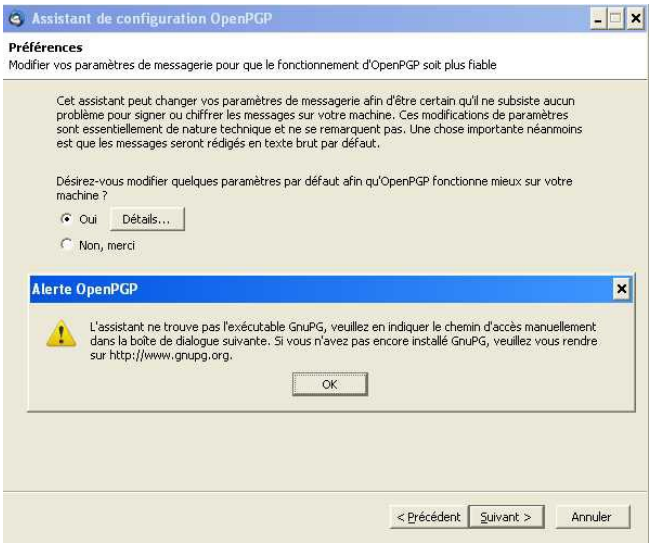
- menu OpenPgp, Assistant de configuration.
- laisser cocher "Oui, je désire que l'assistant m'aide à démarrer", Suivant.
- Identité : cocher "Configurer OpenPGP pour les identités suivantes seulement :" et cocher votre adresse.



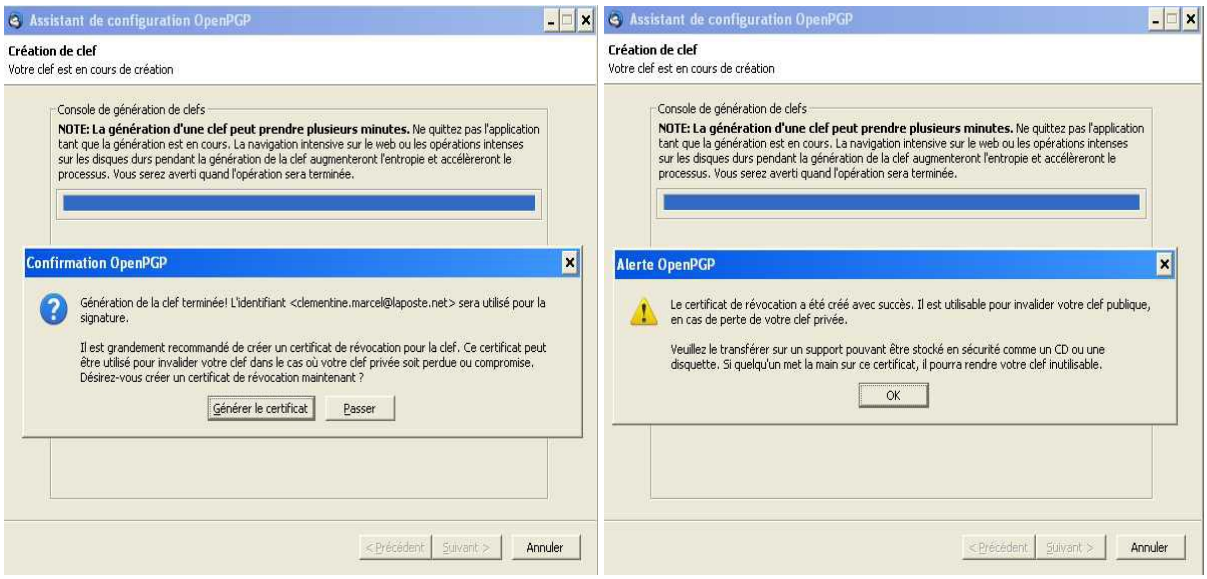
- Signatures : cocher "Oui, je veux signer tous mes messages", Suivant.
- Chiffrement : cocher "Non, je préfère créer des règles par destinataire pour ceux dont je possède la clé publique".
- Préférences : cocher "Oui", voir "Détails" pour plus d'information, Suivant.



Remarque : si l'application GnuPG n'a pas été installée, l'assistant ne peut pas générer les clés.



- Créer une clé : saisir votre phrase secrète OpenPGP pour générer la paire de clés.
  L'assistant vous propose ensuite de créer un certificat de révocation.
- "Générer le certificat".



Compléments

- Si l'assistant ne parvient pas à créer le certificat de révocation, il est possible de le créer manuellement soit à partir du Menu OpenPGP, soit en ligne de commande à l'aide de l'application GnuPG[1] :

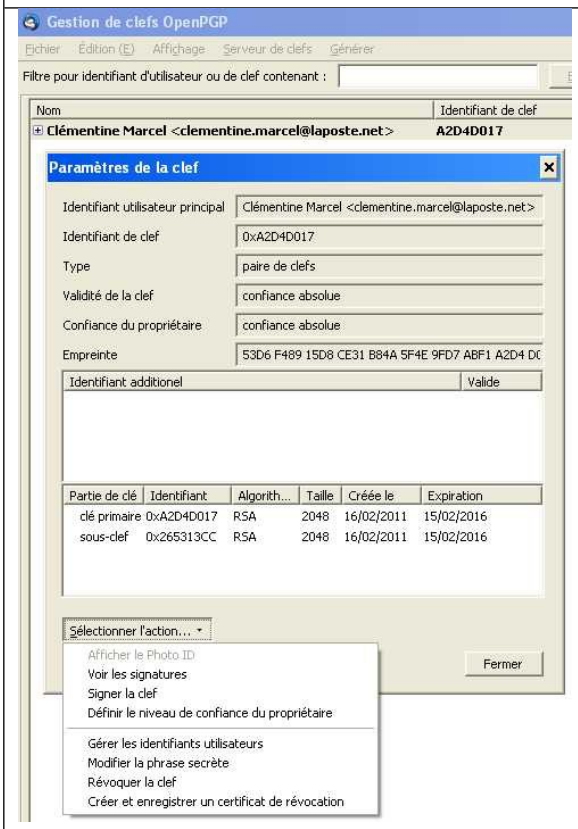
Pré-requis pour la solution en ligne de commande

Paramétrer l'invite de commande en mode d'édition rapide :
- Démarrer, Exécuter, saisir "cmd"
- Clic en haut à gauche de la fenêtre, Propriétés, cocher "Mode d'édition rapide", puis "Enregistrer les fenêtres futures ayant le même titre".

[1] GnuPG est installé par défaut dans "C:\Program Files\GNU\GnuPG". Pour accéder à l'aide, saisir dans une invite de commande : gpg.exe --help

1. À partir du menu OpenPGP

- Menu OpenPGP, Gestion de clés.
- Clic droit, Propriétés sur la clé, Créer et enregistrer un certificat de révocation.



2. En ligne de commande

- Ouvrir une invite de commande
- Exécuter la commande :
  "C:\Program Files\GNU\GnuPG\gpg.exe" --gen-revoke <Identifiant de clé>.

```
C:\Documents and Settings\coordo2>"C:\Program Files\GNU\GnuPG\gpg.exe" --gen-rev
oke 0xA2D4D017

sec  2048R/A2D4D017 2011-02-16 Clémentine Marcel <clementine.marcel@laposte.net>


Générer un certificat de révocation pour cette clé ? (o/N) o
choisissez la cause de la révocation:
  0 = Aucune raison spécifiée
  1 = La clé a été compromise
  2 = La clé a été remplacée
  3 = La clé n'est plus utilisée
  Q = Annuler
(Vous devriez sûrement sélectionner 1 ici)
Votre décision ? 1
Entrez une description optionnelle ; terminez-là par une ligne vide:
>
Cause de révocation: La clé a été compromise
(Aucune description donnée)
Est-ce d'accord ? (o/N) o

Vous avez besoin d'une phrase de passe pour déverrouiller la
clé secrète pour l'utilisateur: « Clémentine Marcel <clementine.marcel@laposte.n
et> »
clé de 2048 bits RSA, ID A2D4D017, créée le 2011-02-16

sortie avec armure ASCII forcée.
Certificat de révocation créé.

Déplacez-le dans un support que vous pouvez cacher ; si Mallory a
accès à ce certificat il peut l'utiliser pour rendre votre clé
inutilisable.
Une bonne idée consiste à imprimer ce certificat puis à le stocker
ailleurs, au cas où le support devient illisible. Mais attention :
le système d'impression de votre machine pourrait stocker ces
données et les rendre accessibles à d'autres personnes !
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (MingW32)
Comment: A revocation certificate should follow

iQEfBCABAgAJBQJNW933Ah0CAAoJEJ/Xq/Gi1NAX+tIIAJyK5pGhBshGUwq6yJKs
aBMMJ7xA/GkRhCjKZ0k5pLs71Ujs3nUxqDpwCXUzNE5Z8GtTUIp1UvPWz0Ue162u
3LVb1nZMevEMiDrBqysfxwffLU54POHjPDvDMgw3ipQItfboi8xGnd7gubJ0w0w+
7T6QFgozri3wy+GtW0iK2QGJSWlBiS7D5CGfbbz58xhZU7mPnh3fxDgDrJvag45
rrxAjHJgCJUAFvtAkxFUuCrGvXPbGXsWUACMZ2QGk29ZvtnfwBGsrrKjb2YDAxJ6
lVXMfZl0NcytqiNY75rz1GMW4ZuGZjI6e/4X8twh3wwpqxEOUG5POGtEAmcP10Ln
4GQ=
=Bwb5
-----END PGP PUBLIC KEY BLOCK-----
```

- Copier le bloc commençant par "-----BEGIN PGP" dans un fichier texte (à conserver en lieu sûr).

- Générer des clés sans assistant :
  menu OpenPGP, Gestion des clés, puis menu Générer, Nouvelle paire de clés.