Seahorse et GPG

Genma

10 septembre 2013

A propos de moi

Où me trouver sur Internet ?

- Le Blog de Genma :
  http ://genma.free.fr
- Twitter : http ://twitter.com/genma

Mes centres d'intérêts ?

Plein de choses dont :

- La veille technologique
- Le chiffrement
- Le cryptoanarchisme

But de cette présentation

Ce que cette présentation est

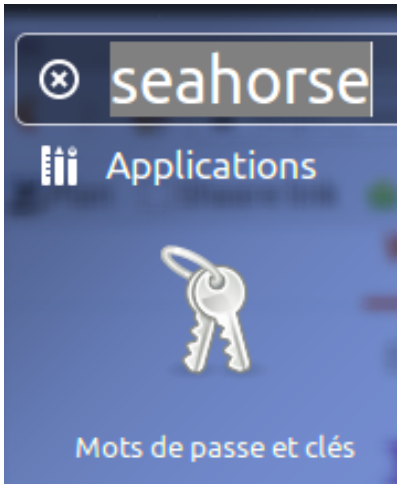
Cette présentation est est un tutoriel sur la création d'une clef GPG de façon graphique en utilisant le logiciel Seahorse disponible sous Ubuntu.
$\Rightarrow$ La clef crée étant alors utilisée pour envoyer/recevoir des mails chiffrés via Thunderbird.

Ce que cette présentation n'est pas

Une explication de GPG, de son principe (clef publique/clef privée). Une connaissance du principe de GPG est nécessaire.

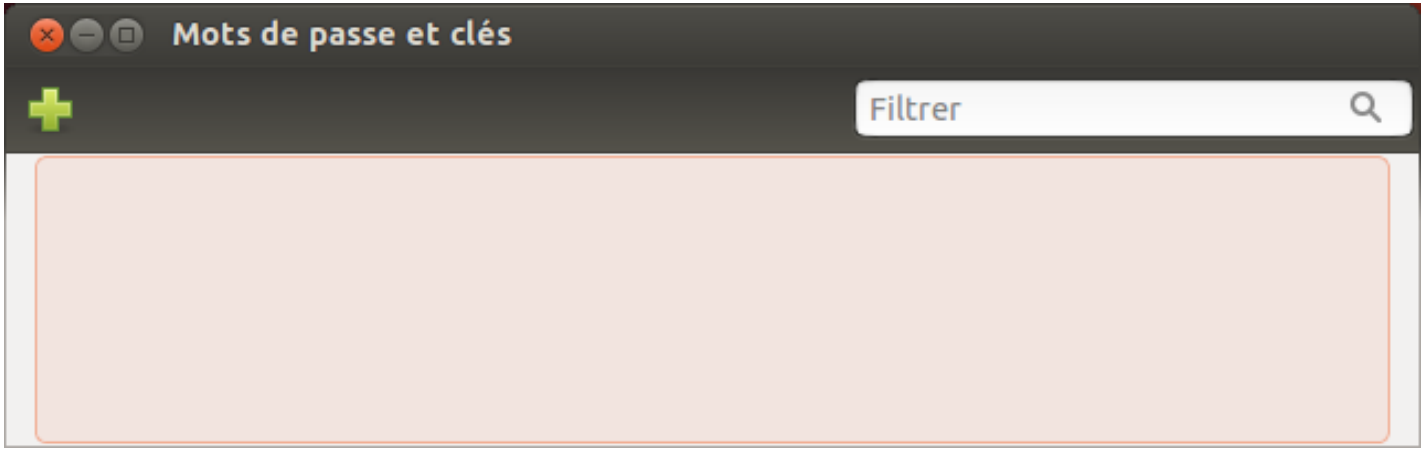
Seahorse

Seahorse - Lancement



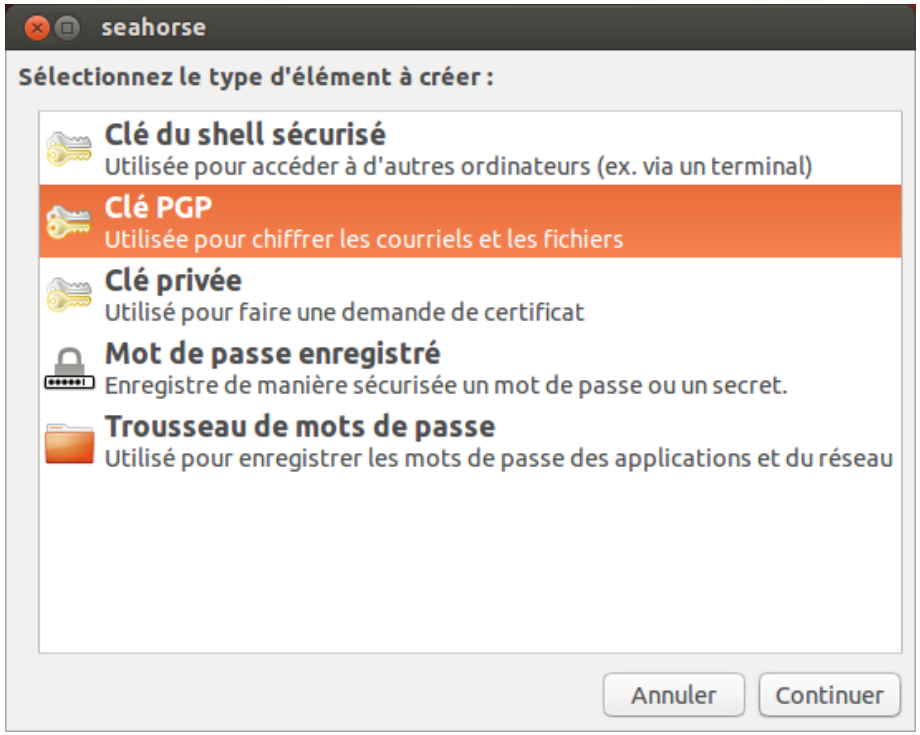
- Pour lancer Searhose, il suffit de taper Seahorse ou de chercher Mots de passes et clés et de valider.

Seahorse - premier lancement



- Au premier lancement, par défaut, l'interface ne contient aucune clef. On va donc en créer une.

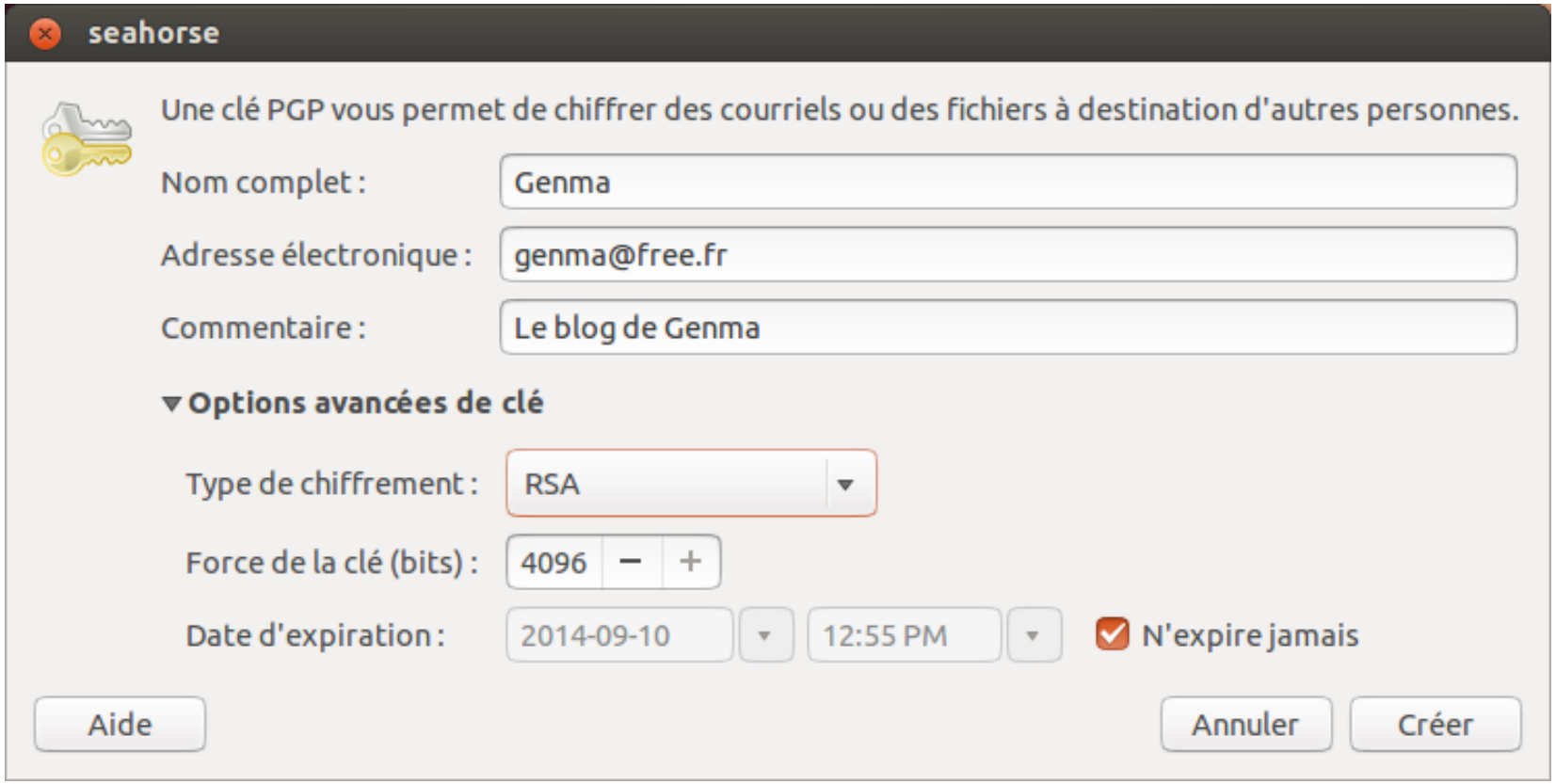
Searhose - choix de la création d'une clef GPG



- On choisira Clé GPG.

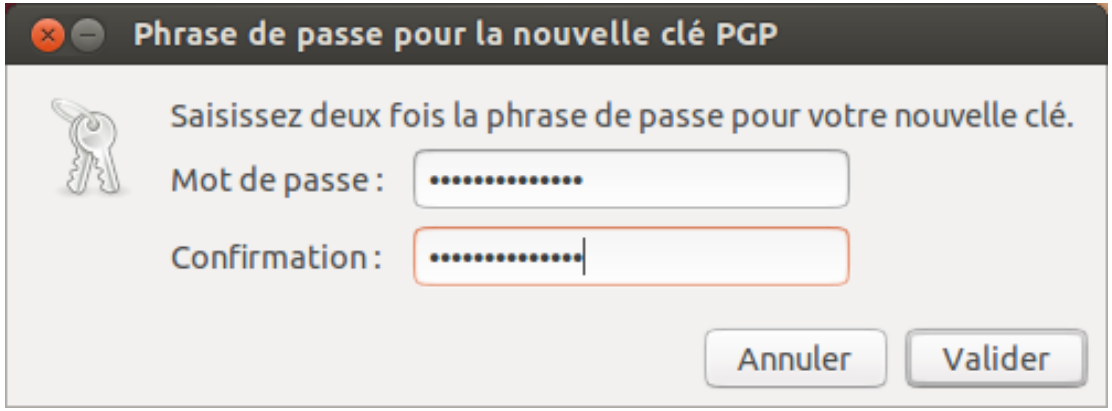
⇒ Seahorse permet aussi de gérer ses clefs SSH, mais ce n'est pas le but de cette présentation.

Searhose -informations sur l'utilisateur



- Différents champs sont à remplir.
- Les deux options importantes sont ici la taille de la clef (4096) et la date d'expiration.

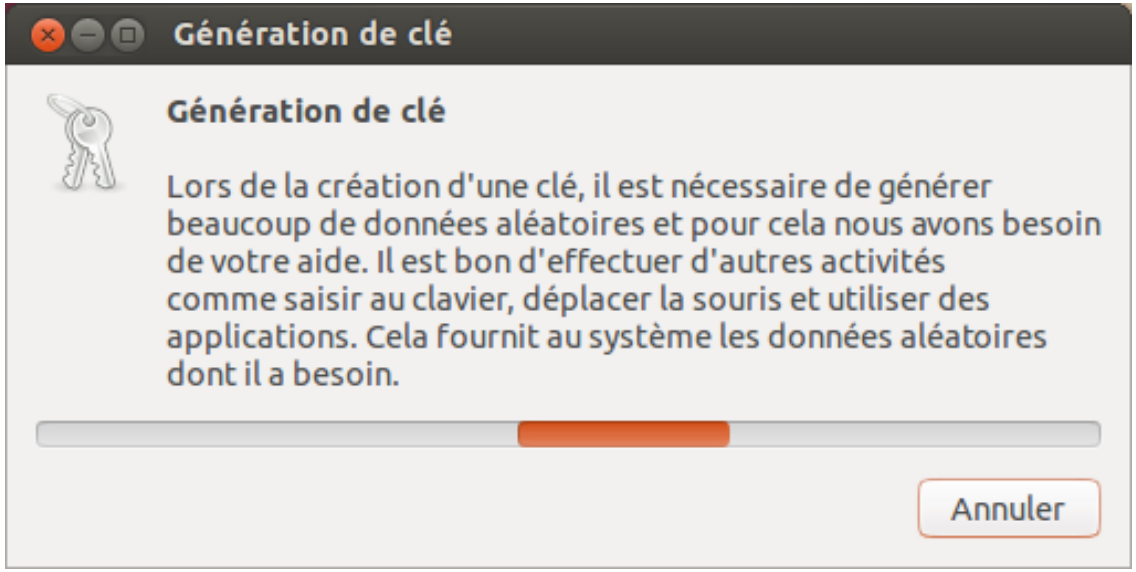
Searhose - la passphrase



- Il faut alors saisir le mot de passe qui sera utilisé par la suite à chaque utilisation de la clef.

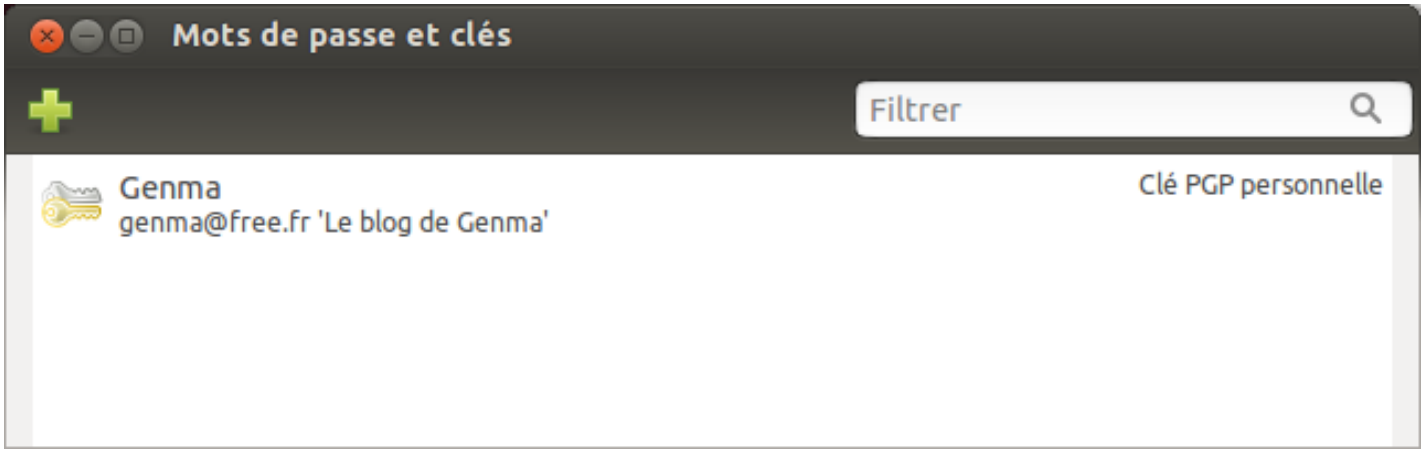
⇒ Plus le mot de passe est compliqué et long (avec des caractères spéciaux, des chiffres), mieux c'est.
⇒ ExempleDeMotDePasse*1979@

Searhose - génération de la clef



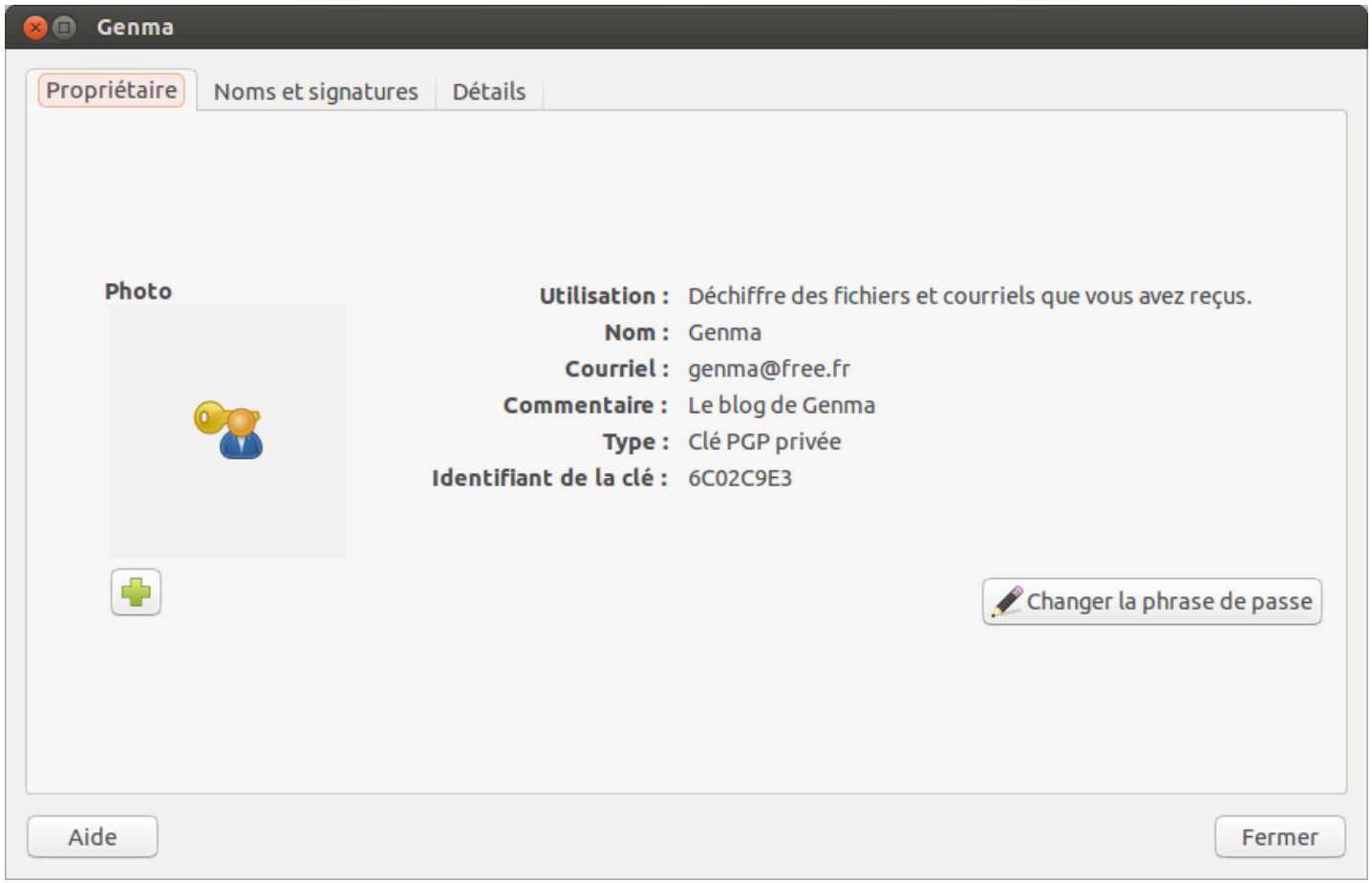
- La génération de la clef commence. Comme il est conseiller de générer de l'aléatoire, personnellement, je lance la commande "ls -R /" dans un terminal.

Searhose - clef crée

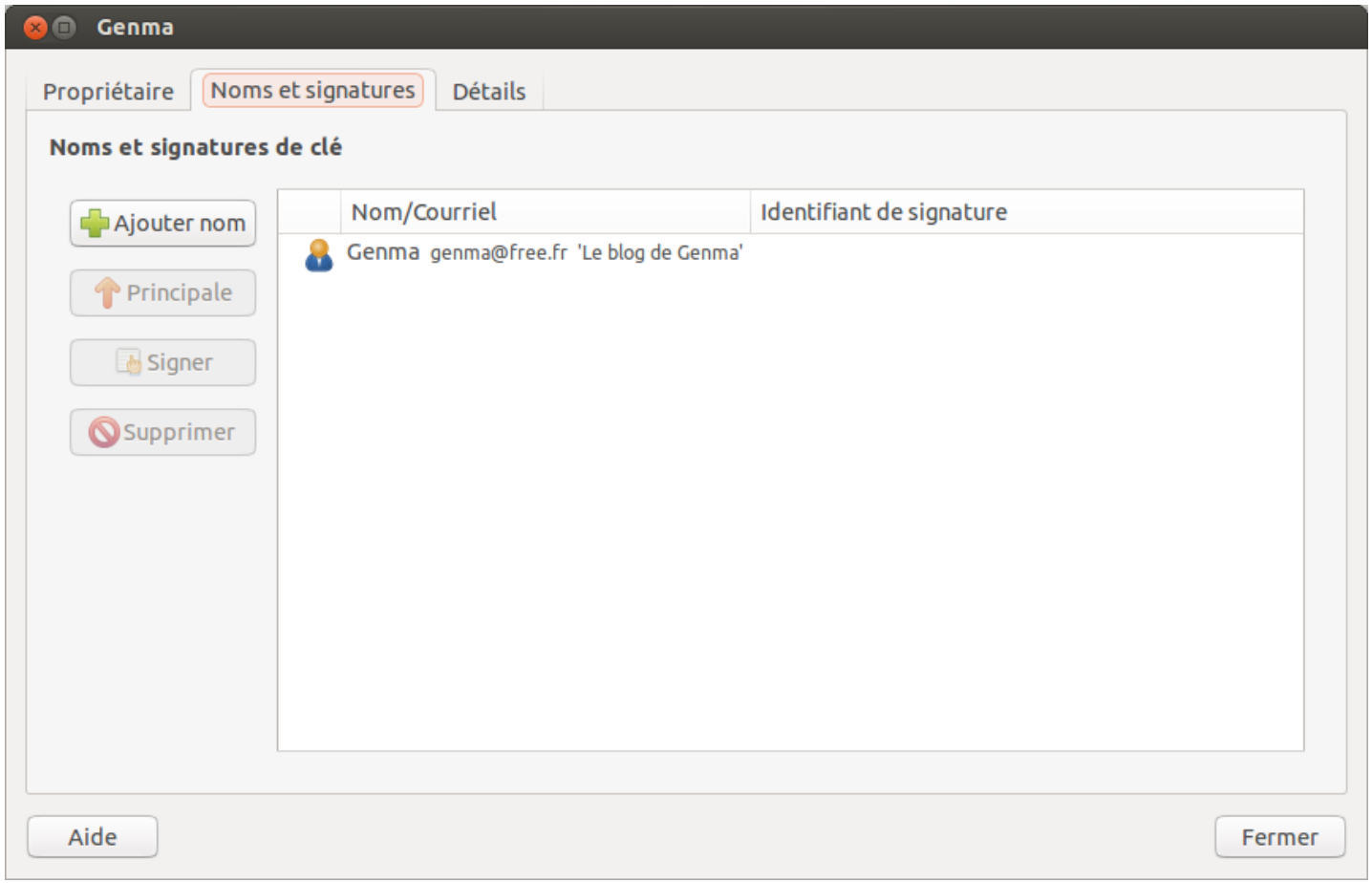


- Une fois la clef créée, elle apparait dans la liste des clefs.

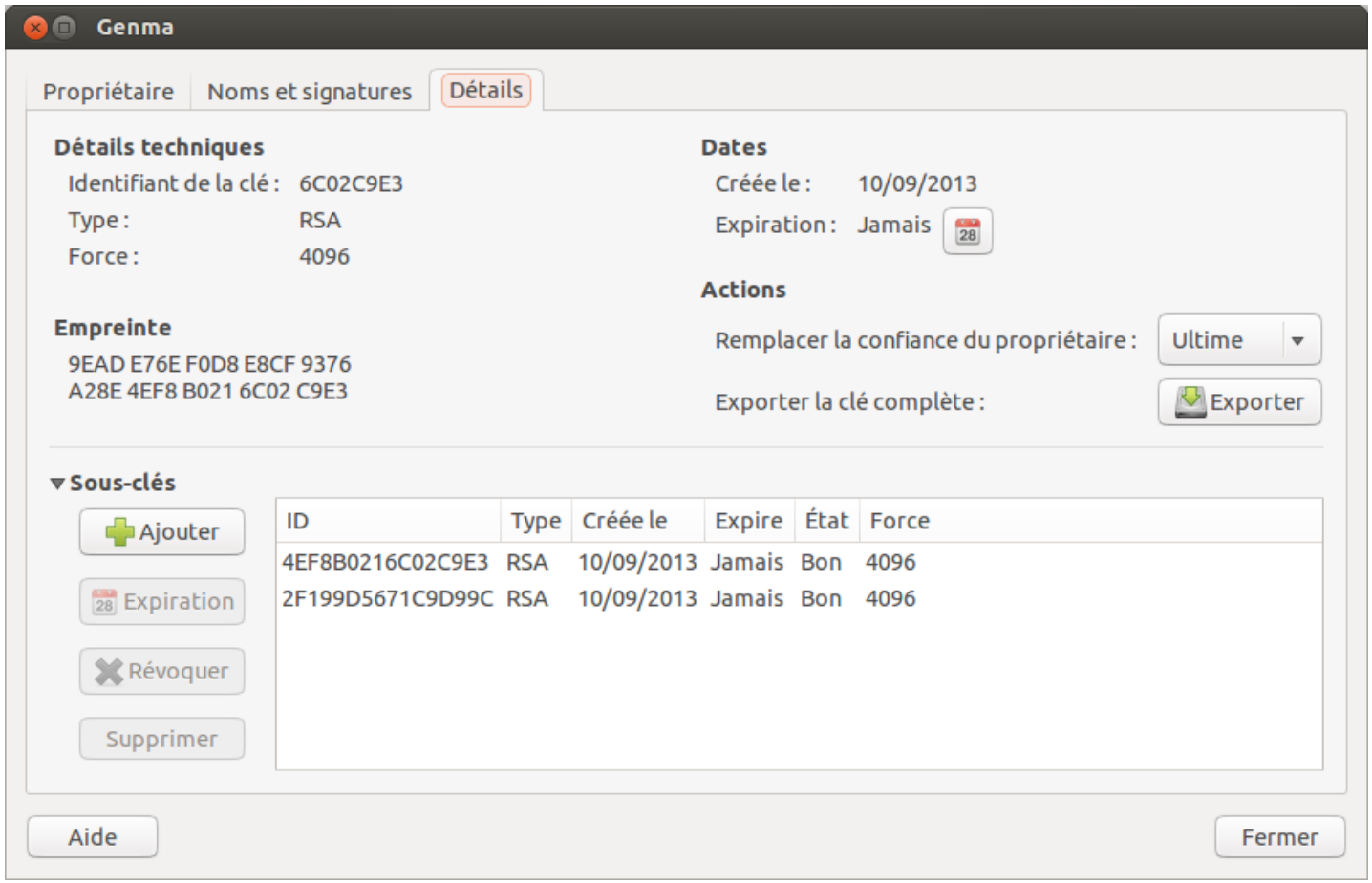
Searhose - détail de la clef 1/3



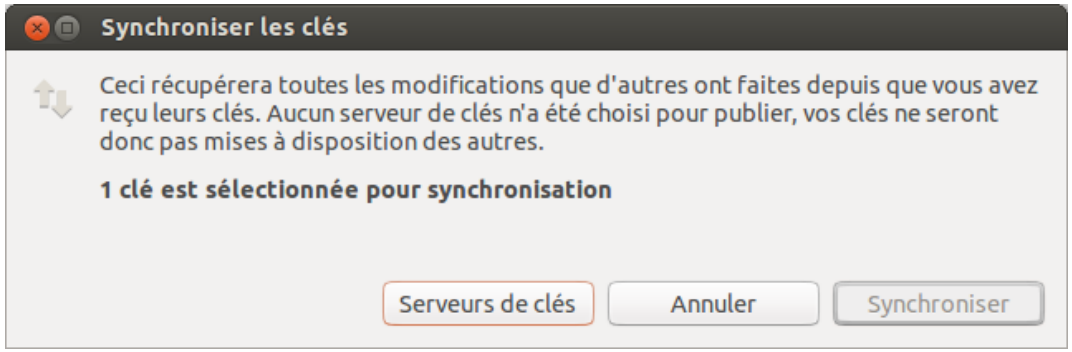
Searhose - détail de la clef 2/3



Searhose - détail de la clef 3/3

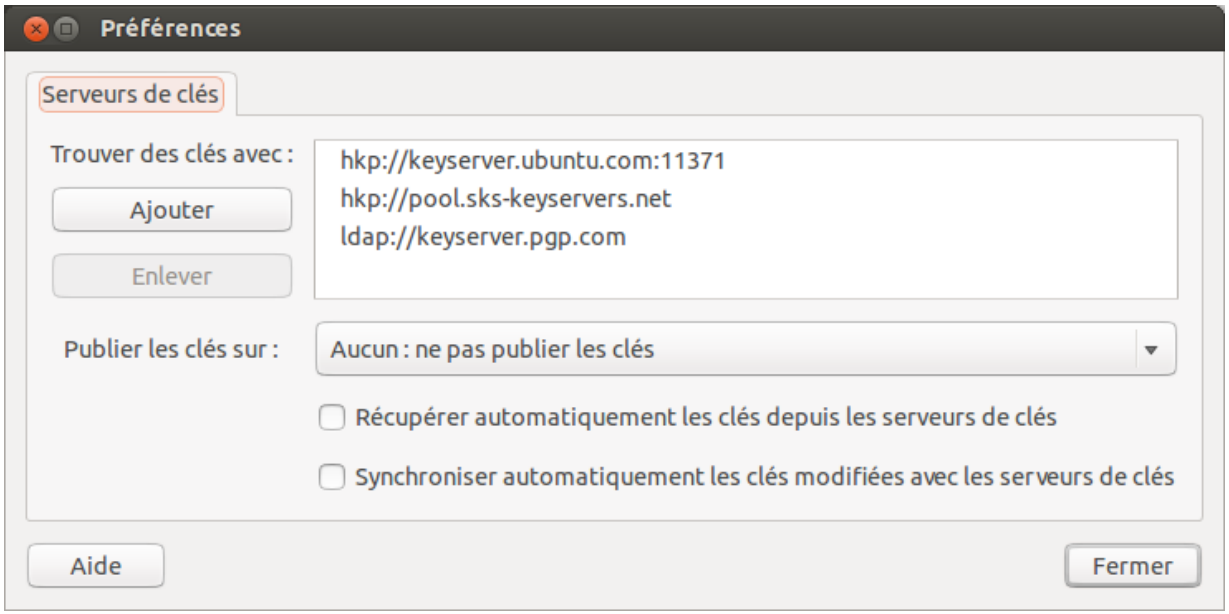


Searhose - Publication de la clef



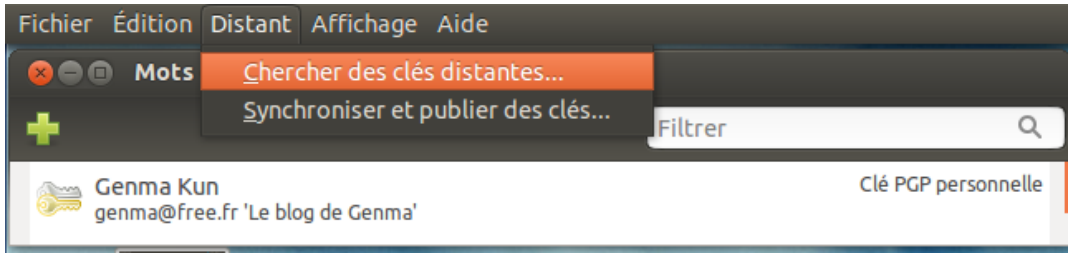
- Pour que la clef publique soit connu et accessible à quiconque souhaite pouvoir nous envoyer un mail chiffré, il faut publier la clef sur les serveurs de clefs.

Searhose - Publication de la clef



- Il est possible de choisir les serveurs de clefs, d'en ajouter. Par défaut, les principaux sont présents.

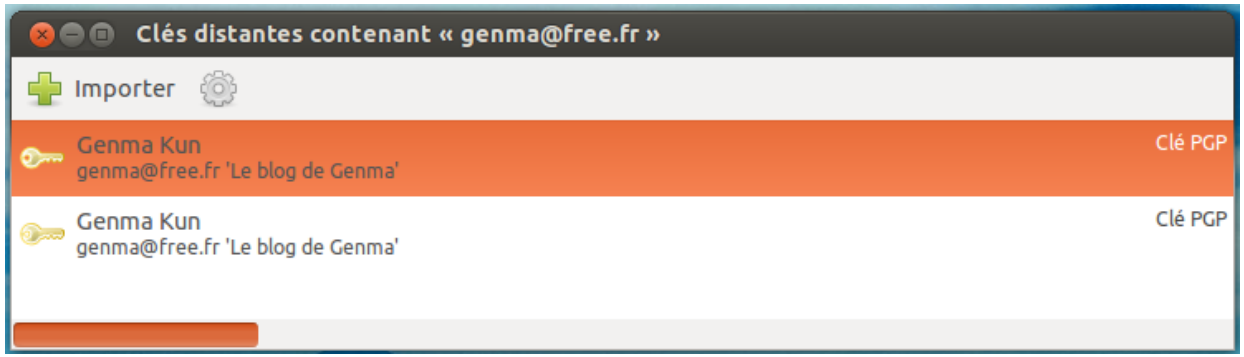
Searhose - Recherche de clefs 1/3



- Pour écrire à quelqu'un dont on ne connait pas encore la clef GPG, on peut rechercher sa clef publique.

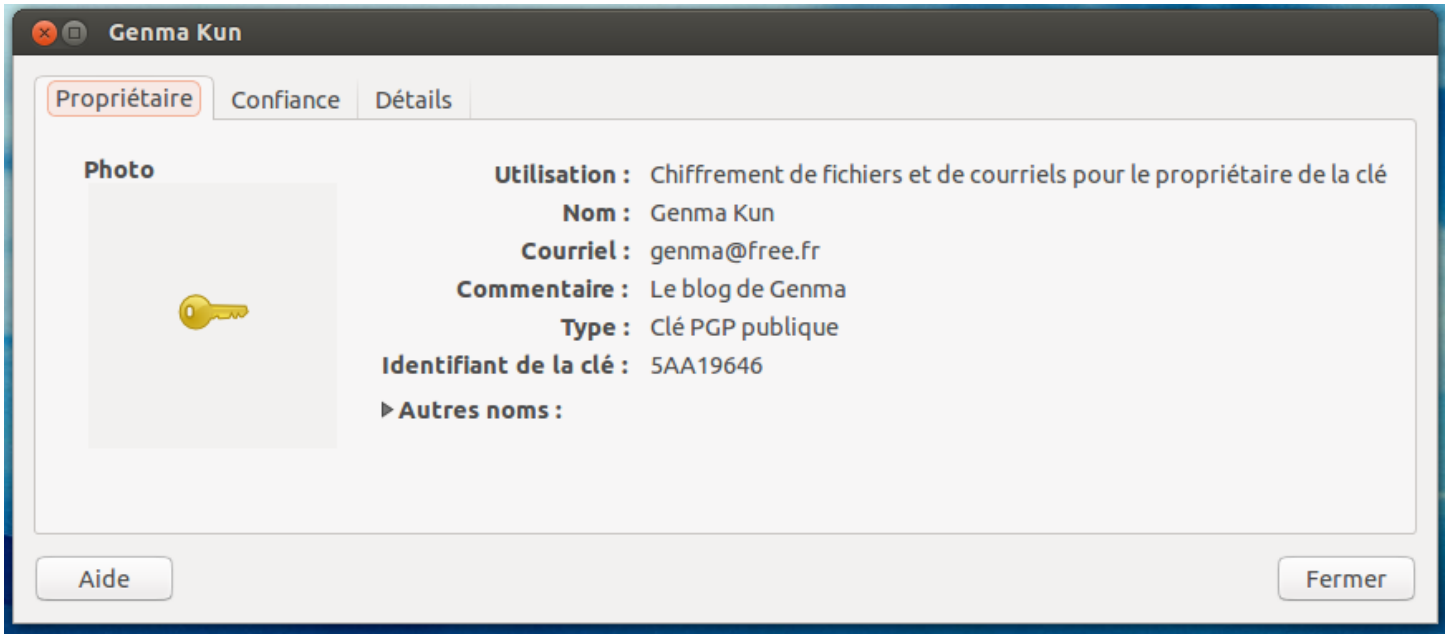
Searhose - Recherche de clefs 2/3

Searhose - Recherche de clefs 3/3



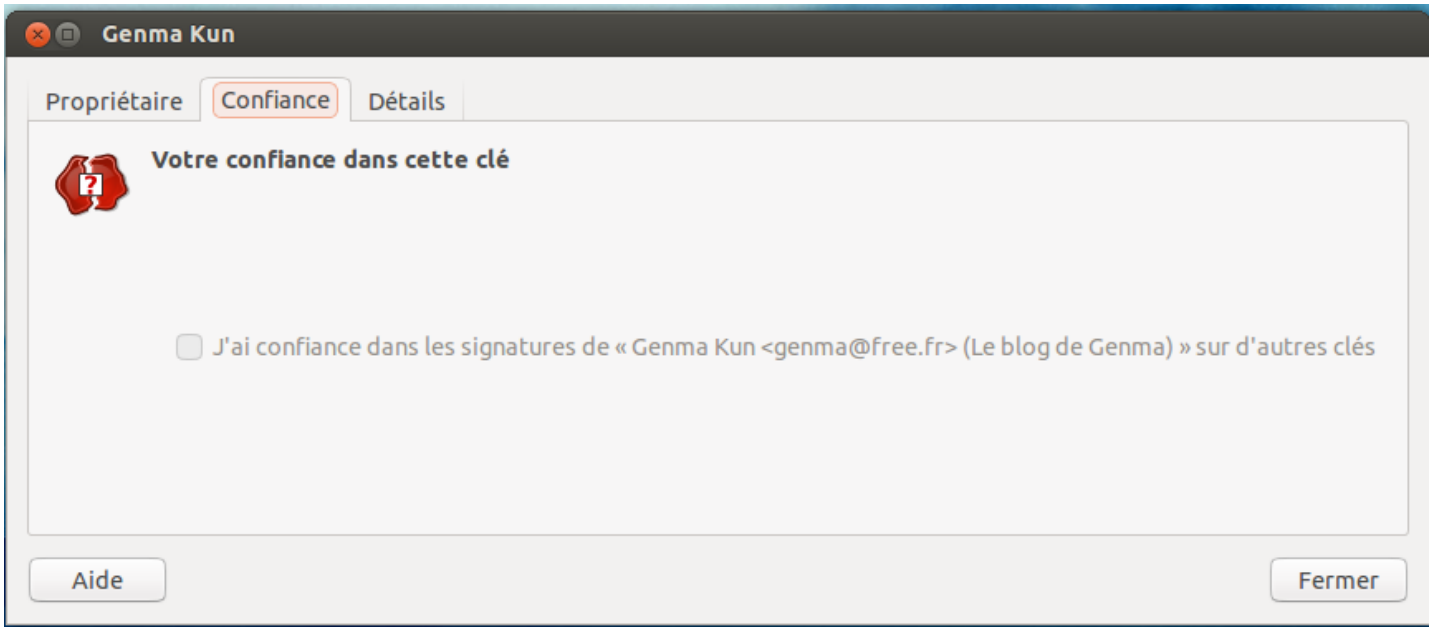
- Les clefs correspondantes sont alors proposées et on peut les ajouter à son trousseau de clefs.

Searhose - Détail d'une clef publique 1/3



- Pour une clef publique, on peut voir les détails de la clef.

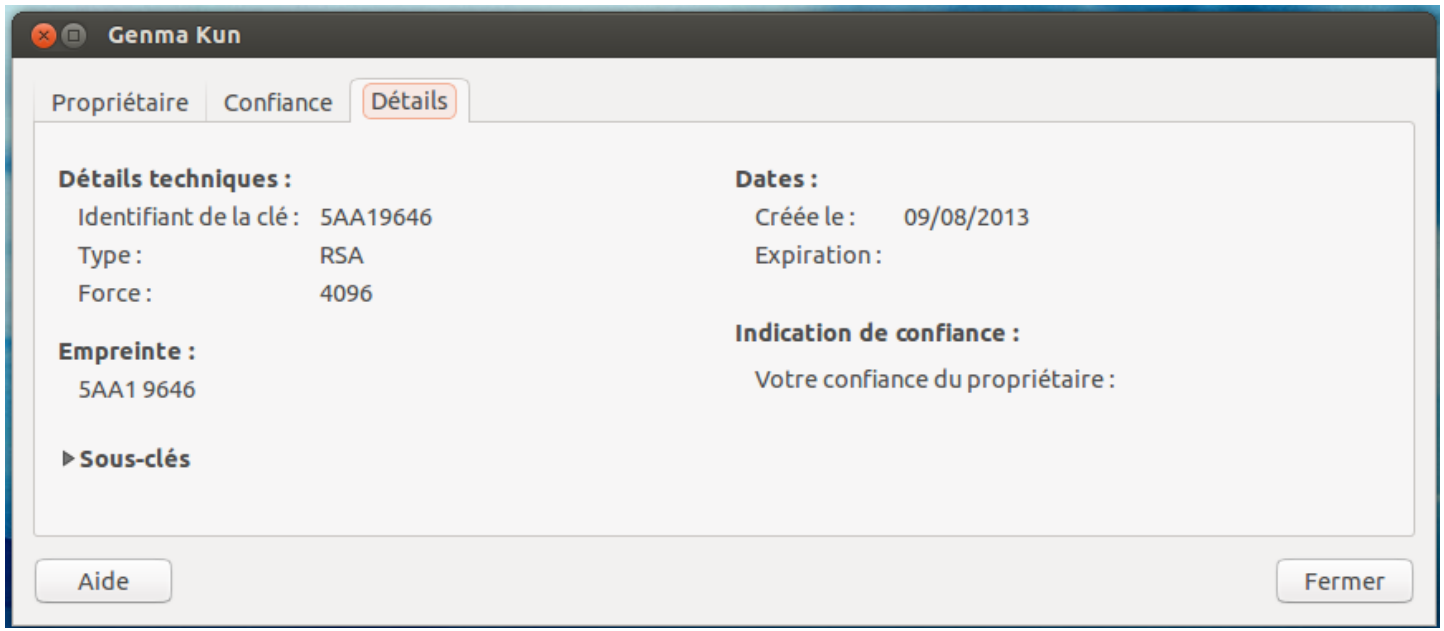
Searhose - Détail d'une clef publique 2/3



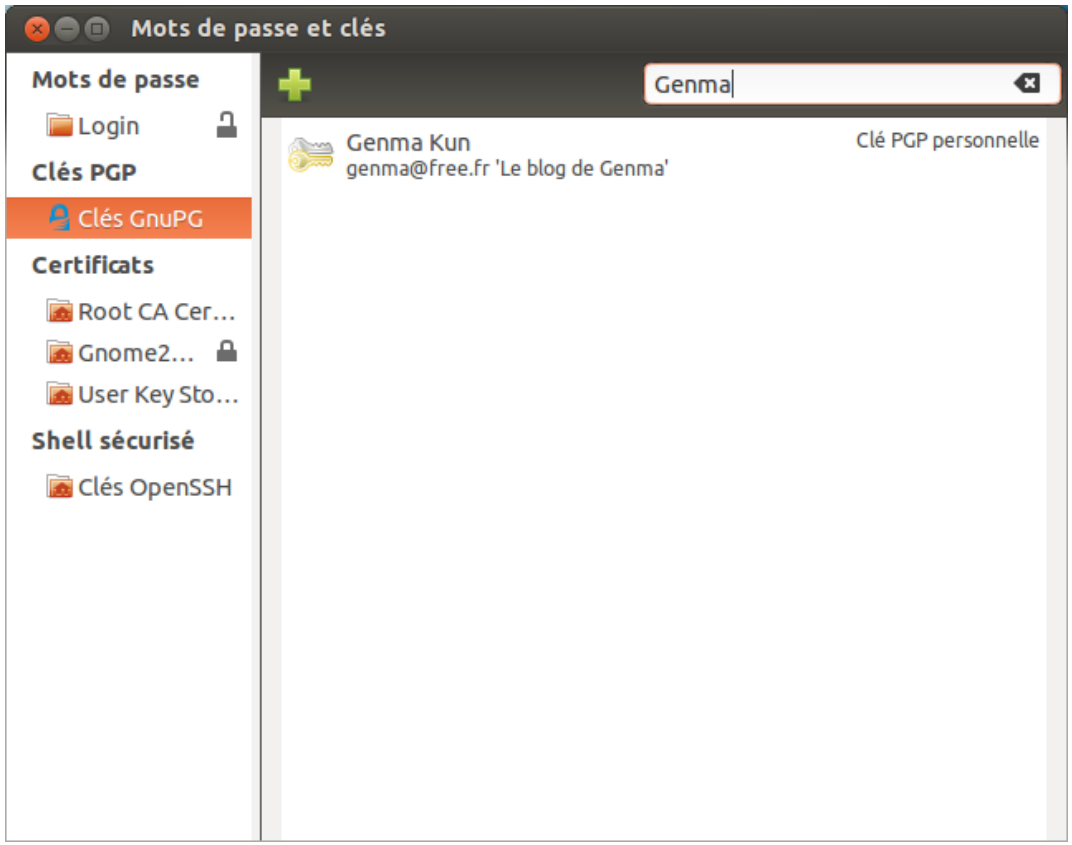
- On voit apparaitre ici la notion de confiance en la clef.

⇒ On valide la clef de quelqu'un lors d'une cryptopartie et on signe alors sa clef avec la notre pour dire : oui, cette clef est bien à celui à qui elle appartient.

Searhose - Détail d'une clef publique 3/3

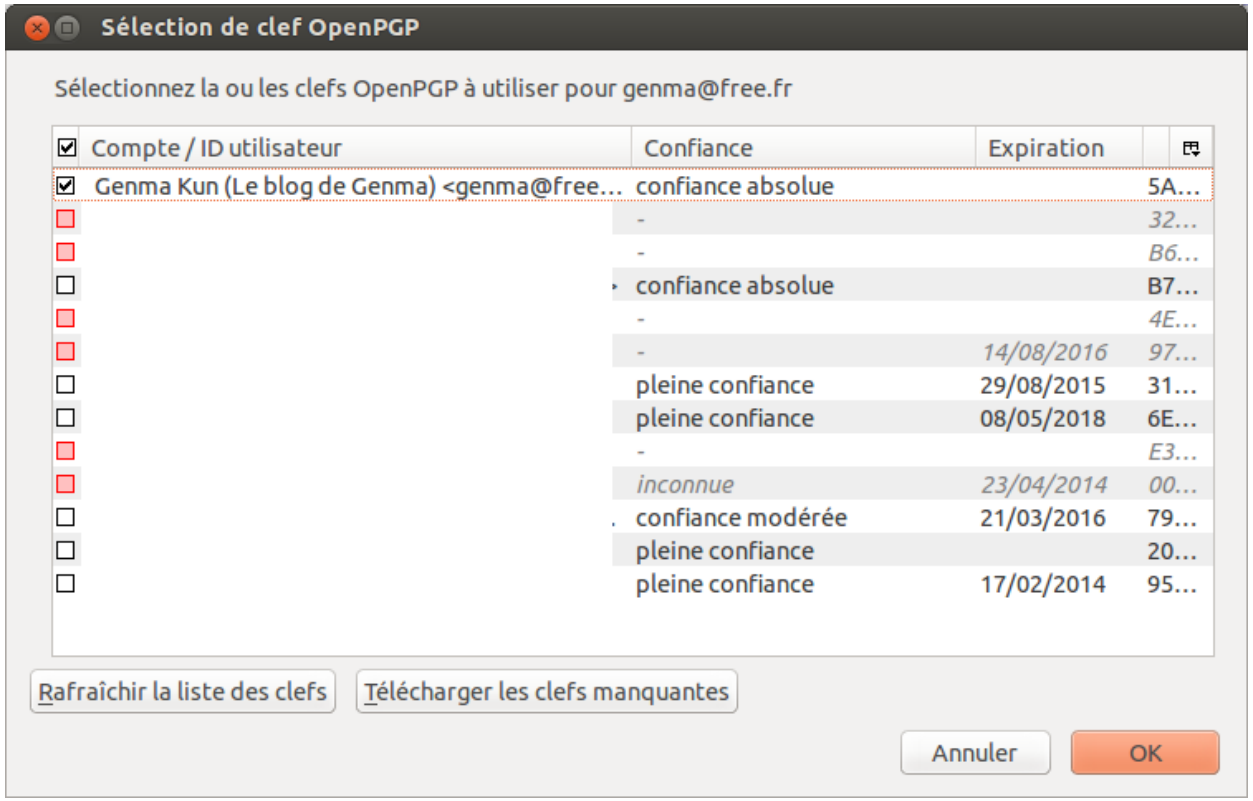


Searhose -Gestion de son trousseau 1/2



⇒ Il est possible de chercher une clef dans son trousseau.

Searhose -Gestion de son trousseau 2/2



⇒ Ou de voir toutes les clefs et la confiance que l'on a dans ces clefs.

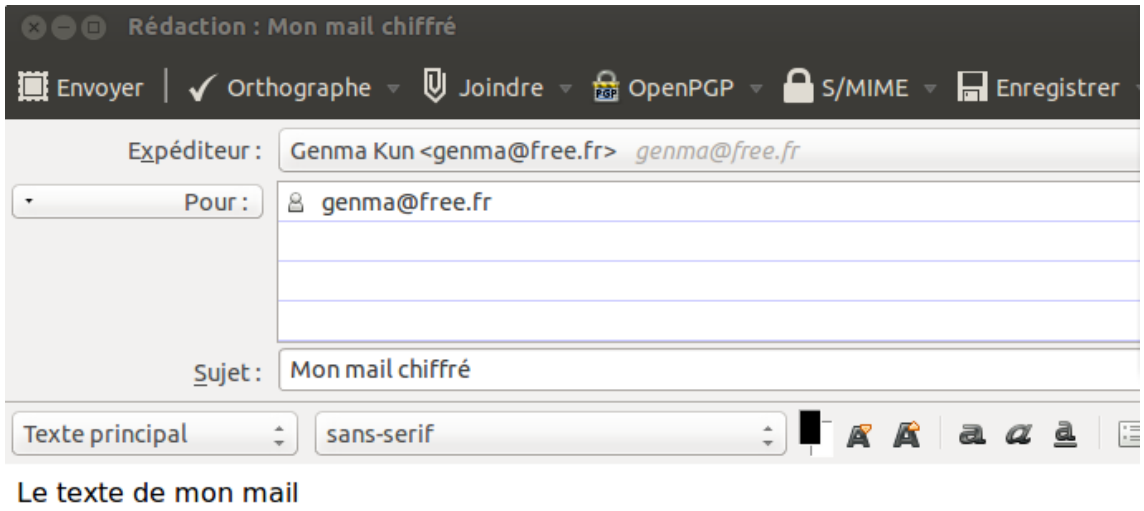
Thunderbird

Thunderbird - Enigmail

- Dans Thunderbird, il suffit d'ajouter l'extension Enigmail.

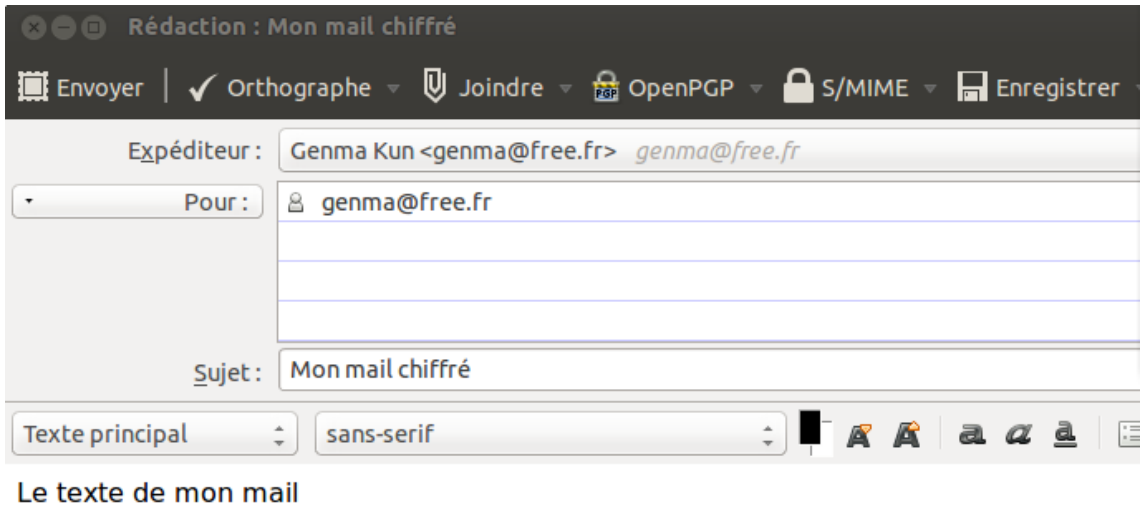
A COMPLETER - A CONTINUER

Thunderbird - Création d'un mail chiffré



- La création d'un mail dans Thunderbird se fait de la même façon qu'un e-mail classique.
- Dans le menu OpenPGP, on peut choisir de signer le mail ou de le chiffrer.

Thunderbird - Envoi/Réception d'un mail chiffré



- A l'envoi du mail (ou à la reception d'un mail chiffré), il est demandé de saisir son mot de passe de sa clef GPG.

A COMPLETER - A CONTINUER

A COMPLETER - A CONTINUER

SAUVEGARDER SES CLEFS GPG
A COMPLETER - A CONTINUER