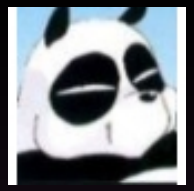
Seahorse et clefs PGP

Genma

24 décembre 2013



A propos de moi

Où me trouver sur Internet ?

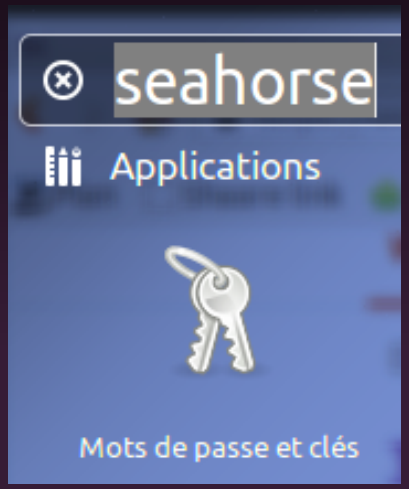
- Le Blog de Genma :
  http ://genma.free.fr
- Twitter :
  http ://twitter.com/genma

Mes centres d'intérêts ?

Plein de choses dont :

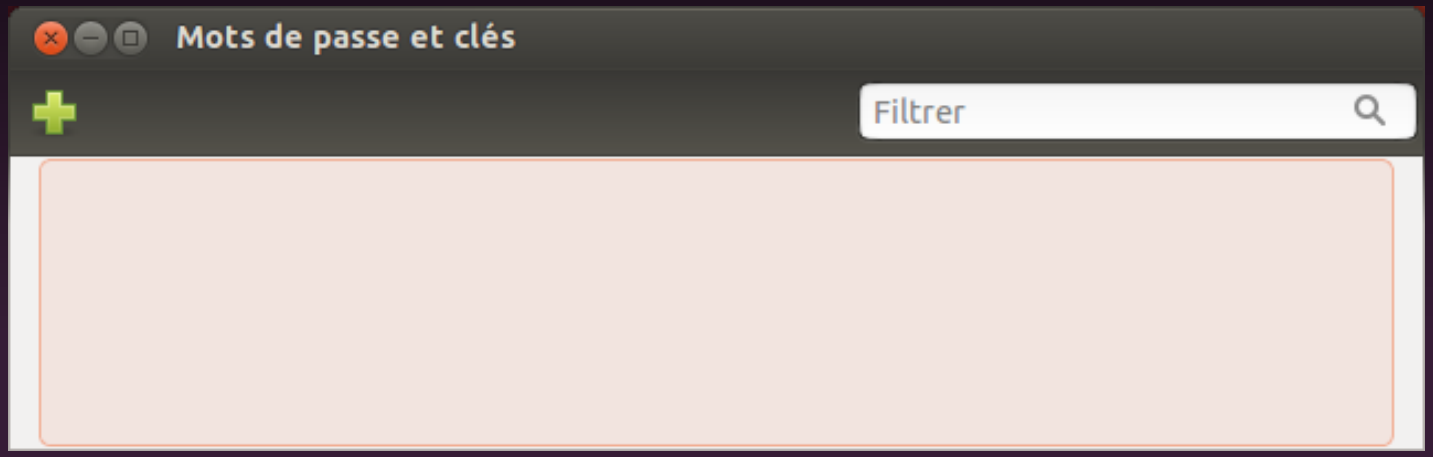
- La veille technologique
- Le chiffrement

Seahorse - lancement



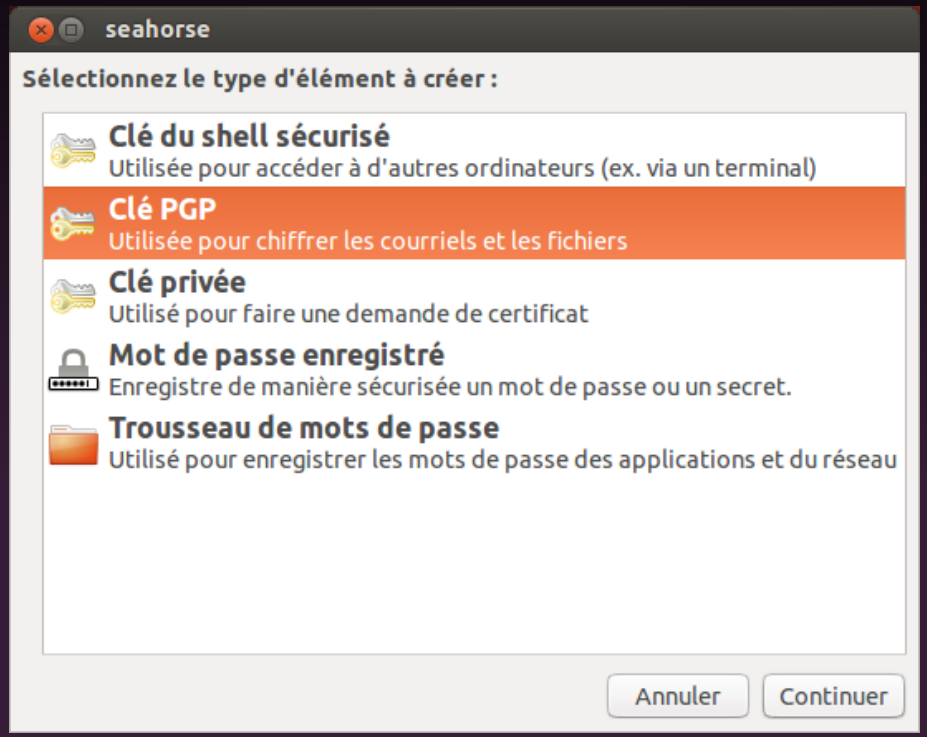
- Pour lancer Seahorse, il suffit de le chercher dans le dash en y tapant "Seahorse" ou "Mots de passes et clés" et de valider.

Seahorse - premier lancement



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

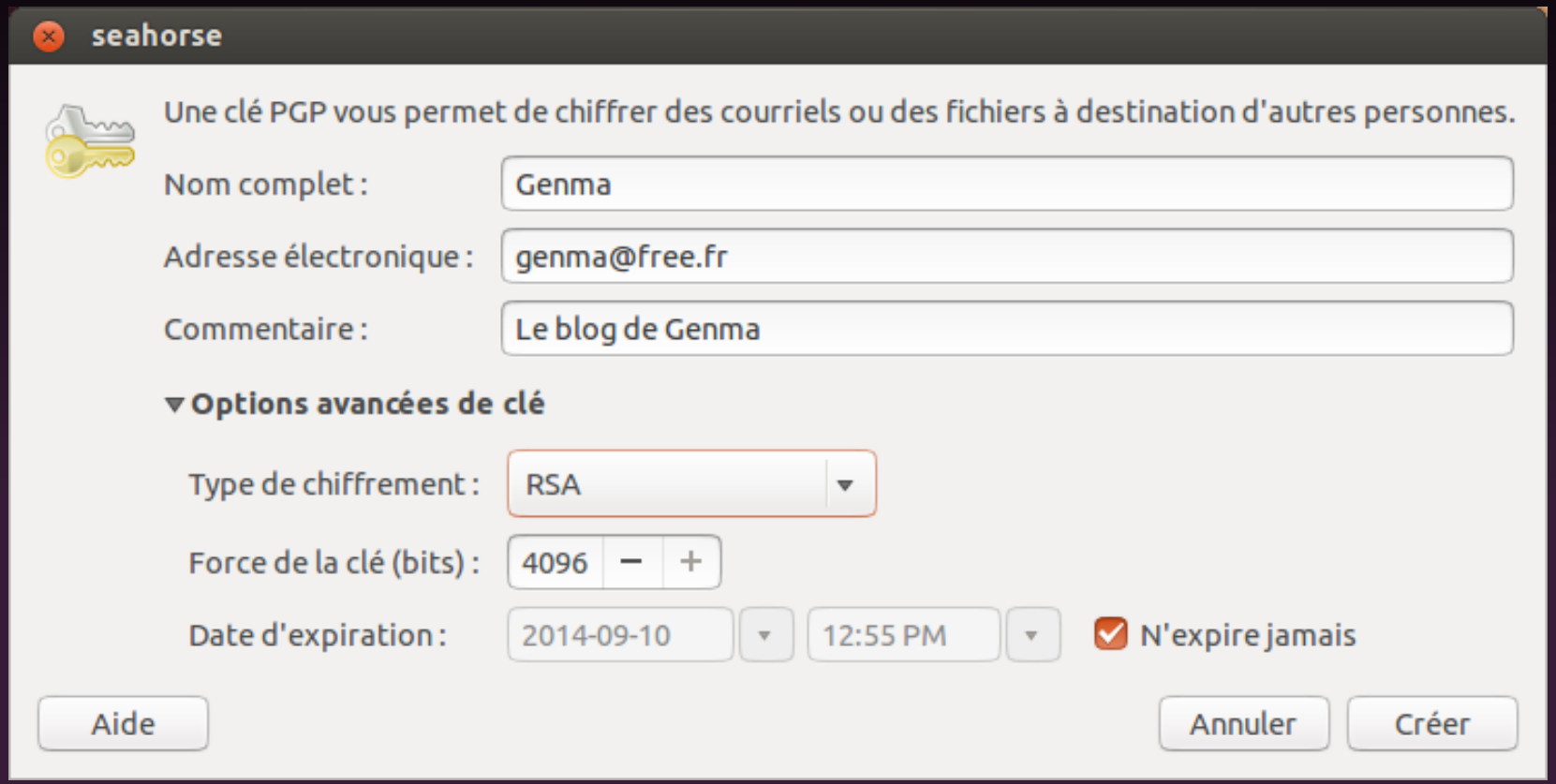
Searhose - choix de la création d'une clef PGP



- On choisira Clé PGP .

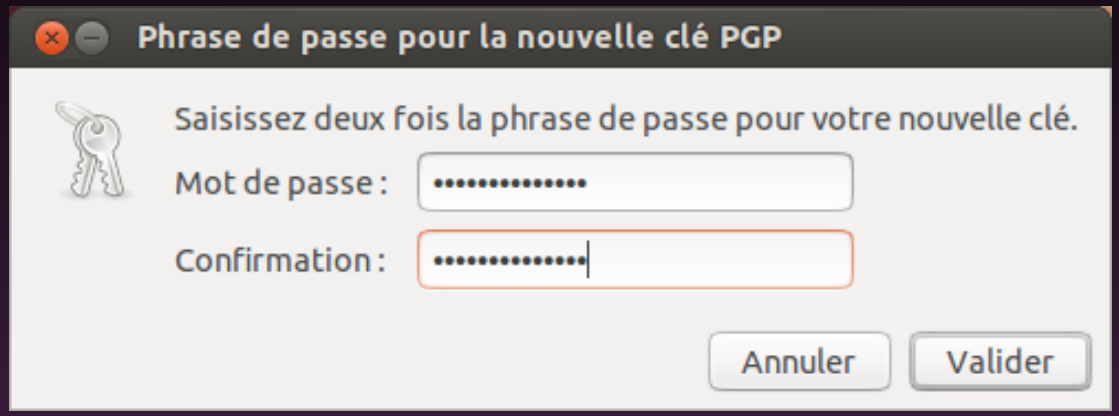
Rq : Seahorse permet aussi de gérer ses clefs SSH, mais ce n'est pas le but de cette présentation.

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.

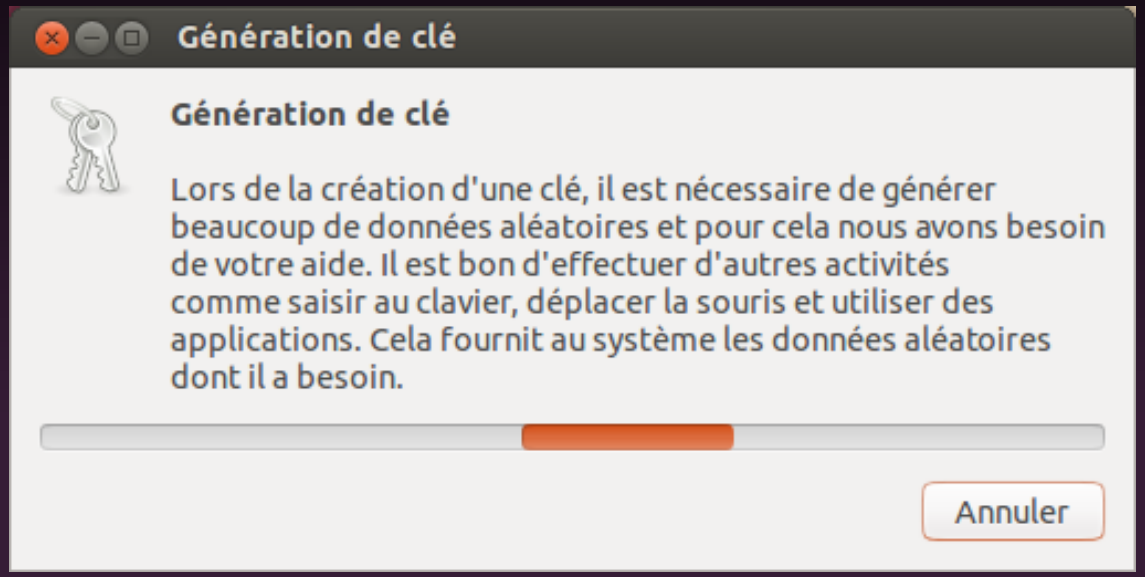
Searhose - la passphrase



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

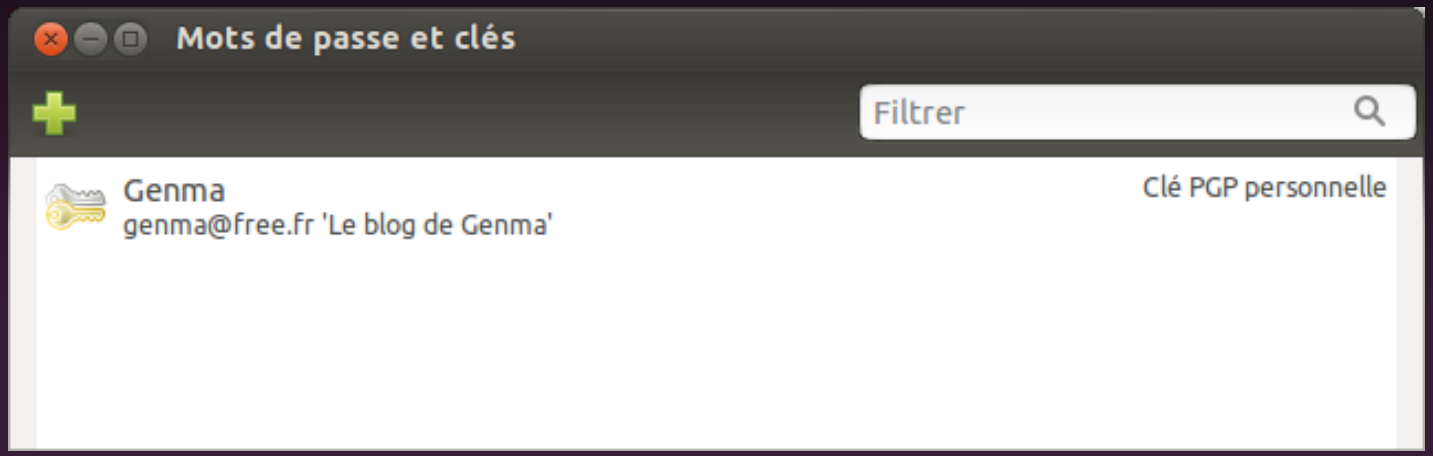
⇒ Plus le mot de passe est compliqué et long (avec des caractères spéciaux, des chiffres), mieux c'est.
⇒ ExempleDeMotDePasse*1979@

Searhose - génération de la clef



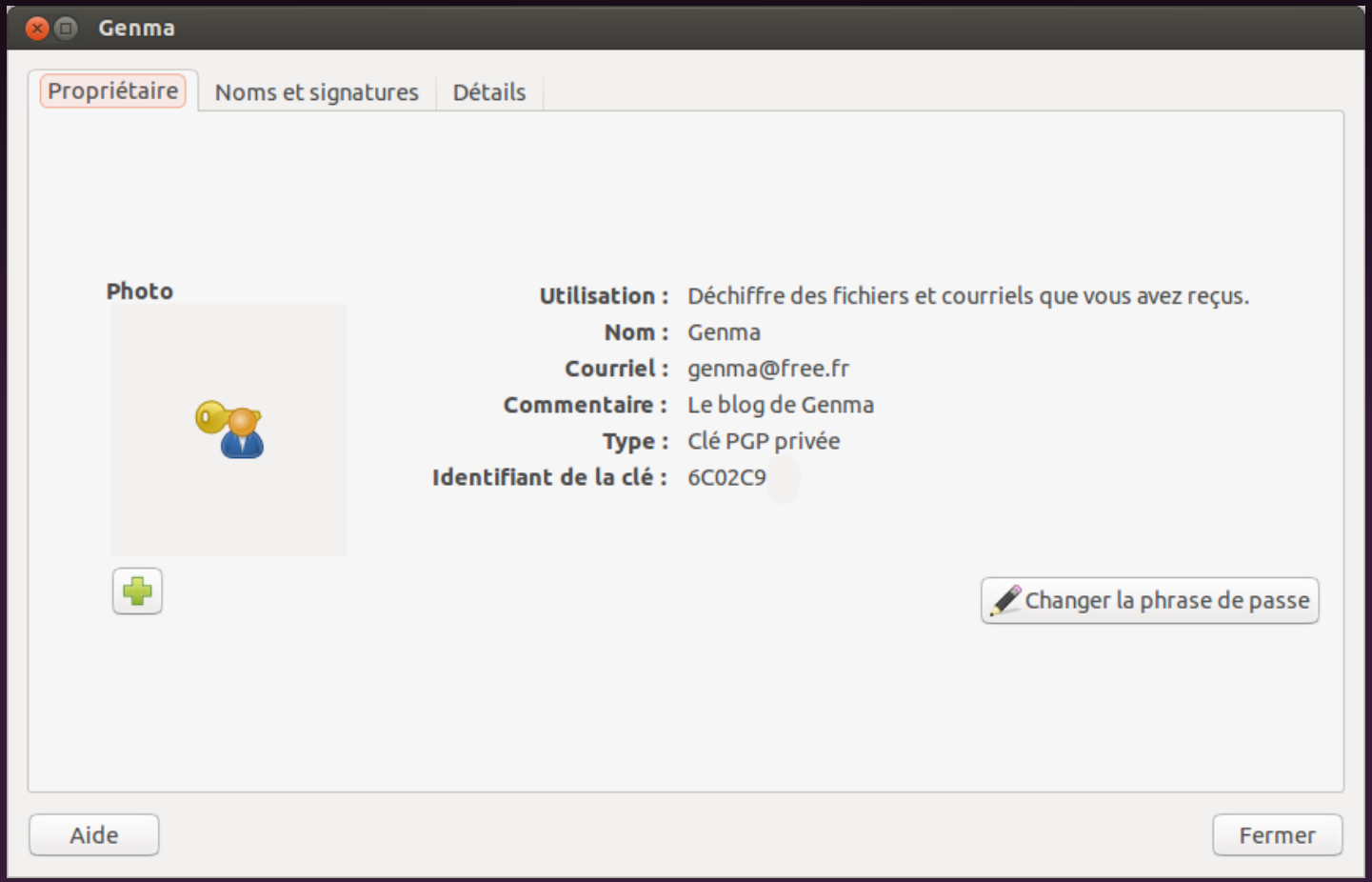
- La génération de la clef commence. Comme il est conseiller de générer de l'aléatoire, personnellement, je lance la commande "ls -R /" dans un terminal.

Searhose - clef créée

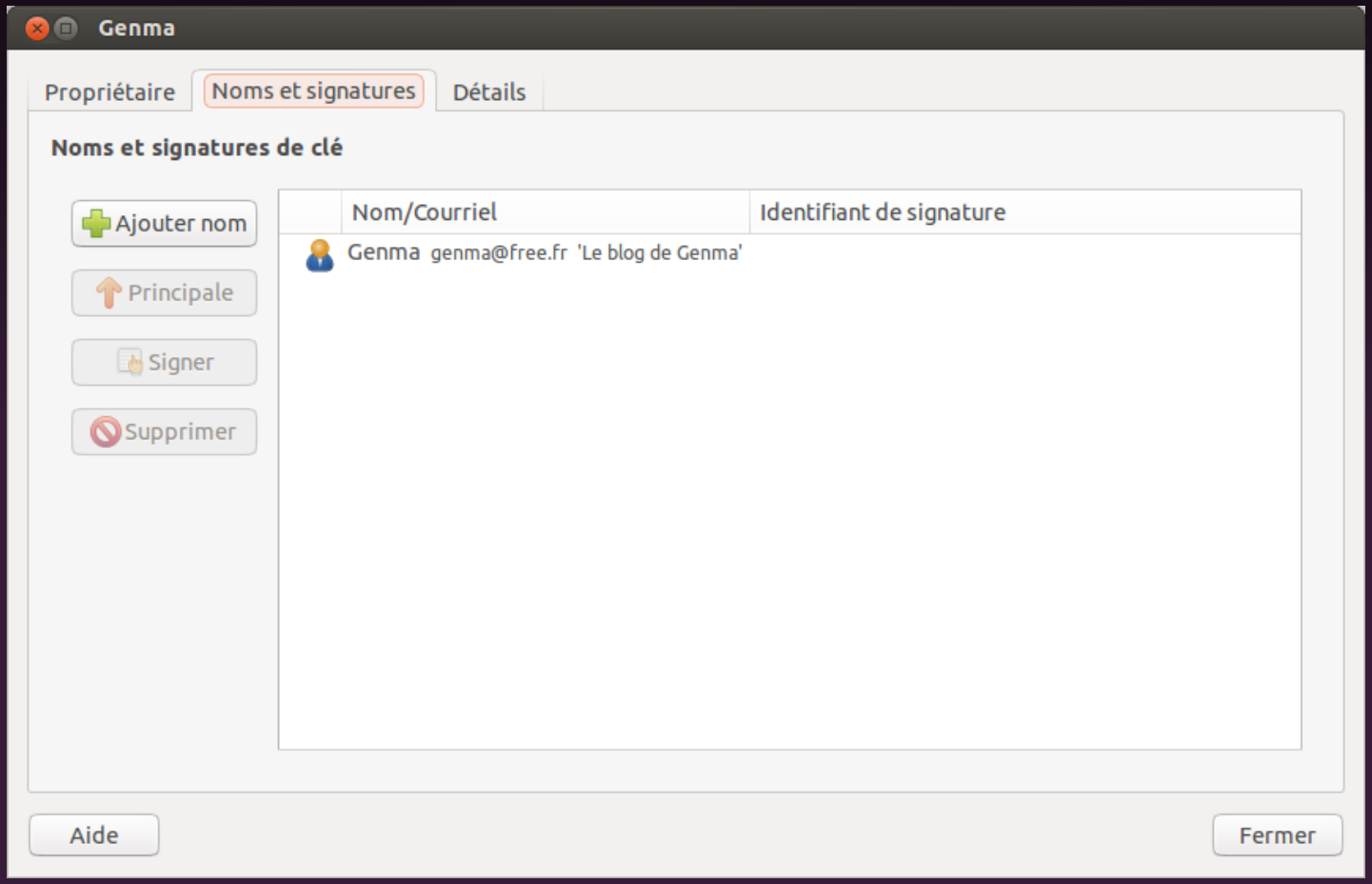


- Une fois la clef créée, elle apparait dans la liste des clefs.

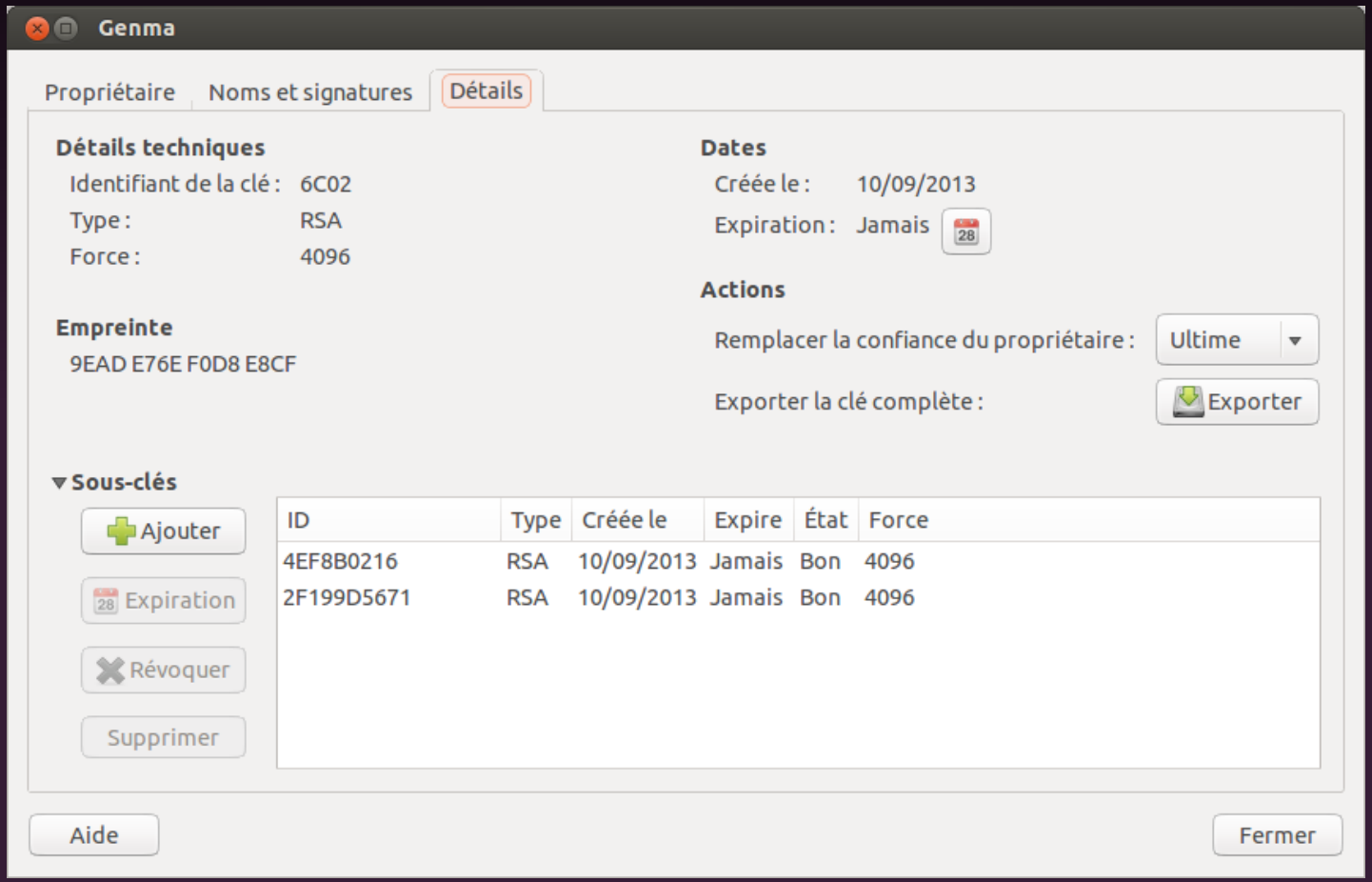
Searhose - détail de la clef 1/3



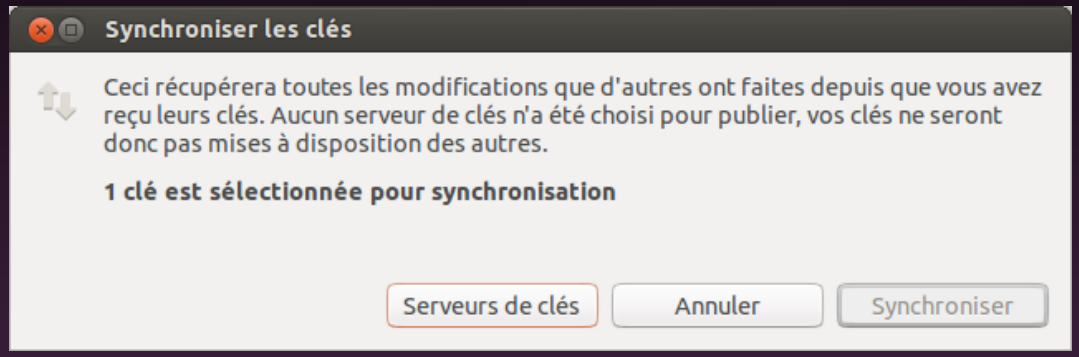
Searhose - détail de la clef 2/3



Searhose - détail de la clef 3/3

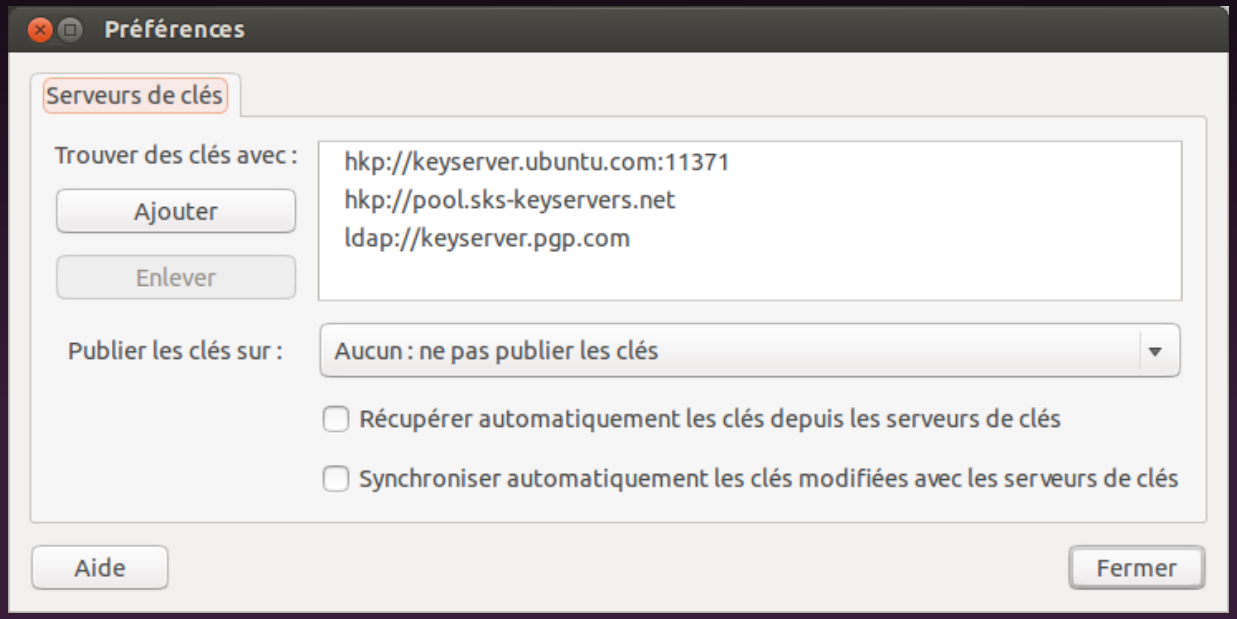


Searhose - publication de la clef



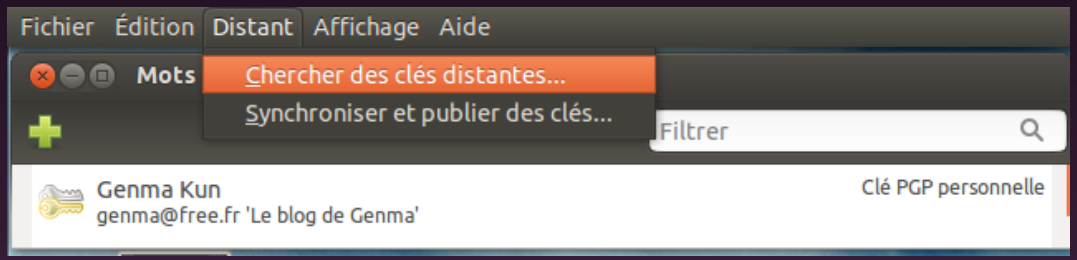
- Pour que la clef publique soit connue et accessible à quiconque souhaite pouvoir nous envoyer un mail chiffré, il faut publier la clef sur les serveurs de clefs.

Searhose - publication de la clef



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

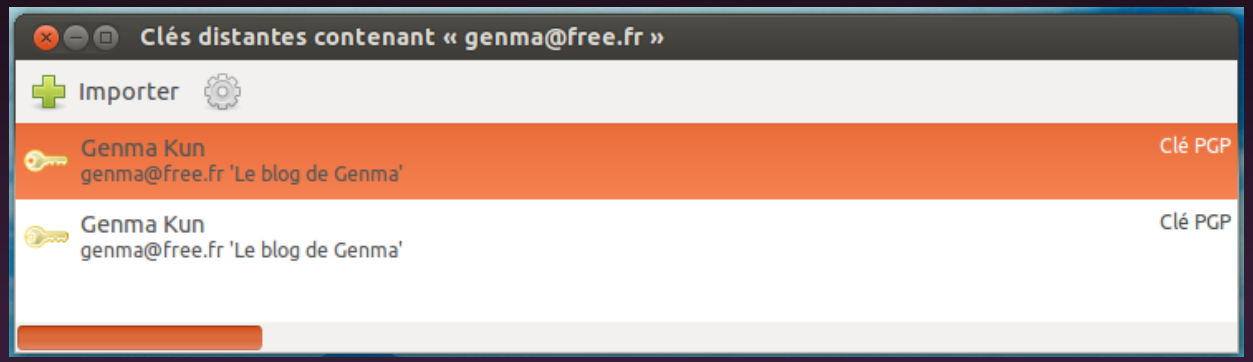
Searhose - recherche de clefs 1/3



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

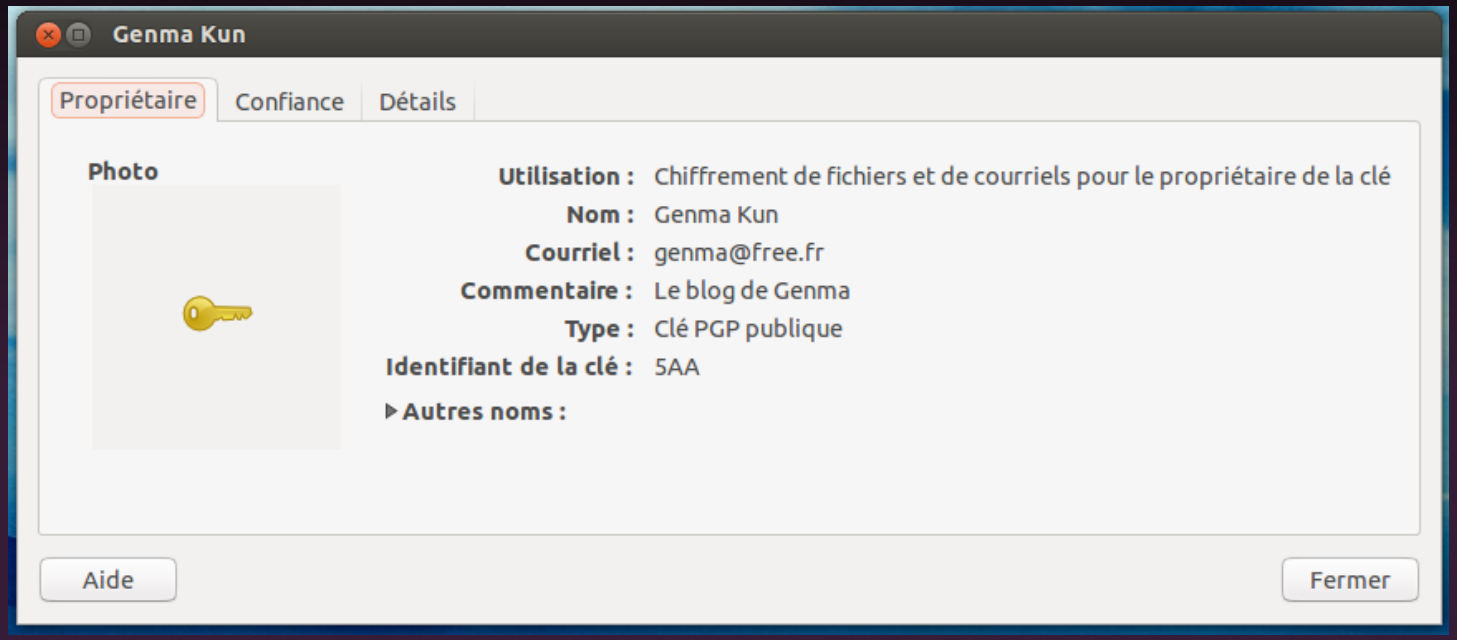
Searhose - recherche de clefs 2/3

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



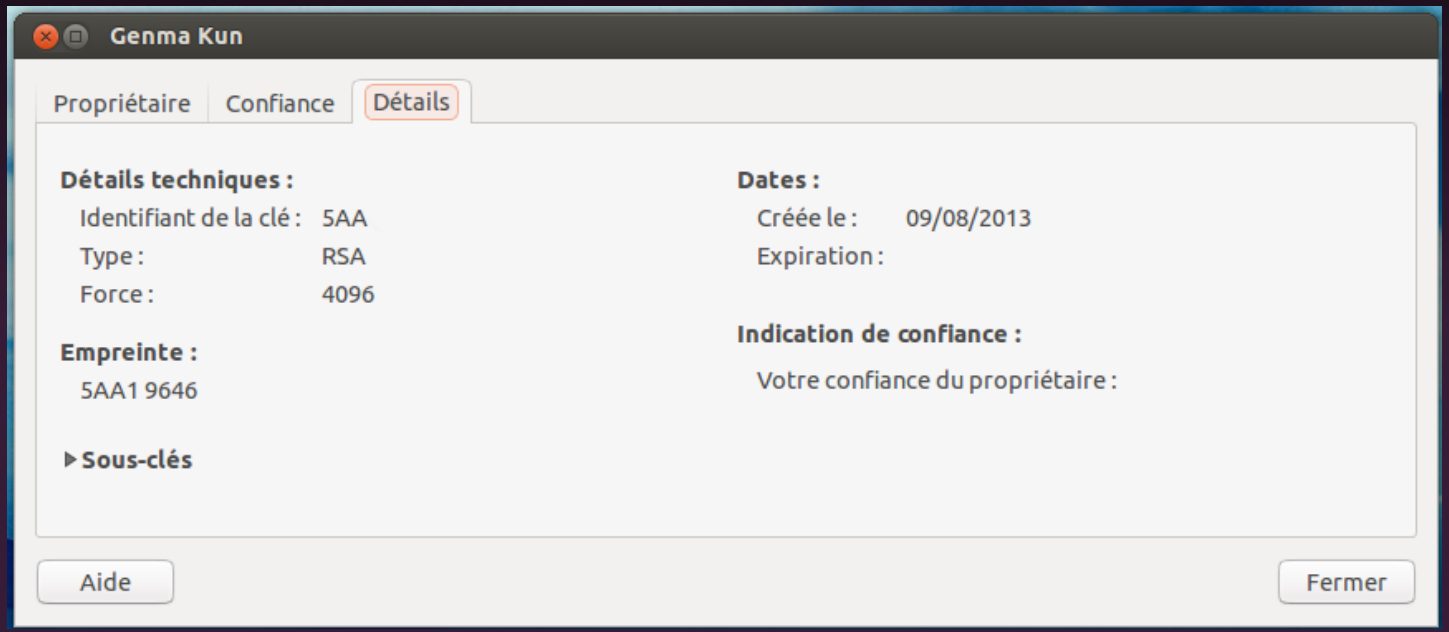
- Pour une clef publique, on peut voir les détails de la clef.

Searhose - détail d'une clef publique 2/3

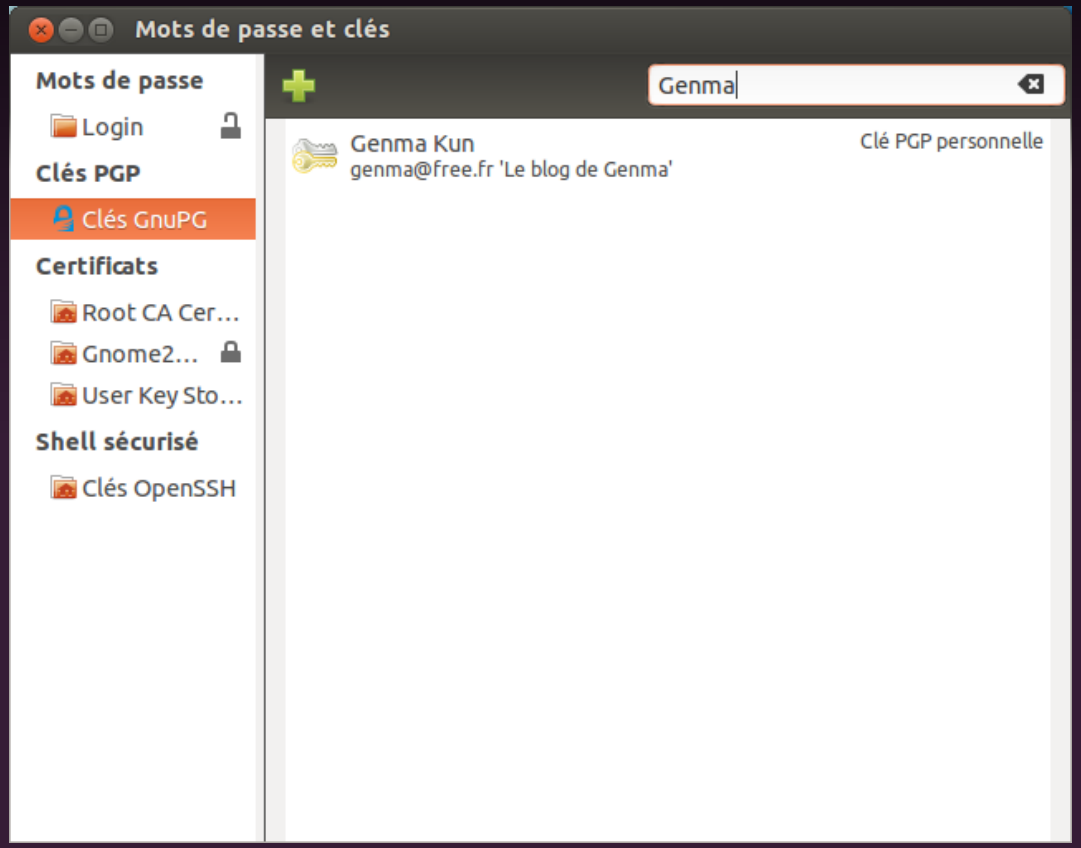
- On voit apparaitre ici la notion de confiance en la clef.

$\Rightarrow$ 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

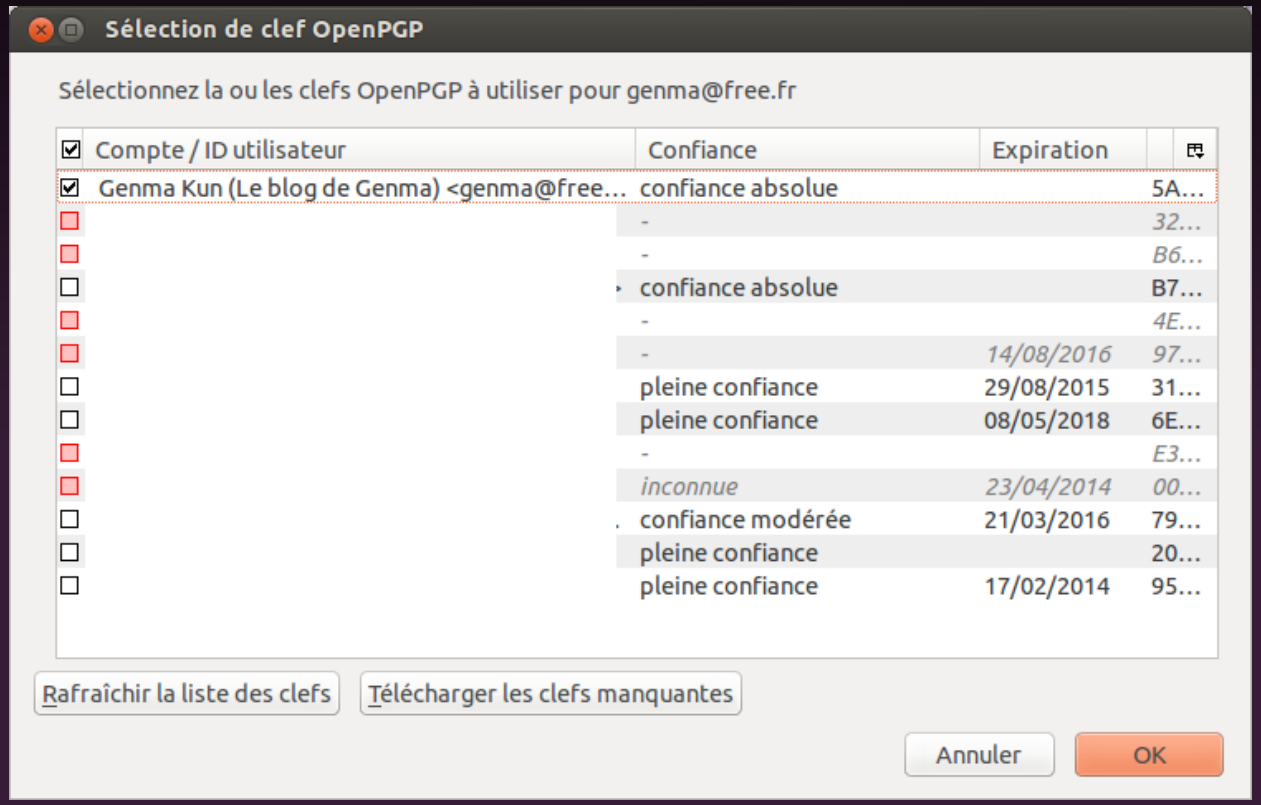


Searhose - gestion de son trousseau 1/2



⇒ 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.

Questions - Démonstration