

Seahorse et GPG

Genma

10 septembre 2013



This work is licensed under the *Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License*.

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



The screenshot shows the homepage of the 'Le Blog de Genma' website. The header features a banner with a panda illustration and the text 'Le Blog de Genma'. Below the banner is a post titled 'Rencontre avec Genma IRL' published on 2 août 2013. The post text discusses a meeting with Genma IRL on August 11th or 12th in Paris. The website includes a sidebar with social media links (Twitter, Facebook, YouTube, etc.) and a search bar. The footer contains the text 'Genma', 'Seahorse et GPG', and the date '10 septembre 2013'.

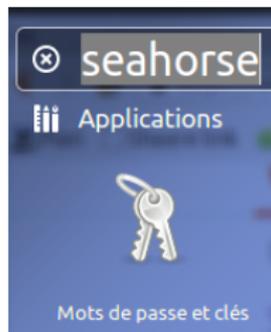
Ce que cette présentation est

Cette présentation est un tutoriel sur la création d'une clef GPG de façon graphique en utilisant le logiciel Seahorse disponible sous Ubuntu.
⇒ La clef créée est 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



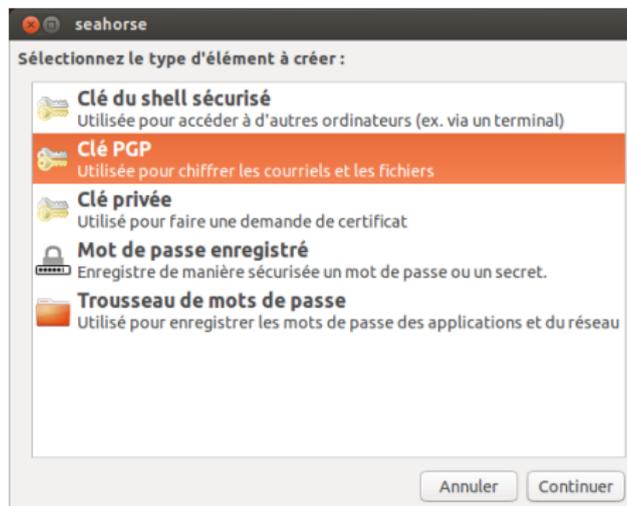
- Pour lancer Seahorse, il suffit de taper Seahorse ou de chercher Mots de passes et clés et de valider.

Seahorse - premier lancement



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

Seahorse - 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.

Seahorse - informations sur l'utilisateur

seahorse

Une clé PGP vous permet de chiffrer des courriels ou des fichiers à destination d'autres personnes.

Nom complet : Genma

Adresse électronique : genma@free.fr

Commentaire : Le blog de Genma

▼ Options avancées de clé

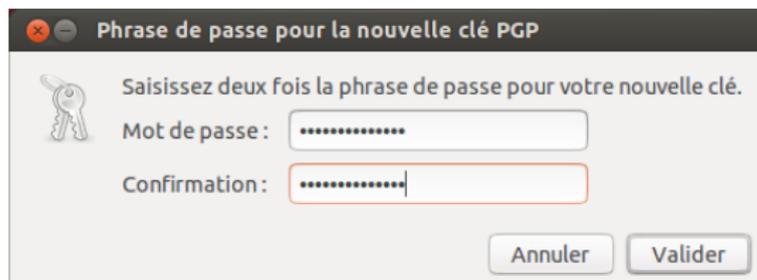
Type de chiffrement : RSA

Force de la clé (bits) : 4096 - +

Date d'expiration : 2014-09-10 12:55 PM N'expire jamais

Aide Annuler Créer

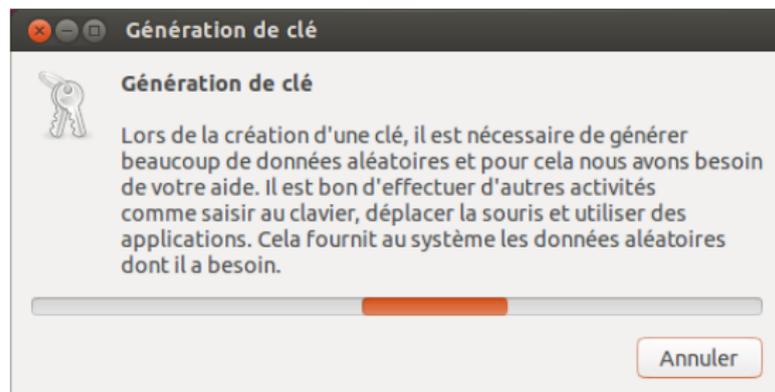
- Différents champs sont à remplir.
- Les deux options importantes sont ici la taille de la clef (4096) et la date d'expiration.



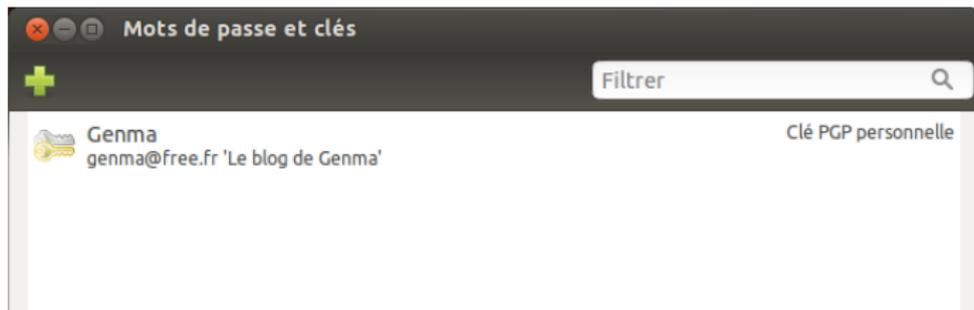
- Il faut alors saisir le mot de passe qui sera utilisé par la suite à chaque utilisation de la clef.

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

⇒ ExempleDeMotDePasse*1979@



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

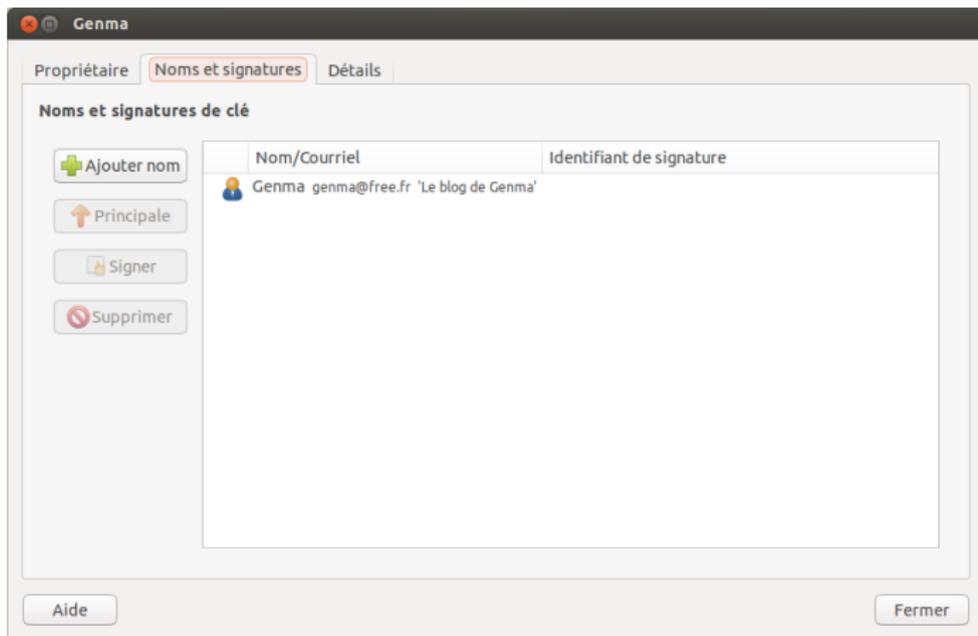


- Une fois la clef créée, elle apparait dans la liste des clefs.

Searhose - détail de la clef 1/3



Searhose - détail de la clef 2/3



Searhose - détail de la clef 3/3

Genma

Propriétaire Noms et signatures **Détails**

Détails techniques

Identifiant de la clé : 6C02C9E3
Type : RSA
Force : 4096

Dates

Créée le : 10/09/2013
Expiration : Jamais

Empreinte

9EAD E76E F0D8 E8CF 9376
A28E 4EF8 B021 6C02 C9E3

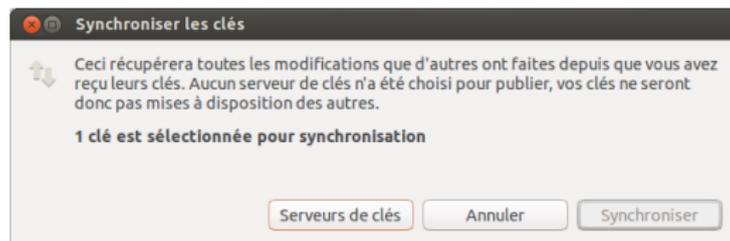
Actions

Remplacer la confiance du propriétaire : Ultime
Exporter la clé complète : Exporter

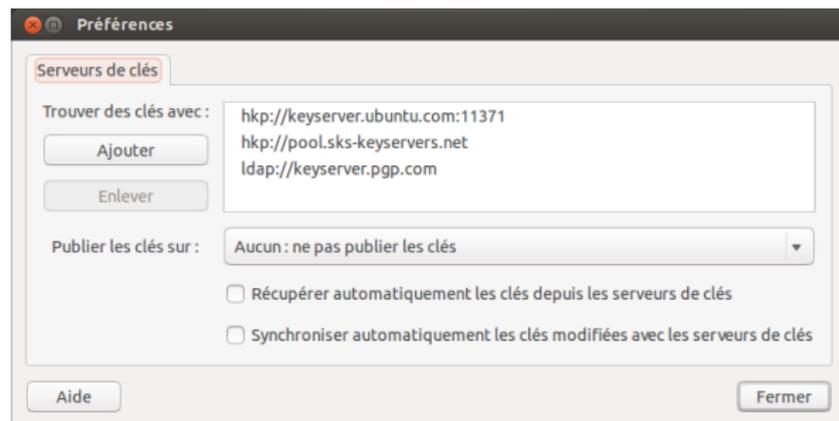
▼ **Sous-clés**

ID	Type	Créée le	Expire	État	Force
4EF8B0216C02C9E3	RSA	10/09/2013	Jamais	Bon	4096
2F199D5671C9D99C	RSA	10/09/2013	Jamais	Bon	4096

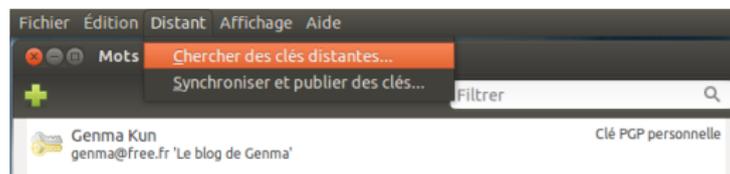
Aide Fermer



- 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.



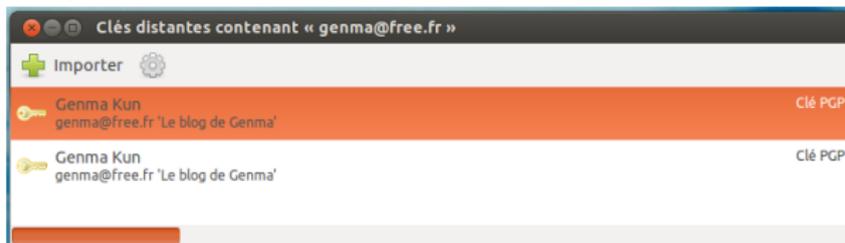
- Il est possible de choisir les serveurs de clefs, d'en ajouter. Par défaut, les principaux sont présents.



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

Searhose - Recherche de clefs 2/3





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

Searhose - Détail d'une clef publique 1/3



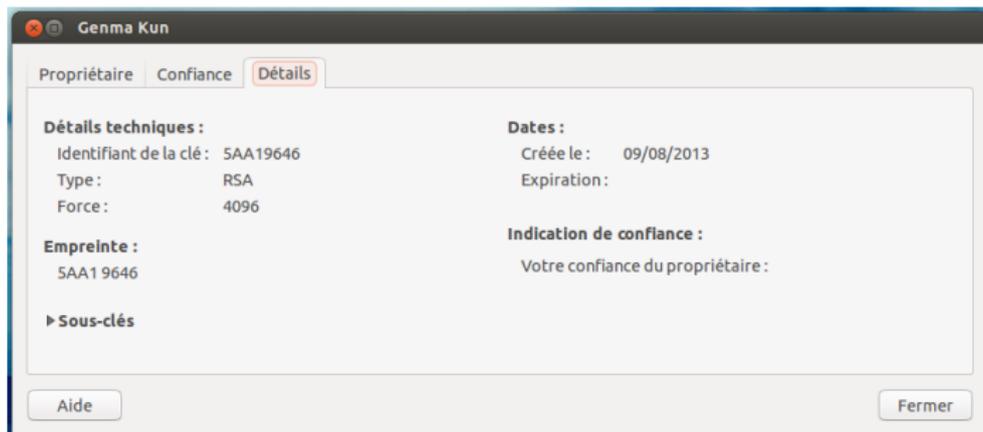
- Pour une clef publique, on peut voir les détails de la clef.



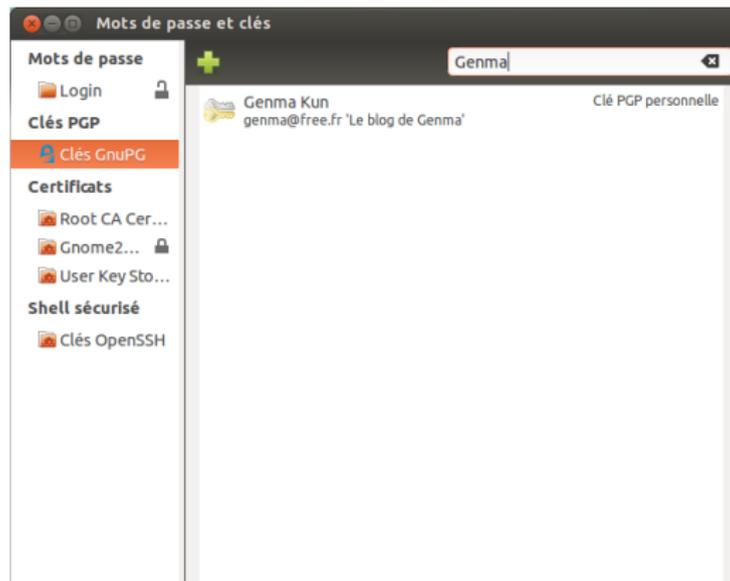
- On voit apparaître ici la notion de confiance en la clef.

⇒ 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.

Seahorse - Détail d'une clef publique 3/3

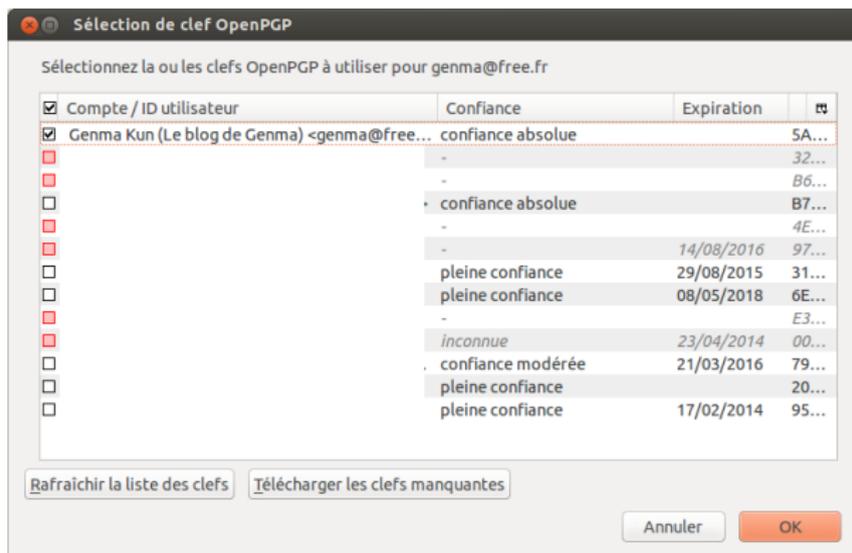


Seahorse - Gestion de son trousseau 1/2



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

Searhose -Gestion de son trousseau 2/2



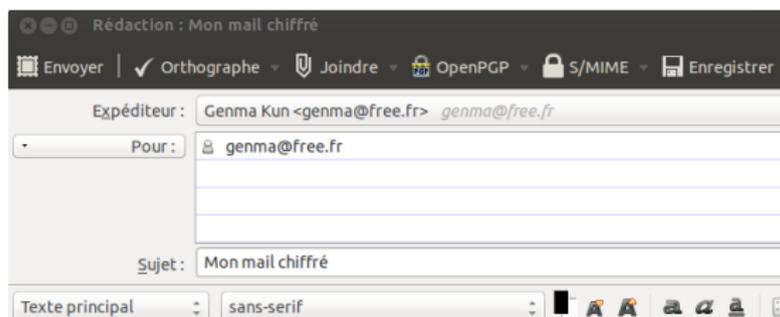
⇒ Ou de voir toutes les clefs et la confiance que l'on a dans ces clefs.

Thunderbird

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

A COMPLETER - A CONTINUER

Thunderbird - Création d'un mail chiffré



Le texte de mon mail

- 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 réception 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