#### Seahorse et GPG

Genma

10 septembre 2013

### $(\mathbf{i} \otimes \mathbf{0})$

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

Genma

Seahorse et GPG

#### 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



#### 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



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



• 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

🛞 💿 seahorse
Sélectionnez le type d'élément à créer :
Clé du shell sécurisé Utilisée pour accéder à d'autres ordinateurs (ex. via un terminal)
Clé PGP Utilisée pour chiffrer les courriels et les fichiers
Clé privée Utilisé pour faire une demande de certificat
Mot de passe enregistré Enregistre de manière sécurisée un mot de passe ou un secret.
<b>Trousseau de mots de passe</b> Utilisé pour enregistrer les mots de passe des applications et du réseau
Annuler Continuer

• On choisira Clé GPG.

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

### Searhose -informations sur l'utilisateur

😣 seal	norse			
<u></u>	Une clé PGP vous perme	t 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	2	Annuler Créer		

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

Genma

80	Phrase de passe p	oour la nouvelle clé PGP
R	Saisissez deux f Mot de passe :	ois la phrase de passe pour votre nouvelle clé.
	Confirmation :	•••••
		Annuler Valider

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

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

 $\Rightarrow$  ExempleDeMotDePasse\*1979@



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



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

🐵 Genma		
Propriétaire Noms et sig	natures Détails	
Photo	Utilisation : Nom : Courriel : Commentaire : Type : Identifiant de la clé :	Déchiffre des fichiers et courriels que vous avez reçus. Genma genma@free.fr Le blog de Genma Clé PCP privée 6C02C9E3
		Changer la phrase de passe
Aide		Fermer

😣 🗊 Genma			
Propriétaire Nom	s et signatures Détails		
Noms et signature	s de clé		
Aiouter nom	Nom/Courriel	Identifiant de signature	
Principale	8 Genma genma⊕free.fr 'Le bli genma⊕free.fr 'Le bli	g de Genma'	
Aide			Fermer

😣 🗊 Genma							
Propriétaire Noms	et signatures Déta	ils					
Détails techniques				Dates			
Identifiant de la clé	: 6C02C9E3			Créée le	e :	10/09/2013	
Type :	RSA 4096			Expirat	ion :	Jamais 🔡	
101001	1070			Actions			
Empreinte 9EAD E76E F0D8 E8 A28E 4EF8 B021 6C0	CF 9376 02 C9E3			Rempla Exporte	icer la er la cl	confiance du propriétaire : é complète :	Ultime 💌
<b>▼</b> Sous-clés							
Aiouter	ID	Туре	Créée le	Expire	État	Force	
	4EF8B0216C02C9E3	RSA	10/09/2013	Jamais	Bon	4096	
28 Expiration	2F199D5671C9D99C	RSA	10/09/2013	Jamais	Bon	4096	
<b>Révoquer</b>							
Supprimer							
Aide							Fermer

80	Synchroniser les clés				
t,	Ceci récupérera toutes les modifications que d'autres ont faites depuis que vous avez reçu leurs clés. Aucun serveur de clés n'a été choisi pour publier, vos clés ne seront donc pas mises à disposition des autres.				
	1 clé est sélectionnée pour synchronisation				
	Serveurs de clés Annuler Synchroniser				

• 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.

rouver des clés avec :	hkp://keyserver.ubuntu.com:11371	
Ajouter	hkp://pool.sks-keyservers.net	
	ldap://keyserver.pgp.com	
Entever		
Publier les clés sur :	Aucun : ne pas publier les clés	•
	Récupérer automatiquement les clés depuis les serveurs de clés	
	Synchroniser automatiquement les clés modifiées avec les serve	urs do cló

• 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 connait pas encore la clef GPG, on peut rechercher sa clef publique.

#### Chercher des clés distantes

Ceci cherchera les clés d'autres personnes sur Internet. Ces clés peuvent être importées dans votre trousseau de clés local.

Serveurs de	clés :			
🗹 hkp://ke	yserver.ubuntu	.com:11371		
🔽 hkp://po	ol.sks-keyserv	ers.net		
🔽 ldap://k	eyserver.pgp.co	om		



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

#### Searhose - Détail d'une clef publique 1/3

😣 🗉 🛛 Genma Kun		
Propriétaire Confiance	Détails	
Photo Com-	Utilisation : Nom : Courriel : Commentaire : Type : Identifiant de la clé : ⊨Autres noms :	Chiffrement de fichiers et de courriels pour le propriétaire de la clé Genma Kun genma@free.fr Le blog de Genma Clé PCP publique SAA19646
Aide		Fermer

• 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

😣 🗐 🛛 Genma Kun			
Propriétaire Co	onfiance Détails		
Détails techniqu	ues:	Dates :	
Identifiant de la	a clé : 5AA19646	Créée le : 09/08/2013	
Type :	RSA	Expiration :	
Force :	4096		
Empreinte :		Indication de confiance :	
5AA1 9646		Votre confiance du propriétaire :	
▶ Sous-clés			
Aide			Fermer

#### Searhose - Gestion de son trousseau 1/2



 $\Rightarrow$  II est possible de chercher une clef dans son trousseau.

~			
	<b>en</b>	m	-
· •	GII		Π.

Ø	Compte / ID utilisateur	Confiance	Expiration	CQ.
•	Genma Kun (Le blog de Genma) <genma@free.< td=""><td> confiance absolue</td><td></td><td>5A</td></genma@free.<>	confiance absolue		5A
		-		32
		-		Вб
		<ul> <li>confiance absolue</li> </ul>		B7
		-		4E
		-	14/08/2016	97
		pleine confiance	29/08/2015	31
		pleine confiance	08/05/2018	6E
		-		E3
		inconnue	23/04/2014	00
		. confiance modérée	21/03/2016	79
		pleine confiance		20
		pleine confiance	17/02/2014	95

 $\Rightarrow$  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

Expéditeur : Cenma Kun <genma@free.fr 2="" genma@free.fr="" genma@free.fr<="" pour:="" th=""></genma@free.fr>
Pour: 8 genma@free.fr
Sujet : Mon mail chiffré
Texte principal ; sans-serif ; <b>F R R A a a b</b>

- 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

©©© Rédaction : Mon mail chiffré ▓Envoyer │ ✔ Orthographe = 0 Joindre = 盘 OpenPGP = 🔒 S/MIME = 🕁 Enregistrer -						
Expéditeur :	Genma Kun <genma@free.fr> genma@free.fr</genma@free.fr>					
• Pour:	genma@free.fr					
<u>S</u> ujet :	Mon mail chiffré					
Texte principal 🗘 sans-serif 🗘 🖡 🕱 🛱 a 🖉 🛓 🔚						
Le texte de mon mail						

• 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

Genma

# SAUVEGARDER SES CLEFS GPG A COMPLETER - A CONTINUER