

Objectif et principe

Sur internet, il est très simple de se faire passer pour quelqu'un d'autre notamment avec le courrier électronique. C'est en effet à la portée de tout le monde d'envoyer un message en spécifiant un autre émetteur dans le paramétrage de son logiciel de messagerie. Par ailleurs, il peut être parfois intéressant d'envoyer des messages cryptés : envoi d'un mot de passe ou d'un code bancaire par exemple.

Pour répondre à ces deux problématiques, il existe un système permettant de signer d'une part et de crypter d'autre part ses messages. Afin d'obtenir un niveau de sécurité suffisant, ce système utilise des algorithmes mettant en place des paires de clefs.

Chaque interlocuteur possède une clef privée et une clef publique. Il est le seul à pouvoir utiliser sa clef privée (en saisissant la phrase secrète associée) alors qu'il diffuse à ses connaissances sa clef publique.

Pour signer un message et donc certifier que l'émetteur est bien la personne mentionnée dans l'entête du message, l'émetteur utilise sa clef privée et le destinataire contrôle grâce à la clef publique correspondante.

Pour crypter un message, l'émetteur utilise sa propre clef privée et la clef publique du destinataire qui pourra alors déchiffrer le message en utilisant sa clef privée.

Ce système s'appelle GnuPG. Il peut être utiliser directement dans Thunderbird grâce à Enigmail, une extension de Thunderbird.

Installation

A l'aide du gestionnaire de paquet, installez les paquets suivants (sous Ubuntu) :

- gnupg
- enigmail
- enigmail-locale-fr
- seahorse

Création d'une paire de clef

Lancez Thunderbird. Vous pouvez utiliser l'assistant Enigmail qui se lance automatiquement mais je vous recommande plutôt cette méthode qui peut s'appliquer quand l'assistant ne se lance pas (c'est le cas lorsqu'on crée un compte mail plus tard) :



Menu OpenPGP > Gestion des clefs

Menu Générer > Nouvelle paire de clefs

Génération de clef OpenPGP X							
Compte / ID utilisateur Hyppolite Dugnou < hdugnou@free.fr> - hdugnou@free.fr 🔹							
Pas de phrase secrète							
Phrase secrète ***** Répétez la phrase secrète *****							
Commentaire							
Expiration de la clef Avancé							
La clef expire dans 5 années 💠 🗹 La clef n'expire jamais							
Générer la clef Annuler							
Console de génération de clefs							
NOTE: La génération d'une clef peut prendre plusieurs minutes. Ne quittez pas l'application tant que la génération est en cours. La navigation intensive sur le web ou les opérations intenses sur les disques durs pendant la génération de la clef augmenteront l'entropie et accélèreront le processus. Vous serez averti quand l'opération sera terminée.							

Choisissez le compte mail concerner par cette clef.

Entrez une phrase secrète dans les deux zones. Celle-ci vous sera demander par la suite à chaque utilisation de votre clef privée. Alors ne l'oubliez surtout pas !

> Bouton Générer la clef

Utilisez votre ordinateur afin de générer des codes aléatoires.

٩	Confirmation OpenPGP 🛛 🗙					
?) Génération de la clef terminée! L'identifiant <hdugnou@free.fr> sera utilisé pour la signature.</hdugnou@free.fr>					
	Il est grandement recommandé de créer un certificat de révocation pour la clef. Ce certificat peut être utilisé pour invalider votre clef dans le cas où votre clef privée soit perdue ou compromise. Désirez-vous créer un certificat de révocation maintenant ?					
	<u>N</u> on <u>O</u> ui					

Créez aussi un certificat de révocation en cas de perte de votre clef privée. > Bouton Oui

Et stockez le en lieu sûr.

٩	Créer et enregistrer le certificat de révocation
<u>N</u> om :	hdugnou@free.fr (0x3126CC2F) rev.asc
Enregistrer dans le <u>d</u> ossier :	Documents 🗧
▷ Parcourir d'autres dossiers	i
	Annuler Enregistrer

Voilà votre paire de clef est créée.

Gestion de clefs OpenPGP								
<u>Fichier</u> <u>E</u> dition Affi <u>c</u> hage <u>S</u> erveur de clefs <u>G</u> énérer								
Filtre pour identifiant d'utilisateur ou de clef contenant :								
		,			1			
Compte / ID utilisateur	Identifiant de c	Туре	Validi	Confi	Expir	₽		
Hyppolite Dugnou <hdugnou@free.fr></hdugnou@free.fr>	3126CC2F	publique/privée	confia	confia				

Signez votre paire de clefs : clic droit et "Signer la clef". Cette opération est nécessaire pour certains serveurs de clefs.

3	OpenPGP - Signature de clef	×
Clef à signer : Empreinte :	Hyppolite Dugnou <hdugnou@free.fr> - 0x3126CC2F 9CD6 6AB7 09A6 047E 2E3B E90A 346F 46B2 3126 CC2F</hdugnou@free.fr>	
Clef pour signer :	Hyppolite Dugnou <hdugnou@free.fr> - 0x3126CC2F</hdugnou@free.fr>	\$
Avec quelle atte	ntion avez-vous vérifié que la clef que vous êtes sur le point de signer appartient bien à la personne désignée ci-dessus	? ٦
🔾 Je ne souhait	e pas répondre	
🔾 Je n'ai pas du	tout vérifié	
🔘 J'ai fait une ve	érification rapide	
)'ai fait une ve	érification très poussée)
Signature loca	le (non evnortable)	_
	OK Annuler	•

Vous pouvez répéter ces opérations pour chacun de vos comptes de messagerie.

Vous pouvez aussi utiliser la même paire de clefs pour plusieurs comptes mail. Dans ce cas, faites un clic droit sur la paire de clefs et choisissez "Gérer les identifiants utilisateur", ajoutez alors vos autres adresses mail

Modifier Fidentifiant utilisateur principal								
Clef à modifier : Hyppolite Dugnou <hdugnou@free.fr> - 0x3126CC2F</hdugnou@free.fr>								
Identifiant utilisateur disponible :								
Hyppolite Dugnou <hdugnou@free.fr></hdugnou@free.fr>								
Ajouter Définir comme principal Supprimer Révoquer								
Fermeria Fenetre								

Publication de la clef publique

Vous pouvez envoyer par mail votre clé publique à vos interlocuteurs en faisant un clic droit sur vos clefs et "Envoyer des clefs publiques par courrier électronique"

🐮 Rédaction : (pas de sujet)	
Eichier Édition Affichage Insérer Format Options OpenPGP Outils	s Aid <u>e</u>
Envoyer Contacts Orthographe Joindre OpenPGP S/MI	ME Enregistrer
E⊻péditeur : Hyppolite Dugnou <hdugnou@free.f hdug="" pièces<="" td=""><td>jointes :</td></hdugnou@free.f>	jointes :
Pour:	26CC2F.asc
Texte principal ‡ Largeur variable ‡ A A B	$I \underline{\cup} \stackrel{1-}{\coloneqq} \stackrel{1-}{\longleftarrow} \stackrel{1-}{\longrightarrow} \stackrel{1-}{\longrightarrow} $

Il est aussi possible de publier ses clefs publiques par l'intermédiaire de serveurs de clefs consultables par tous. Ceci permettra à vos interlocuteurs de les retrouver automatiquement. Clic droit et "Envoyer les clefs publiques vers un serveur de clefs". Choisissez n'importe lequel des serveurs proposés.

Sélection:	nez le serveur de clefs 💦 🗙						
Envoyer la clef publique 0x3126CC2F - Hyppolite Dugnou <hdugnou@free.fr> au serveur de clefs :</hdugnou@free.fr>							
Serveur de clefs pool.sks-keyservers.net							
	Annuler OK						

Envoi d'un message signé

Une fois les clefs générées, la signature d'un message se fait très simplement avec Thunderbird et Enigmail. Créer un nouveau message en cliquant sur le bouton "Ecrire" (ou "Répondre") tout en maintenant la touche Maj (shift). Ceci permet de créer un nouveau message sans mise en forme (gras, italique...). Cela permet une meilleur compatibilité avec les autres logiciels de vérification de signature.

Cliquer sur le menu OpenPGP et cochez "Signer le message"

🐮 Rédaction : Test de message signé 📃 🗆 🗙									
<u>F</u> ichier	Éditio <u>n</u>	<u>A</u> ffichag	e O <u>p</u> tions	Ope <u>n</u> PGP	<u>O</u> utils	Aid <u>e</u>			$\langle \rangle$
Envoyer	Cont	J tacts (ab c Orthographe	- Ū Joindre	e Op	🔒 🚦	S/MIME	E Enregist	rer
E <u>x</u> pédite	eur : Hy	yppolite D	ugnou <hdu< td=""><td>gnou@free.</td><td>fr> - ŀ</td><td>ndugnou@</td><td>@free.fr</td><td></td><td>+</td></hdu<>	gnou@free.	fr> - ŀ	ndugnou@	@free.fr		+
Ţ	Pour	: 📧 jpn	norfin@free.f	r					
<u>S</u> ujet :	Test <u>de</u>	message	signé						
Ceci es	t un mes	ssage sig	né.						
		5 5	,						
									1

Vous remarquerez le petit crayon en vert en bas à droite de la fenêtre.

Une confirmation ou une demande de votre phrase secrète apparaît afin de pouvoir utiliser votre clef privée pour la signature.

٩	Autoriser l'accès à la phrase de passe 📃 🗖 🗙
R	Vous avez besoin d'une phrase de passe pour déverrouiller la clé secrète pour l'utilisateur: "Hyppolite Dugnou <hdugnou@free.fr>" clé 1024 bits DSA, ID 3126CC2F, créée 2008-09-21</hdugnou@free.fr>
	La phrase de passe est présente en mémoire cache.
	🗹 Toujours demander avant d'utiliser une phrase de passe en cache
	(CAnnuler) <u>Autoriser</u>

Envoi d'un message chiffré

De même que pour la signature, il est préférable de créer un message en maintenant la touche Maj (shift). Tapez votre message et dans le menu OpenPGP, cochez "Signer le message" et "Chiffrer le message".

Ħ		Rédaction : T	est de mes	age chiffré		_ _ _ _ _
<u>F</u> ichier	Éditio <u>n A</u> fficha	ige O <u>p</u> tions (Ope <u>n</u> PGP <u>O</u> ၊	utils Aid <u>e</u>		$\langle \rangle$
		abc	. 0 .	. 🔒 .	· 🔒 .	V. 🚺
Envoyer	Contacts	Orthographe	Joindre	OpenPGP	S/MIME	Enregistrer
E <u>x</u> pédite	eur : Hyppolite	Dugnou <hdug< td=""><td>nou@free.fr></td><td>- hdugnou</td><td>@free.fr</td><td>\$</td></hdug<>	nou@free.fr>	- hdugnou	@free.fr	\$
7	Pour : 📧 jr	omorfin@free.fr				
Ţ	Pour :					
<u>S</u> ujet :	Test de messaç	ge chiffré				
Ce mess	age ne sera lis	sible que par s	son destinata	aire !		

Cette fois-ci, le crayon et la clef sont en vert en bas à droite de la fenêtre de message.

Envoyez votre message.

Il est alors nécessaire de rechercher la clef publique du destinataire. Les serveurs de clefs sont là pour ça. Cliquez sur le bouton "Télécharger les clefs manquantes" si votre destinataire n'est pas dans la liste. Puis cochez-le dans la liste des clefs. Puis OK.

0	Sélection de clef OpenPGP									
ſ	Le destinataire est invalide, n'est pas de confiance ou n'a pas été trouvé									
	jpmorfin@mobilisoft.com									
ſ	Sélectionnez les destinataires pour le chiffrement									
	Compte / ID utilisateur	Confiance	Expir	Identifia	E\$					
	Hyppolite Dugnou <hdugnou@free.fr></hdugnou@free.fr>	confiance a		3126CC2F						
	Jean-Pierre Morfin (Informaticien indépendant) < jpmorfin@	. pas confiance		0FDB29F2						
	□ Envoyer le message non chiffré									
(
l	<u>R</u> afraîchir la liste des clefs <u>Tél</u> écharger les clefs manquantes									
	ОК	Annuler	Créer règle(s) par destina	taire					

Réception d'un message chiffré

Si vous recevez un message qui a été chiffré par votre interlocuteur, votre phrase secrète vous sera automatiquement demandée pour le déchiffrer. Une petite enveloppe apparaît dans l'entête du message afin de connaître le niveau de confiance attribuée à la clef ayant signé et chiffrée le message.

Niveau de confiance des clefs

Dans le gestionnaire de clefs, il est possible d'attribuer un niveau de confiance à chacune des clefs qui y sont stockées. Ceci en fonction de leur origine. Si vous avez obtenu une clef directement depuis votre interlocuteur (sur un support physique : CD, clef USB...) vous pouvez lui attribuer une confiance élevée. Alors que si vous l'avez simplement trouver sur un serveur de clefs, votre niveau de confiance sera plus modéré.

Clic droit sur la clef et "Définir le niveau de confiance du propriétaire"

🈋 OpenPGP - Définir le niveau de confiance du 🗙
Clef à considérer : Jean-Pierre Morfin (Informaticien
Quel est votre niveau de confiance dans cette clef ?
) Je ne sais pas
○ Je n'ai PAS confiance
J'ai modérément confiance
J'ai pleinement confiance
⊖ J'ai une confiance absolue
Annuler OK

Ces informations de niveau de confiance vous seront indiquées par la suite lors de la réception d'un nouveau message signé en cliquant sur l'enveloppe de l'entête du mail.

Une bonne pratique est de aussi de signer les clefs dans lesquels vous avez confiance. Clic droit sur la clef et "Signer la clef"

3	OpenPGP - Signature de clef	×
Clef à signer : Empreinte :	Jean-Pierre Morfin (Informaticien indépendant) <jpmorfin@mobilisoft.com> - 0x0FDB29F2 D6B3 4056 052F 11C3 EC8A E1AB DB00 6B63 0FDB 29F2</jpmorfin@mobilisoft.com>	
Clef pour signer :	Hyppolite Dugnou <hdugnou@free.fr> - 0x3126CC2F</hdugnou@free.fr>	\$
Avec quelle atter Je ne souhait Je n'ai pas du J'ai fait une vo j'ai fait une vo	ntion avez-vous vérifié que la clef que vous êtes sur le point de signer appartient bien à la personne désignée ci-dessus e pas répondre tout vérifié árification rapide árification très poussée	?
🗌 Signature loca	le (non exportable)	r

Ces informations sont alors partagées via les serveurs de clefs permettant ainsi la mise en commun du niveau de confiance des clefs sur le réseau. Pour connaître les personnes ayant signé une clef : clic droit sur une clef publique et "Voir les signatures".

Aller plus loin avec Seahorse

Seahorse est un outils de gestion de clefs plus pointu. Avec lui, vous pourrez par exemple inclure votre photo à votre clef, ajouter des sous clefs à vos clefs et faire tout un tas d'opérations les concernant.

Enigmail et Seahorse s'appuient tous les deux sur gnupg et partage donc la même base de clefs. gnupg peut d'ailleurs être utilisé directement en ligne de commande. Pour plus d'informations, tapez dans un terminal : man gnupg

Sauvegarder ses clefs

Il est très important de ne pas perdre ses propres clefs (paires privées et publiques). Pour les sauvegarder, vous pouvez les exporter avec un clic droit sur la clef et "Exporter les clefs vers un fichier" que vous mettrez en lieu sûr. Si vous utilisez un utilitaire de sauvegarde, il suffit de sauvegarder le dossier /home/votreLogin/.gnupg

Dernier conseil : ne diffusez jamais vos clefs privées. Même s'il faut une phrase secrète pour l'utiliser, il existe des outils pour les "cracker".

Jean-Pierre Morfin cours sous licence <u>Creative Commons By</u> http://www.g3l.org/