CHIFFRER

ET

SIGNER

SES EMAILS AVEC

ENIGMAIL

POUR THUNDERBIRD

Par Maisse Sébastien



Document en date du 02 mai 2006

Sommaire

Concernant ce document :	
Préambule :	3
Qu'est-ce que Enigmail ?	4
Téléchargement de GNUPG :	4
Installation de GNUPG :	5
Téléchargement de ENIGMAIL :	9
Installation de ENIGMAIL :	9
Configuration de ENIGMAIL :	11
Ressources :	24
Quelques url's :	
Conclusion :	
Merci !	

Concernant ce document :

Ce document a pour vocation de vous aider dans la mise en application de l'extension **Enigmail** pour le client de messagerie **Thunderbird** développé par l'équipe Mozilla.

L'extension en question vous permettra de signer et/ou chiffrer vos prochains e-mails.

Préambule :

Bienvenue dans ce document qui a pour but de vous faire découvrir l'installation ainsi que la configuration de l'extension Enigmail (utilisant GNUPG) dans Thunderbird.



OpenPGP (enigmail) installé dans Thunderbird

<u>Qu'est-ce que Enigmail</u>?

Enigmail est une extension qui permet d'utiliser au sein de Thunderbird, un logiciel de type GNUPG (qui permet de chiffrer/déchiffrer et signer des e-mails).

Voici une petite définition disponible sur Wikipédia.org

Enigmail est un plugin de signature numérique et de chiffrement pour les clients email Mozilla et Mozilla Thunderbird, sous Microsoft Windows, Linux, Mac OS X et d'autres systèmes d'exploitation comme Solaris et FreeBSD, ou même AIX.

Il utilise GnuPG pour assurer la partie cryptographie de ses opérations, mais en se greffant à un client graphique de courrier électronique il évite d'avoir recours à la ligne de commande pour signer et chiffrer messages et fichiers.

Téléchargement de GNUPG :

Avant toute chose, nous devons tout d'abord procéder à l'installation du logiciel GNUPG (<u>GNU Privacy Guard</u>), c'est un équivalent de PGP en version Open source.

Ce logiciel est disponible gratuitement sur le site officiel :

http://www.gnupg.org/

Si vous souhaitez télécharger directement le programme d'installation pour l'environnement windows :

ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.3.exe

Note : à la date de rédaction de ce document, la version disponible était la 1.4.3

Installation de GNUPG :

Une fois le programme d'installation téléchargé, on double clique dessus...



On clique sur Next

🌍 GNU Privacy Guard Setup		_
Choose Components Choose which features of GNU	Privacy Guard you want to instal	
Check the components you wa install. Click Next to continue.	nt to install and uncheck the comp	ponents you don't want to
Select components to install:	Base NLS Tools Documentation	Description Position your mouse over a component to see its description.
Space required: 4.2MB		
Nullsoft Install System v2.06		
	< Back	Next > Cancel

On clique sur Next

nstall Options			NUN
GnuPG Language Selection			U
en - English	-		
be - Belarusian			
ica - Catalá Ica - Cadau			
da - Danish			
de - Deutsch			
el - Greek			
en - English			
en@boldquot - English			
en englade - English			
les - Español			
et - Eesti keel			
- 1999 SC 50107 CS			
fi - Suomi			
fi - Suomi fr - Français			

On choisi la langue (fr – Français) dans le cas présent puis on clique sur le bouton Next

🗑 GNU Privacy Guard Setup		
Choose Install Location		(VIII)
Choose the folder in which to install G	iNU Privacy Guard.	
Setup will install GNU Privacy Guard in Browse and select another folder. Cli	the following folder. To install in ck Next to continue.	a different folder, click
Destination Folder		
C:\Program Files\GNU\GnuPG		Browse
Space required: 4.2MB		
Space available: 62.0GB		
Nullsoft Install System v2.06		
	< Back Ne	xt > Cancel

On choisi le répertoire d'installation puis on clique sur Next

GNU Privacy Guard Setup		2
Choose Start Menu Folder Choose a Start Menu folder for the GN	U Privacy Guard shortcuts.	
Select the Start Menu folder in which y can also enter a name to create a new	ou would like to create the program folder.	's shortcuts. You
GNU Privacy Guard		
Accessoires Antispyware Antivirus Bureautique Démarrage Developpement Ethereal Gestion de temps Hamachi		
Lecteur video - audio		
lleaft Tastall Sustan u.C. 05		
lisore tristali bystern v2.00	1/2 (Sec.)	

On clique sur Next

🛜 GNU Privacy Guard Setup			_ 🗆 🗙
Installation Complete Setup was completed successfully.			
Completed			
Show details			
Mulleoft Testall Sustemu 2.06			
Nullson unscall bystellin v2,00	< Back	Next >	Cancel

L'installation s'est bien déroulée...



On clique sur le bouton Finish

Téléchargement de ENIGMAIL :

GNUPG installé, nous pouvons à présent télécharger l'extension Enigmail. Pour ce faire, il faut aller faire un tour sur le site officiel : <u>http://enigmail.mozdev.org/</u>

L'archive est disponible en suivant lien ci-dessous :

http://www.mozilla-enigmail.org/downloads/enigmail-0.94.0-tb15-win32.xpi

Par ailleurs, une traduction de l'extension est disponible à l'url suivante :

http://www.mozilla-enigmail.org/downloads/lang/0.9x/enigmail-fr-FR-0.9x.xpi

Note : lors de la rédaction de ce document, la version en date disponible était la 0.94.0

Installation de ENIGMAIL :

Concernant l'installation de Enigmail, il faut lancer votre client de messagerie **Thunderbird**, une fois lancé aller dans le menu **Outils** / **Extensions**, là, soit vous faite un glisser-déposer du fichier de l'extension enigmail soit vous Cliquer sur le bouton **Installer**.

Procédure pour l'installation d'une extension



On clique sur le bouton *Installer*

On choisit le répertoire contenant notre extension « enigmail-0.94.0-tb15-win32.xpi »



On clique sur bouton Installer maintenant

🥞 Extensi	ons	
2	Talkback 1.5.0.2 Submit a crash report to Mozilla.org.	
-	MinimizeToTray 0.0.1.2006030906+ Permet de réduire les fenêtres Mozilla vers la zone de notification	
-	Enigmail 0.94.0 Enigmail sera installé(e) au prochain démarrage de Thunderbird.	0.0.0.0.0.0
_	Enigmail fr-FR 0.94.0 Enigmail fr-FR sera installé(e) au prochain démarrage de Thunderbird.	
Insta	aller X Désinstaller Options Mises à jour Obtenir d	l'autres e:

Voilà, nos deux extensions (enigmail et enigmail fr-FR) sont installées

<u>NOTE</u> : Il faut **redémarrer** Thunderbird pour prendre en compte l'extension nouvellement installée.

Configuration de ENIGMAIL :

Notre extension étant installée, nous allons à présent la configurer. Pour ce faire, aller dans le menu **OpenPGP** / **Préférences**, nous allons tout d'abord définir le chemin d'accès de GNUPG (que nous avions installer précédemment).

référence	es OpenPGP	×
Général	Envoi Sélection clef PGP/MIME Avancé Débogage	
Param	nètres généraux	
Chemin	n exécutable GnuPG C:\Program Files\GNU\GnuPG\gpg,, Parcourir,	
Paramè	ètres supplémentaires pour GnuPG	
Paran	mètres phrase secrète	e .
Mémo	oriser la phrase secrète pendant 5 minutes d'inactivité	
E F	Pas de phrase secrète pour l'utilisateur	
Serveu	r(s) de clefs:	
randor	m.sks.keyserver.penguin.de, subkeys.pgp.net, pgp.mit.edu, ldap://certserver.pgp.com	
Exempl	le: sks.dnsalias.net, pgp.mit.edu, ldap://certserver.pgp.com	
	Réinitialiser	
	OK Annuler	

Par défaut, GNUPG se situe dans c:\Program Files\GNU\GnuPG

On clique sur le bouton OK pour valider notre choix.

Ceci étant fait, nous allons définir notre première clef publique / privée, pour ce faire rendez-vous dans le menu **OpenPGP** / **Gestion des clefs**.

🖥 Gesti	on de cle	efs OpenPG	P						
Eichier	Edition	Affichage	<u>S</u> erveur de clefs	<u>G</u> énérer					
iltre pou	ır identifia	nt d'utilisate	ur ou de clef contena	int :		Effac	er		
Comp	te / ID ut	ilisateur		Identifiant	Туре	Niveau	Confian	Expiration	E.
					N				
					45				

Comme vous pouvez le voir, il n'y a pour le moment aucune clef.

🥞 Ges	tion de cl	efs OpenPG	P						_	
Eichier	Edition	Affichage	<u>S</u> erveur de clefs	Génér	er					
Filtre po	our identifia	ant d'utilisate	ur ou de clef conten:	<u>N</u> ot Cer	velle paire de cl tilicat de révoca	efs tion	Efface	er		
Com	pte / ID ut	ilisateur			Identifiant	Туре	Niveau	Confian	Expiration	E.
<u> </u>										

Nous allons générer une nouvelle clef

Génération de	clef OpenPGP		<u>×</u>
Compte / ID uti	lisateur TheCyberSet		· · · · · · · · · · · · · · · · · · ·
🔽 Utiliser la	clef générée pour l'iden	tité sélectionnée	
🔲 Pas de phra	se secrète		
Phrase secrète	****	Répétez la phrase secrète	*****
Commentaire	la clé pour mon compt	e perso	
La clef expire d	dans 5 an anr moi jou Annuler	nées 🔸 Г La clef n'expire : nées is rs	jamais
Console de géi NOTE: La gén génération est génération de terminée.	nération de clefs nération d'une clef p en cours. La navigation la clef augmenteront l'e	eut prendre plusieurs minute n intensive sur le web ou les opéra Intropie et accélèreront le process	s. Ne quittez pas l'application tant que la ations intenses sur les disques durs pendant la sus. Vous serez averti quand l'opération sera

La présente clef va être définie pour le compte mail

Compte / ID Utilisateur : on choisi l'adresse e-mail pour laquelle on souhaite générer une clef

Phrase secrète : La phrase secrète doit être définie pour une meilleure sécurité.

Commentaire : un petit commentaire pour la forme.

La clef expire dans : choisissez la durée de votre clef selon vos besoins.

énération de clef (DpenPGP		
Compte / ID utilisateu	r TheCyberSeb		•
Utiliser la clef ge	énérée pour l'iden	tité sélectionnée	
🔲 Pas de phrase sec	rète		
hrase secrète 🛛 ***	****	Répétez la phrase secrète	****
Commentaire la cl	é pour mon compt	e perso	
Expiration de la clef	Avancé		
2048			
Générer la clef	Annuler		
Console de générati	on de clefs ——		
NOTE: La générati génération est en co génération de la clef terminée.	ion d'une clef po ours. La navigation augmenteront l'e	eut prendre plusieurs minute n intensive sur le web ou les opér ntropie et accélèreront le process	S. Ne quittez pas l'application tant que la ations intenses sur les disques durs pendant la sus. Vous serez averti quand l'opération sera
[
<u>[</u>			

Dans l'onglet Avancé, on peut définir la taille et le type de clef.

Par défaut, on aura une clef avec une taille de 2048 et utilisant le type DSA & El Gamal

Pas de phra: hrase secrète	e secrète	Répétez la phrase secrète	****
ommentaire	la clé pour mon compte	e perso	
xpiration de la i	lef Avancé I		
La clef expire d	ans 3 anr	iées 💌 🗖 La clef n'expire	amais
La clef expire d	ans 3 ann	iées 💌 🗖 La clef n'expire	amais
La clef expire d Générer la clef	ans 3 ann	iées 💌 🗖 La clef n'expire	amais
La clef expire o Sénérer la clef	ans 3 and	iées 💌 🗖 La clef n'expire	amais

On clique sur le bouton Générer la clef



Un message qui vous demande confirmation pour la génération de votre clef publique et privée.

Génération de	clef OpenPGP		X
Compte / ID util	isateur TheCyberSeb clef générée pour l'ident	ité sélectionnée	
Pas de phra	se secrète		,
Phrase secrète	*****	Répétez la phrase secrète	*****
Commentaire	la clé pour mon compte	e perso	
Expiration de la	clef Avancé		
La clef expire o	dans 5 anr	nées 💌 🗖 La clef n'expire	jamais
Générer la clef	Annuler		
 Console de géi NOTE: La gén génération est génération de terminée. 	nération de clefs ération d'une clef pe en cours. La navigation la clef augmenteront l'er	eut prendre plusieurs minute i intensive sur le web ou les opér ntropie et accélèreront le proces:	es. Ne quittez pas l'application tant que la ations intenses sur les disques durs pendant la sus. Vous serez averti quand l'opération sera
		\searrow	

Génération des clefs en cours...

<u>Note</u> : Selon la puissance de votre ordinateur, cela prendra plus ou moins de temps, de quelques minutes à quelques heures. *Patience*...



Une boite de dialogue qui vous invite à la création d'un certificat de révocation, en cas de perte ou de vol de votre clé privée. On clique sur le bouton Oui.

Vous serez invité à indiquer un répertoire où votre certificat de révocation sera enregistré.

Ceci étant votre phrase secrète vous sera demander avant la génération du certificat.

Question	n OpenPGP X
?	Veuillez saisir votre phrase secrète OpenPGP ou le code PIN de votre carte à puce
-	****
	Mémoriser pendant 5 minutes d'inactivité

Voilà le certificat a bien été créé...



On clique sur le bouton OK

💐 Gestion de clefs OpenPGP						
Eichier Edition Affichage Serveur de clefs Générer						
Plice pour identinant d'utilisateur ou de cier contenant :						
Compte / ID utilisateur	Identifiant	Туре	Niveau de confian	Confiance du pro	Expiration	EŞ.
TheCyberSeb (la clé pour mon compte perso)	74F54E3C	publique/privée	confiance absolue	confiance absolue	01/05/2011	
[J						

La clé publique / privée a bien été générée comme on peut le voir dans l'ecran ci-dessus.

Ceci fait, nous allons vérifier que Thunderbird a bien pris en compte notre configuration.

Pour ce faire, aller dans le menu Outils / Paramètres des comptes

Choisissez votre compte e-mail pour lequel vous avez générer une clef.

aramètres des comptes	
 Paramètres serveur Copies et dossiers Rédaction et adressage Espace disque 	Options OpenPGP (Enigmail) Enigmail fournit le support OpenPGP pour le chiffrement et la signature de messages. Il est nécessaire d'avoir le logiciel GnuPG (gpg) pour utiliser cette fonctionnalité. Image: Activer le support OpenPGP (Enigmail) pour cette identité
 Sécurité OpenPGP Accusés de réception Sécurité Paramètres serveur Copies et dossiers Rédaction et adressage Espace disque Sécurité OpenPGP Accusés de réception Sécurité Dossiers locaux Espace disque Serveur sortant (SMTP) 	 Utiliser l'adresse électronique de cette identité pour identifier la clef OpenPGP Utiliser un identifiant de clef particulier (ex: 0x1234ABCD) : 0x74F54E3C Choisir une clef Options de rédaction par défaut Signer les messages non chiffrés par défaut Signer les messages chiffrés par défaut Chiffrer les messages par défaut Avancé Envoyer l'en-tête « OpenPGP » Envoyer l'identifiant de clef OpenPGP Envoyer l'URL pour l'accès à la clef :
Ajouter un compte	
Compte par dé <u>f</u> aut	
Supprim <u>e</u> r le compte	
	OK Annuler

Vérifier que le support Enigmail est bien activé. Si ce n'est pas le cas cochez la case Activer le support OpenPGP (Enigmail) pour cette identité Ceci étant, nous allons pouvoir rédiger notre premier e-mail signé...

Pour ce faire cliquer sur l'icône Ecrire ou menu Fichier / Nouveau / Message

Comme vous pouvez le voir, il y a une icône supplémentaire (OpenPGP) :

Envoyer Contacts Orthographe Joindre Open C + S/MIME Enregistrer
Expéditeur : Signer le message Ctrl+Maj+S
Pour : Real Utiliser PGP/MIME pour ce message Ignorer les règles par destinataire
Sujet : test PGP
un petit mail crypté avec PGP :p

Taper votre e-mail comme à l'habitude... Puis cliquez sur le bouton OpenPGP.

Comme vous pouvez le voir par défaut, l'e-mail votre être signé.

Si je souhaite chiffrer l'e-mail ... je choisi l'option Chiffrer le message.

📽 Rédaction : OPENPGP	
Eichier Edition Affichage Options OpenPGP Qutils Aide	
Envoyer Contacts Orthographe Joindre OpenPGP S/MIME Enregistrer	0
Expéditeur : Signer le message Ctrl+Maj+S	•
✓ Chiffrer le pessage Ctrl+Maj+M Utiliser PGP/MIME pour ce message Ignorer les règles par destinataire	
Sujet : OPENPGP	
on harr or proceeding (<u>internet</u> ,))	

Si je souhaite choisir à nouveau Signer le message, vous aurez un message d'avertissement

Alerte O	penPGP	×
?	Vous avez modifié manuellement la signature. De ce fait, pendant la rédaction de ce message, activer ou non la signature ne dépend plus de l'activation ou non du chiffrement. Ne plus afficher cette fenêtre de dialogue	
	<u> </u>	

On clique sur le bouton OK

Kédaction : OPENPGP	
Eichier Edition Affighage Options OpenPGP Qutils Aide	
Envoyer Contacts Orthographe Joindre OpenPGP S/MIME Enregistrer	$\langle \rangle$
Expéditeur : Signer le message Ctrl+Maj+S	*
✓ Chiffrer le message Ctrl+Maj·M	
Utiliser PGP/MIME pour ce message	
Ignorer les règles par destinataire	
Sujet : OPENPGP	
Un mail crypté avec OPENPGP (enigmail) :)	

Dans le cas suivant par exemple, l'e-mail sera signé et chiffré...

Ceci étant, je vais juste signer l'e-mail que je veux envoyer...



Votre phrase secrète vous sera demandé

A cet instant l'e-mail signé est parti...

Dans le cas où vous souhaitez envoyer un e-mail chiffré, il vous faudra disposer de la clef publique de votre destinataire.

TheCyberSeb (la clé pour mon compte perso) confiance abs 01/05/2011 74F54E3C	TheCyberSeb (la clé pour mon compte perso) confiance abs 01/05/2011 74F54E3C	Complet / ID duisaceur Confiance Expiration Destinant TheCyberSeb (la clé pour mon compte perso) confiance abs 01/05/2011 74F54E3C
k	k	
ß	\mathbf{k}	ß
R	Ŗ	3
R	\mathbf{k}	Ŗ
	R	Ŕ
Ŕ		≩
\mathbf{k}	R	ß
\mathbf{k}		ß
	<i>I</i> -3	R
k₅	<i>\</i> }	ß
\mathbf{k}	R	\searrow
		Ŀ\$
\searrow	\mathbf{k}	
\searrow	\mathbf{k}	\mathbf{k}
\mathbf{k}		<i>\</i> ₃
\mathbb{R}	\searrow	6
\mathbf{k}	\searrow	4
\searrow	\searrow	
15	rs	72

Visiblement, il n'est pas dans la liste des destinataires susceptibles de pouvoir recevoir du courriel chiffré. Ceci ayant pour action de faire une recherche sur un des serveurs de clef.

On clique sur le bouton Télécharger les clefs manquantes



Dans le cas présent, la personne destinataire ne dispose pas de clef.

		100	-	
Compte / ID utilisateur	 Confiance	Expiration	Identifiant	Ę

Ici, pas trop de choix, l'e-mail sera envoyé non chiffré.

L'e-mail que j'ai envoyé tout-à-l'heure est bien arrivé...

Date: Tue, 02 May 2006 15:25:24 +0200	
De: TheCyberSeb	
À:	
Objet: OPENPGP	
BEGIN PGP SIGNED MESSAGE Hash: SHA1	
Un mail crypté avec OPENPGP (enigmail) :) BEGIN PGP SIGNATURE Version: GnuPG v1.4.3 (MingW32) Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org	
iD8DBQFEV13EcenRP3T1TjwRAjICAKCrk7RerPAv9WXbPGptleQ31zIzpACgt5FG 0W4txL4355KJ2H1/WWHTg7s= =2QOa END PGP SIGNATURE	

Ressources :

Quelques url's :

Enigmail : http://enigmail.mozdev.org/

Thunderbird : http://www.mozilla-europe.org/fr/products/thunderbird/

GNUPG : http://www.gnupg.org/

Portail de la cryptologie (wikipedia) : http://fr.wikipedia.org/wiki/Portail:Cryptologie

Conclusion :

Vous avez à présent une base pour utiliser le chiffrement ainsi que la signature pour vos prochains e-mails.

Si vous avez des questions / suggestions concernant ce document, je vous encourage à me contacter soit par e-mail à <u>thecyberseb@hotmail.com</u>, soit en laissant un message sur le forum qui se trouve à l'url suivante :

http://forum.monserveurperso.com

Pour de plus amples documents sur divers sujets, faites un tour à l'url ci-dessous...

http://tutorial.monserveurperso.com

Merci !

Au site internet qui publie avec ou sans ma bénédiction mon document.

Merci à Monsieur Pat pour la relecture ainsi que la correction orthographique.

MERCI d'avoir pris le temps de lire ce document :-)