Installer GPG et Enigmail sur Mozilla en 12 étapes

(Windows, Linux, MacOS X)

1. Pour Windows et MacOS X, vérifier que le programme GnuPG (WinPT ou MacGPG) est installé sur l'ordinateur (version <u>Windows</u>, version <u>MacOS X</u>)

2. Vérifier que le programme <u>Enigmail</u> est installé sur l'ordinateur

2.1 Vous pouvez aussi installer le module de traduction française pour Mozilla ainsi que pour Enigmail

3. Si le compte courrier n'a pas encore été créé dans Mozilla, le faire:



Assistant de création de compte 🗙
Paramétrage du nouveau compte
Pour recevoir des messages, vous devez d'abord créer et paramétrer un compte Courrier ou Forums.
Cet assistant va collecter les informations nécessaires à la création d'un compte Courrier ou Forums. Si vous êtes incapable de répondre à certaines questions, veuillez contacter votre Administrateur Système ou votre Fournisseur d'Accès Internet.
Sélectionnez le type de compte que vous voulez créer :
Compte Courrier
O Compte Forums
<pre>< Précédent Suivant > Annuler</pre>

Assistant de création de compte
Information sur le serveur
Sélectionnez le type du serveur de réception.
POP O IMAP
Entrez le nom du serveur de réception (par exemple, « pop.exemple.fr »).
Nom du serveur : pop.monfai.fr
Entrez le nom du serveur d'envoi (SMTP) (par exemple, « smtp.exemple.fr »).
Nom du <u>s</u> erveur : smtp.monfai.fr
< Précédent Suivant > Annuler

Assistant de création de compte	×
Nom d'utilisateur	
Entrez le nom d'utilisateur donné par votre fournisseur de courrier (par exemple, « pmartin »). <u>N</u> om d'utilisateur : dupont	
< Précédent Suivant > Annu	er

Assistant de création de compte	×
Nom du compte	
Entrez le nom avec lequel vous souhaitez vous référer à ce compte (par exemple « Compte Travail », « Compte personnel » ou « Compte Forums »).	
Nom du <u>c</u> ompte : dupont@monfai.fr	
< Précédent Suivant > Annule	er)

Assistant de création	de compte 🗙
Félicitations !	
Veuillez vérifier que les informatio correctes. Nom du compte : Nom d'utilisateur :	ons ci-dessous sont dupont@monfai.fr dupont
Adresse : Nom du serveur de réception : Type du serveur de réception : Nom du serveur d'envoi (SMTP) :	dupont@monfai.fr pop.monfai.fr POP3 smtp.monfai.fr
Cliquez sur Terminer pour enregis quitter l'assistant.	trer ces paramètres et
<pre></pre>	cédent Terminer Annuler

4. Dans les paramètres courrier, décocher l'option "Rédiger les messages en HTML":

Paramè	tres des comptes courrier et foru	ms 🕨	
∽dupont@monfai.fr	Paramètres du compte	- <dupont@monfai.fr></dupont@monfai.fr>	
-Copies et dossiers -Adressage -Espace disque -Accusés de réception	Pour envoyer du courrier, le nécessaires. Si vous ne les administrateur système ou v Internet (FAI).	s informations suivantes sont connaissez pas, contactez votre votre fournisseur d'accès	
Dossiers locaux Serveur sortant (SMTP)	Identité		
	Chaque compte dispose d'informations sur l'expéditeu qui sont systématiquement transmises avec les messages. Elles vous identifient auprès de vos destinataires.		
	Votre nom :	Jean Dupont	
	Adresse électronique :	dupont@monfai.fr	
	Adresse pour la réponse :		
	Organisation :		
	Apposer cette signature	:	
Ajouter un compte		Choisir	
Compte par défaut	Rédiger les messages e		
Effacer le compte		Avancé	
	C	OK Annuler <u>A</u> ide	

5. Générer sa paire de clefs OpenPGP (clef publique / clef privée):

	Courrier entrant	: pour dupond@monfai.fr - Mozilla	×
<u>Fichier</u> Edition Affichage	A <u>l</u> ler à <u>M</u> essages	E <u>n</u> igmail <u>O</u> utils Fe <u>n</u> être A <u>i</u> de	
Fichier Edition Affichage	Aller à Messages	Enigmail Qutils Fenêtre Aide Déchiffrer/vérifier Importer la clef publique Sauvegarder le message déchiffré ✓ Déchiffrer/vérifier automatiquement les messages Qublier la phrase de passe Préférences Préférences Préférences avancées Afficher la console Afficher le journal (log) Générer une clef Mise à jour Aide A propos d'Enigmail	acer é ⊯
🔟 🖂 📴 🚺 Chargé	l	Non-lus : 0 Total :	0 = 11C = //

	Enigmail I	Keygen Page		×
Identifiant utilisateur	Jean Dupond <dupond@monf< th=""><th>ai.fr> ▼</th><th>our signer</th><td></td></dupond@monf<>	ai.fr> ▼	our signer	
🗌 Sans phrase de pa	sse			
Entrez la phrase de pa	asse ******	Répétez la phrase de passe	****	_
Commentaire				
Clef OpenPGP				
Générer une clef	Annuler			
NOTE: La génération génération est en co pendant la génératio quand l'opération se	d'une clef peut prendre plusieu urs. La navigation intensive sur n de la clef augmenteront l'entr ra terminée.	rs minutes. Ne quittez pas Mo: le web ou les opérations inten opie et accélèreront le process	zilla tant que la ses sur les disques dur sus. Vous serez averti	s
<pre>gpg: Generating a ++++++++++++++++++++++++++++++++++++</pre>	standard key	· · · · · · · · · · · · · · · · · · ·	+ . + + + + + + + + + + + + + + + + + +	
				1110
				-

5.1 La paire de clefs peut aussi être générée dans un terminal avec la commande:

gpg --gen-key



6. La paire de clefs OpenPGP contient une clef publique (pour chiffrer) et une clef secrète (pour déchiffrer).

Les "trousseaux" contenant toutes les clefs sont les fichiers pubring.gpg et secring.gpg du répertoire "gnupg":

🗖 dupont@lo	calhost.loca	ldomain: A	nome/dup	ont			×
[dupont@loca total 32 -rw -rw -rw -rw [dupont@loca	lhost dupont 1 dupont 1 dupont 1 dupont 1 dupont 1 dupont ilhost dupont	t]\$ 11 ~/.s dupont dupont dupont dupont dupont t]\$	nup9 7736 10573 600 1048 1280	jui jui jui jui	17 18 17 17 18	19:22 gpg.conf 10:28 pubring.gpg 19:26 random_seed 19:24 secring.gpg 10:28 trustdb.gpg	

7. Paramétrer Enigmail:



	Préférences	
Catégorie	Enigmail	
 Apparence Navigateur Composeur Courrier et Forum Confidentialité et Cookies Images Fenêtres publicit Formulaires Mots de passe Enigmail Mot de passe pr SSL Certificats Validation Avancées Hors-ligne et espa 	Adresse courriel ou identifiant de clef: dupond@monfai.fr Sans Utiliser l'adresse d'expéditeur afin de déterminer la clef GPG pour signer Options de chiffrement par défaut O Pas de chiffrement par défaut O Chiffrer si possible O Chiffrer+signer si possible Mémoriser le mot de passe pendant 5 minutes d'inactivité Avancées Réinitialiser Aide Désinstaller Enigmail Mettre à jour Enigmail	phrase de pas

Préférences a	vancées d'Enigmail							
Chemin d'accès de l'exécutable GPG								
Lors de l'envoi d'un courrier	Options supplémentaires							
Signer les messages par défaut	Toujours confirmer avant l'envoi							
Signer les messages dans les forums par défaut	Utiliser le commentaire par défaut dans la signature							
☑ Chiffrer pour moi-même	Cacher les boutons/menus SMIME							
Toujours avoir confiance en l'identifiant utilisateur	Treat '' as signature separator							
☑ Autoriser le format texte coulé (RFC 2646)	Capturer le webmail (expérimental)							
Options PGP/MIME								
O Ne jamais utiliser PGP/MIME								
Utiliser PGP/MIME si possible								
O Toujours utiliser PGP/MIME								
Algorithme de hachage: SHA1								
Serveur de clefs: pgp.mit.edu								
Déboguage d'Enigmail								
Répertoire du journal (log)								
Adresse de messagerie de test dupond@monfai.fr	Tester							
Utiliser la signature et le chiffrement à la volée (exp	périmental)							
Réinitialiser								
	OK Annuler							

8. Exporter sa clef publique OpenPGP et l'insérer dans un message pour l'envoyer à ses correspondants:

E			Ré	édaction : Ma clef PGP		×
*	<u>Fichier</u> <u>E</u> ditio	n <u>A</u> ffichage	Options	E <u>n</u> igmail <u>O</u> utils Fe <u>n</u> être A <u>i</u> de		
		3 93	•	Envoi par <u>d</u> éfaut		500
		gEnvoi Adress	se Joindre	Envoi <u>s</u> igné	-	ШШ
	Expéditeur :	Jean Dupor	nd <dupor< td=""><td>Envoi <u>c</u>hiffré</td><td></td><td></td></dupor<>	Envoi <u>c</u> hiffré		
	- Pou	r · 💷 id@m(onfai fr	<u>E</u> nvoi chiffre+signe Envoi sans chiffromont		
	▼ Pou	r · 📾	Jilai.II		-	
	100			Options d'envoi par defaut		
				Utiliser PGP/MIME pour ce message		
	Suiot · Ma.c	of PGP		Annuler le chiffrement	-	
*				Insérer une clef publique		
				<u>O</u> ublier la phrase de passe		
				Aide		
						=III:- //



Rédaction : Ma clef PGP	×
<u>F</u> ichier <u>E</u> dition <u>A</u> ffichage O <u>p</u> tions E <u>n</u> igmail <u>O</u> utils Fe <u>n</u> êt	re A <u>i</u> de
EnigEnvoi Adresse Joindre Enregistrer	m
Expéditeur : Jean Dupond <dupond@monfai.fr></dupond@monfai.fr>	Pièces jointes :
✓ Pour : jd@monfai.fr	
▼ Pour :	
Suiet : Ma def PGP	
Clef publique de dupond@monfai.fr	
Clef publique de dupond@monfai.fr BEGIN PGP PUBLIC KEY BLOCK Version: GnuPG v1 2 1 (GNU/Linux)	
Clef publique de dupond@monfai.fr BEGIN PGP PUBLIC KEY BLOCK Version: GnuPG v1.2.1 (GNU/Linux)	
Clef publique de dupond@monfai.fr BEGIN PGP PUBLIC KEY BLOCK Version: GnuPG v1.2.1 (GNU/Linux) mQGiBD8hLhcRBACKWo7hf+ViQfDp/9pOwittRBCdtkgWuUb+nS01	tulrMZ8VOWSAW
Clef publique de dupond@monfai.fr BEGIN PGP PUBLIC KEY BLOCK Version: GnuPG v1.2.1 (GNU/Linux) mQGiBD8hLhcRBACKWo7hf+ViQfDp/9pOwittRBCdtkgWuUb+nSOT H+KzMEVLTOcnpzAqAUIWXCouqf2vH5/fKDgkLOsf2d3/p+NZ/FJ7	tulrMZ8VOWSAW YeCzIUDeMd2ai
Clef publique de dupond@monfai.fr BEGIN PGP PUBLIC KEY BLOCK Version: GnuPG v1.2.1 (GNU/Linux) mQGiBD8hLhcRBACKWo7hf+ViQfDp/9pOwittRBCdtkgWuUb+nSOT H+KzMEVLTOcnpzAqAUIWXCouqf2vH5/fKDgkLOsf2d3/p+NZ/FJ7 vuZuOX2mx95QgLuael1kq7qgYJRyNHflH1ZPGQf53sJImxK825LH	tulrMZ8VOWSAW 7eCzIUDeMd2ai Rbt1nlwCgwshF
Clef publique de dupond@monfai.fr BEGIN PGP PUBLIC KEY BLOCK Version: GnuPG v1.2.1 (GNU/Linux) mQGiBD8hLhcRBACKWo7hf+ViQfDp/9pOwittRBCdtkgWuUb+nSOt H+KzMEVLTOcnpzAqAUIWXCouqf2vH5/fKDgkLOsf2d3/p+NZ/FJJ vuZuOX2mx95QgLuael1kq7qgYJRyNHflH1ZPGQf53sJImxK825LH gyg3KhF+GZOu/XIrOCrgrocD/3S7kuYJXXlduqs2QLGn59jbWoRn	tulrMZ8VOWSAW YeCzIUDeMd2ai Rbt1nlwCgwshF hC/QzV19g/PsD
Clef publique de dupond@monfai.fr BEGIN PGP PUBLIC KEY BLOCK Version: GnuPG v1.2.1 (GNU/Linux) mQGiBD8hLhcRBACKWo7hf+ViQfDp/9pOwittRBCdtkgWuUb+nSOT H+KzMEVLTOcnpzAqAUIWXCouqf2vH5/fKDgkLOsf2d3/p+NZ/FJJ vuZu0X2mx95QgLuael1kq7qgYJRyNHflH1ZPGQf53sJImxK825LH gyg3KhF+GZOu/XIrOCrgrocD/3S7kuYJXXlduqs2QLGn59jbWoRr ppOKhpUoGXIDtDttKNjFlg0V9SGcJe1t3qZ4XqsQws80VoJaQm02 Puci7kc5N4tVXc1/bcc8Ccr2000SDn8Lf44bHZYMgfpuJ251	tulrMZ8VOWSAW YeCzIUDeMd2ai Rbt1nlwCgwshF hC/QzV19g/PsD zK9IqKxXUikVb
Clef publique de dupond@monfai.fr BEGIN PGP PUBLIC KEY BLOCK Version: GnuPG v1.2.1 (GNU/Linux) mQGiBD8hLhcRBACKWo7hf+ViQfDp/9pOwittRBCdtkgWuUb+nS07 H+KzMEVLTOcnpzAqAUIWXCouqf2vH5/fKDgkLOsf2d3/p+NZ/FJ7 vuZu0X2mx95QgLuael1kq7qgYJRyNHflH1ZPGQf53sJImxK825LH gyg3KhF+GZOu/XIrOCrgrocD/3S7kuYJXXlduqs2QLGn59jbWoRn ppOKhpUoGXIDtDttKNjFlg0V9SGcJe1t3qZ4XqsQws80VoJaQm02 PvciZkG5N4tVYc1/bcs8CwXkSCCgQQ9SDn8Lf44bHZXMgfpvI7SM plan4/9WsPUTL01XHo2M4EDr5SDuxiPhytBnxN4vkKYZePAGI4K	tulrMZ8VOWSAW 7eCzIUDeMd2ai Rbt1nlwCgwshF nC/QzV19g/PsD zK9IqKxXUikVb M9hnqHehbuLty rbLHZ6Ec8B730
Clef publique de dupond@monfai.fr BEGIN PGP PUBLIC KEY BLOCK Version: GnuPG v1.2.1 (GNU/Linux) mQGiBD8hLhcRBACKWo7hf+ViQfDp/9pOwittRBCdtkgWuUb+nSOf H+KzMEVLTOcnpzAqAUIWXCouqf2vH5/fKDgkLOsf2d3/p+NZ/FJ7 vuZu0X2mx95QgLuael1kq7qgYJRyNHflH1ZPGQf53sJImxK825LH gyg3KhF+GZOu/XIrOCrgrocD/3S7kuYJXXlduqs2QLGn59jbWoRr ppOKhpUoGXIDtDttKNjFlg0V9SGcJe1t3qZ4XqsQws80VoJaQm02 PvciZkG5N4tVYc1/bcs8CwXkSCCgQQ9SDn8Lf44bHZXMgfpvI7SN pJapA/9WsPUTIQ1XHo2M4EDr5SDuxjPhxtRnxN4vkKYZePAGI4K6 21XJxEUq9X/HtfBrK1vll0bNt/ndxn0Gu4F0Y7+A4C1bhUuXgYf	tulrMZ8VOWSAW 7eCzIUDeMd2ai Rbt1nlwCgwshF nC/QzV19g/PsD zK9IqKxXUikVb M9hnqHehbuLty zbLH76Ec8R73Q f+LBKxEM58vYE
Clef publique de dupond@monfai.fr BEGIN PGP PUBLIC KEY BLOCK Version: GnuPG v1.2.1 (GNU/Linux) mQGiBD8hLhcRBACKWo7hf+ViQfDp/9pOwittRBCdtkgWuUb+nSOt H+KzMEVLTOcnpzAqAUIWXCouqf2vH5/fKDgkLOsf2d3/p+NZ/FJJ vuZuOX2mx95QgLuael1kq7qgYJRyNHflH1ZPGQf53sJImxK825LH gyg3KhF+GZOu/XIrOCrgrocD/3S7kuYJXXlduqs2QLGn59jbWORr ppOKhpUoGXIDtDttKNjFlgOV9SGcJe1t3qZ4XqsQws80VoJaQm02 PvciZkG5N4tVYc1/bcs8CwXkSCCgQQ9SDn8Lf44bHZXMgfpvI7SM pJapA/9WsPUTIQ1XHo2M4EDr5SDuxjPhxtRnxN4vkKYZePAGI4Ko 21XJxEUq9X/HtfBrK1yll0bNt/ndxn0Gu4F0Y7+A4CI1bhUuXgYi 3R7bPXTcYtfz4CoDR+IXKF73HYH4CxXKWX9d1hB1btLOMzVSrL01	tulrMZ8VOWSAW 7eCzIUDeMd2ai Rbt1nlwCgwshF hC/QzV19g/PsD zK9IqKxXUikVb M9hnqHehbuLty zbLH76Ec8R73Q f+LBKxEM58vYE zSmVhbiBEdXBv
Clef publique de dupond@monfai.fr BEGIN PGP PUBLIC KEY BLOCK Version: GnuPG v1.2.1 (GNU/Linux) mQGiBD8hLhcRBACKWo7hf+ViQfDp/9pOwittRBCdtkgWuUb+nSOT H+KzMEVLTOcnpzAqAUIWXCouqf2vH5/fKDgkLOsf2d3/p+NZ/FJJ vuZu0X2mx95QgLuael1kq7qgYJRyNHflH1ZPGQf53sJImxK825LH gyg3KhF+GZOu/XIrOCrgrocD/3S7kuYJXXlduqs2QLGn59jbWoRr ppOKhpUoGXIDtDttKNjFlg0V9SGcJe1t3qZ4XqsQws80VoJaQm02 PvciZkG5N4tVYc1/bcs8CwXkSCCgQQ9SDn8Lf44bHZXMgfpvI7SM pJapA/9WsPUTIQ1XHo2M4EDr5SDuxjPhxtRnxN4vkKYZePAGI4KG 21XJxEUq9X/HtfBrK1yll0bNt/ndxnOGu4F0Y7+A4CI1bhUuXgYJ 3R7bPXTcYtfz4CoDR+IXKF73HYH4CxXKWX9d1hB1btL0MzVSrLQ1	tulrMZ8VOWSAW 7eCzIUDeMd2ai Rbt1nlwCgwshF nC/QzV19g/PsD zK9IqKxXUikVb M9hnqHehbuLty cbLH76Ec8R73Q F+LBKxEM58vYE tSmVhbiBEdXBv FxECARkFAi8b

8.1 La clef publique OpenPGP peut aussi être copiée dans un fichier "maclef.asc" en tapant dans un terminal la commande: gpg --export -a dupont@monfai.fr > maclef.asc

9. Importer une clef publique envoyée par un correspondant:

	Ma clef PGP -	Brouillons pour dupond@monfai.fr - Mozilla		
_ <u>Fichier</u> <u>Edition</u> <u>Affichage</u>	A <u>l</u> ler à <u>M</u> essages	E <u>n</u> igmail <u>O</u> utils Fe <u>n</u> être A <u>i</u> de		
A 0		<u>D</u> échiffrer/vérifier	7 0 .	
		Importer la clef publique	20 W	
Nom - 88	eau Dechittrer Repon	Sauvegarder le message déchiffré	imer stop	
Nom V La	Vue : Tous	 Déchiffrer/vérifier <u>a</u>utomatiquement les messages 	Effa	
	🗐 Sujet	Oublier la phrase de passe	∇ Priorité	
Brouillons	∞ Ma clef PGP			
🗇 Modèles		Préférences		
🛱 Envoyés		Préférences a <u>v</u> ancées		
🛄 Corbeille		Afficher la console		
🕨 📃 Dossiers locaux		Afficher le journal (log)		
	Enigmail: Clique	<u>G</u> énérer une clef	iointe au me	
	✓ Sujet : Ma cle	<u>M</u> ise à jour	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
	De : Jean [<u>A</u> ide		
	Date : 08:54	A <u>p</u> ropos d'Enigmail	er le brouillon.	
	À : jd@m	<u>onfai.fr</u>	-	
Clef publique de dupond@monfai.fr				
BEGIN PGP PUBLIC KEY BLOCK				
Version: GnuPG v1.2.1 (GNU/Linux)				
modippohi happacking 7h f. Viofpr (oportit + PPCd+kally) ih up Soty lpu79VowSAM				
H+KzMEVI.TOcnpzAgAUIWXCougf2vH5/fKDgkL0sf2d3/p+NZ/EJ7eCzIUDeMd2aj				
vuZuOX2mx95QgLuael1kq7qgYJRyNHflH1ZPGQf53sJImxK825LRbt1nlwCgwshF				
gyg3KhF+GZOu/XIrOCrgrocD/3S7kuYJXXlduqs2QLGn59jbWoRnC/QzV19g/PsD				
	ppOKhpUoGXIDtDtt	KNjFlgOV9SGcJe1t3qZ4XqsQws80VoJaQmOzK9IqKxXUikVb	1	
	PvciZkG5N4tVYc1/	bcs8CwXkSCCgQQ9SDn8Lf44bHZXMgfpvI7SM9hnqHehbuLty		
	21XIXEU00X/Htfpm	HOZMHEDE SSDUX JENX UKNXNAVKKI ZEPAGI AKODLH / GEC8K / 3Q K1v110hNt /ndvn0Cu4F0Y7+A4CT1hhliuYaVf+I RKvEMSSvVE		
🔟 🖂 💁 🚺 Chargé	21AD ABOQOA/ HTTDI	Non	-lus : 0 Total : 1 =	



10. Pour lister les clefs de son trousseau OpenPGP, dans un terminal taper la commande:

gpg --list-keys



11. Envoyer un message chiffré au format OpenPGP :

Rédaction : Message chiffré				
<u>Fichier</u> Edition Affichage	O <u>p</u> tions E <u>n</u> igmail <u>O</u> ut	ils Fe <u>n</u> être A <u>i</u> de		
EnigEnvoi Adresse	Joindre Enregistrer		M	
Expéditeur : JEnvoi via E	nigmail (chiffre/signe)	Pièces jointes	:	
	@monfai.fr			
Bonjour, Ceci est un test de messa	ge chiffré			



12. Déchiffrer un message chiffré en OpenPGP :



Copyright (c) 2003, pplf