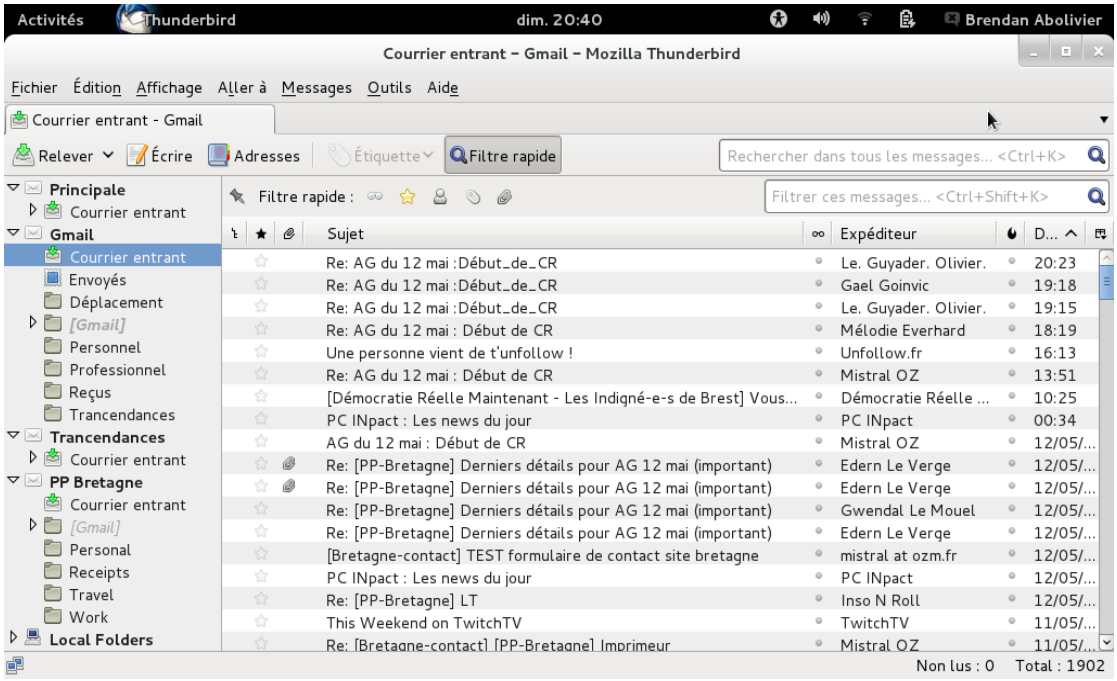
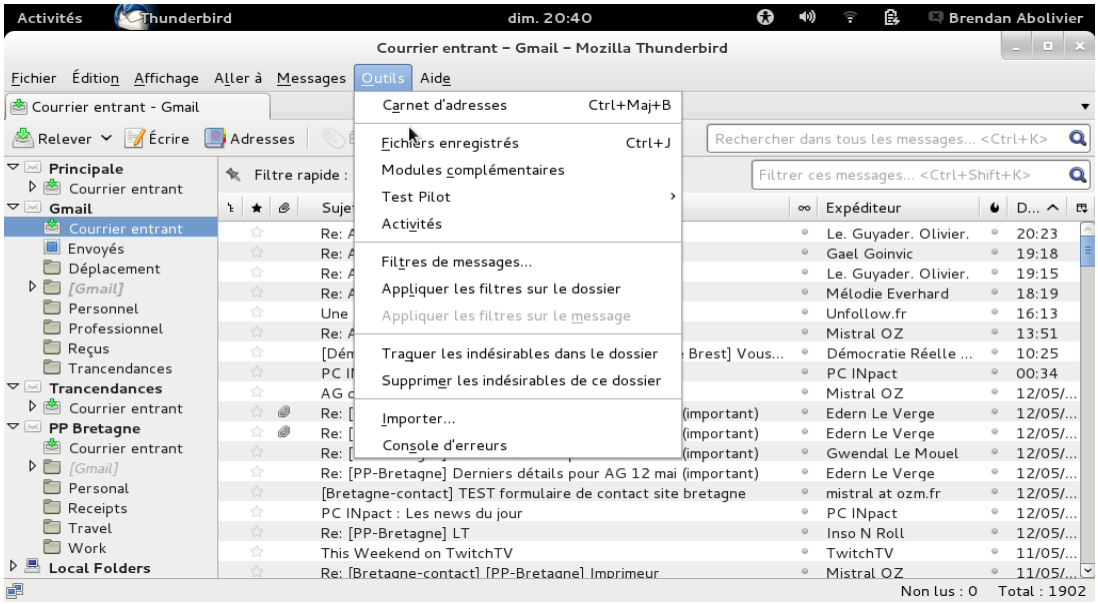
Tutoriel pour clef PGP avec Thunderbird

Si vous ne connaissez pas Thunderbird, il s'agit d'un client mail assez complet proposé par Mozilla. Si vous êtes sous Windows, vous pouvez le télécharger ici, si vous êtes sous Linux merci de voir avec la doc de votre distribution.

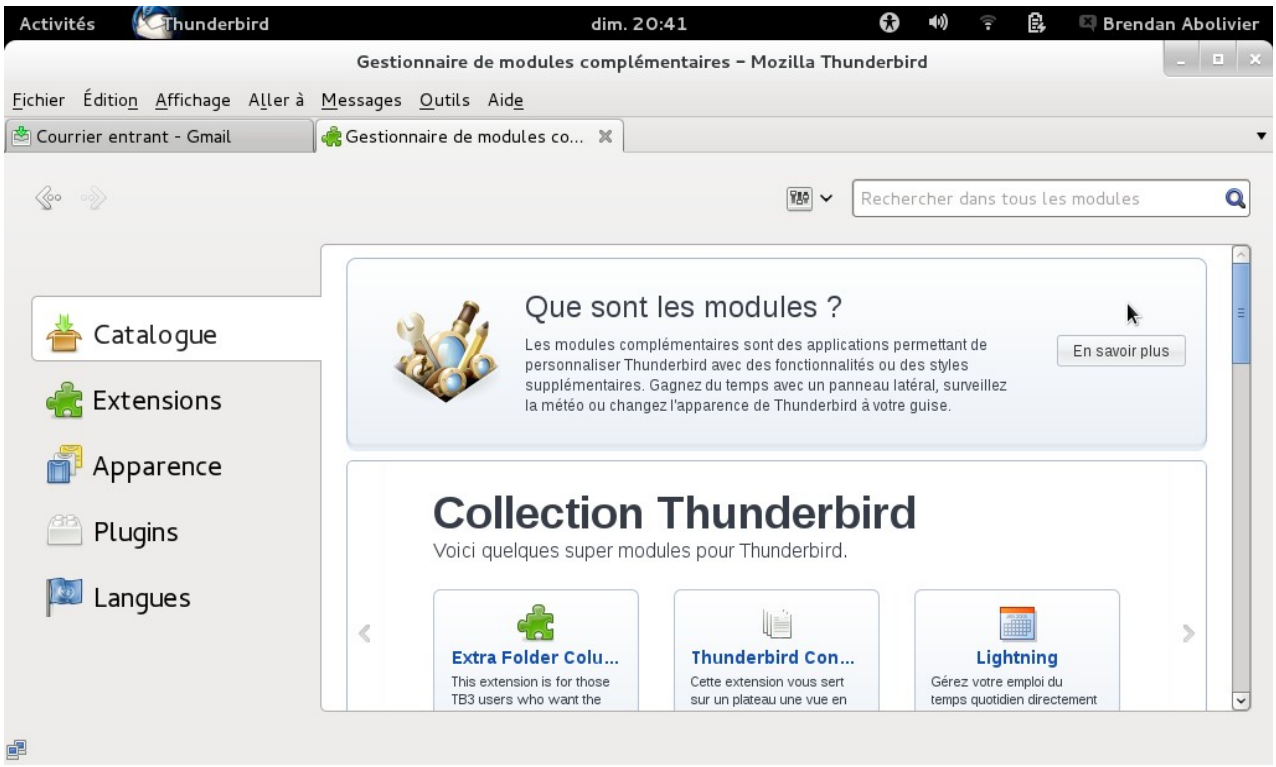
Tout d'abord, une fois que vous aurez téléchargé et installé Thunderbird, et que vous l'avez configuré (via l'utilitaire au démarrage), vous arrivez sur cette fenêtre :



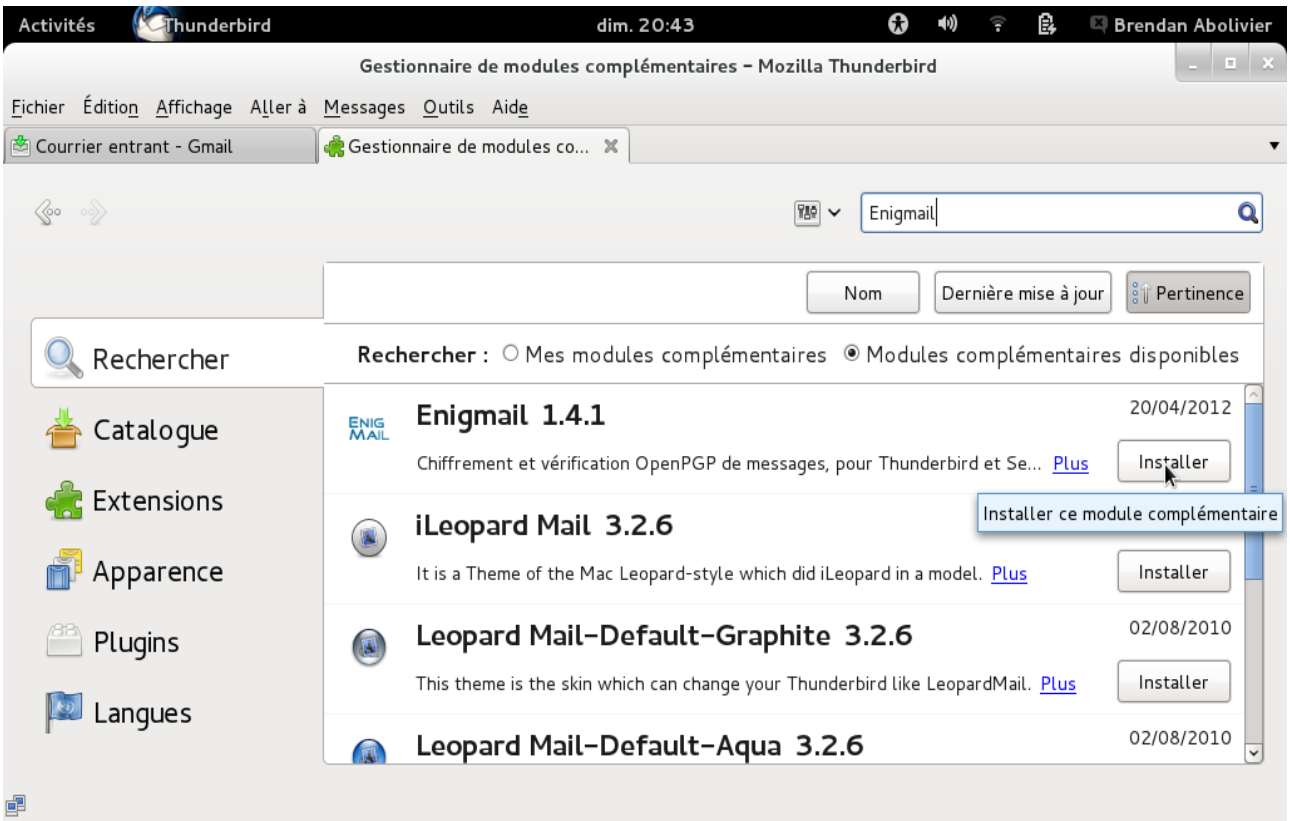
Allez dans l'onglet « Outils » puis cliquez sur « Modules complémentaires »

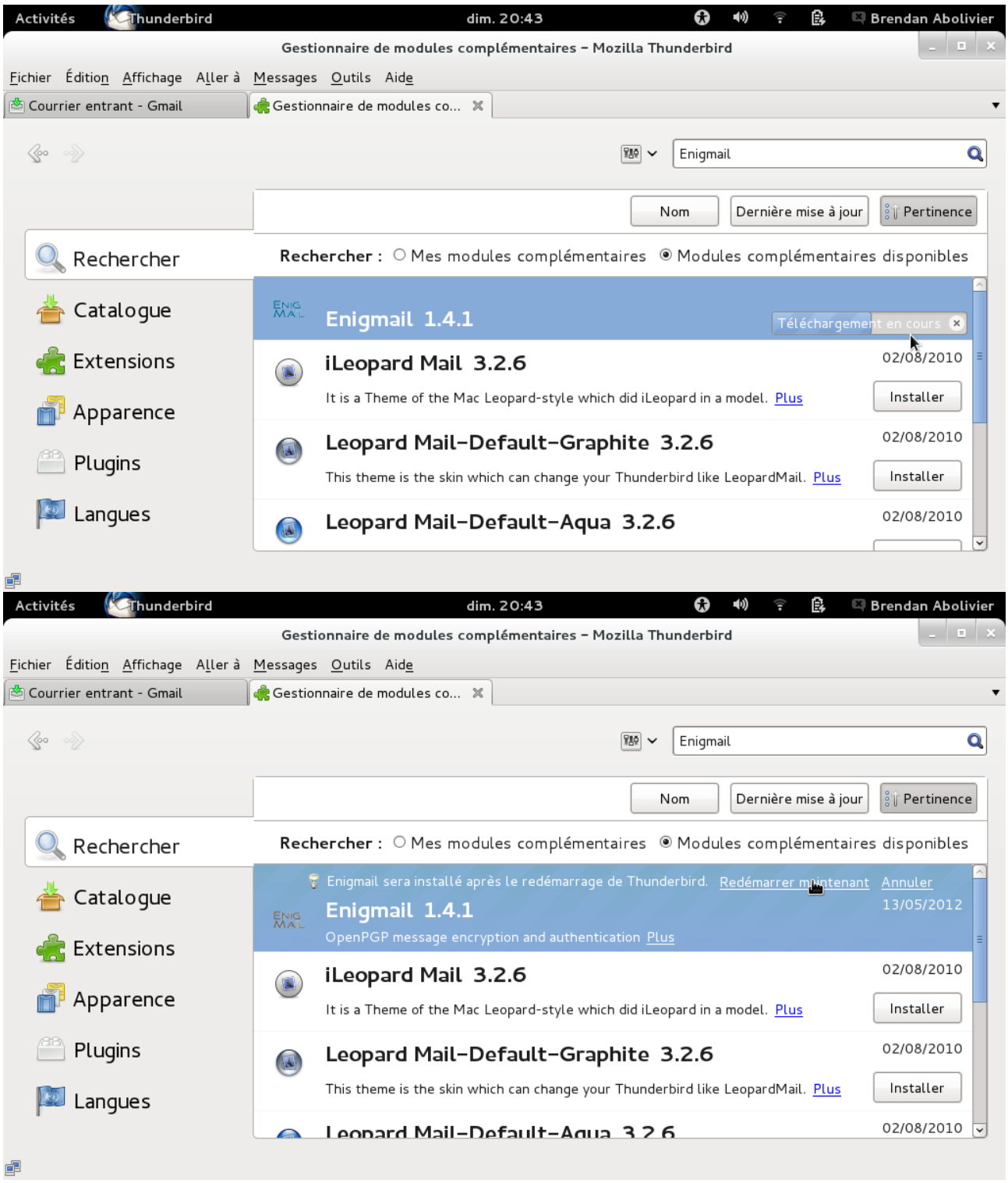


Vous arrivez normalement sur cette fenêtre :

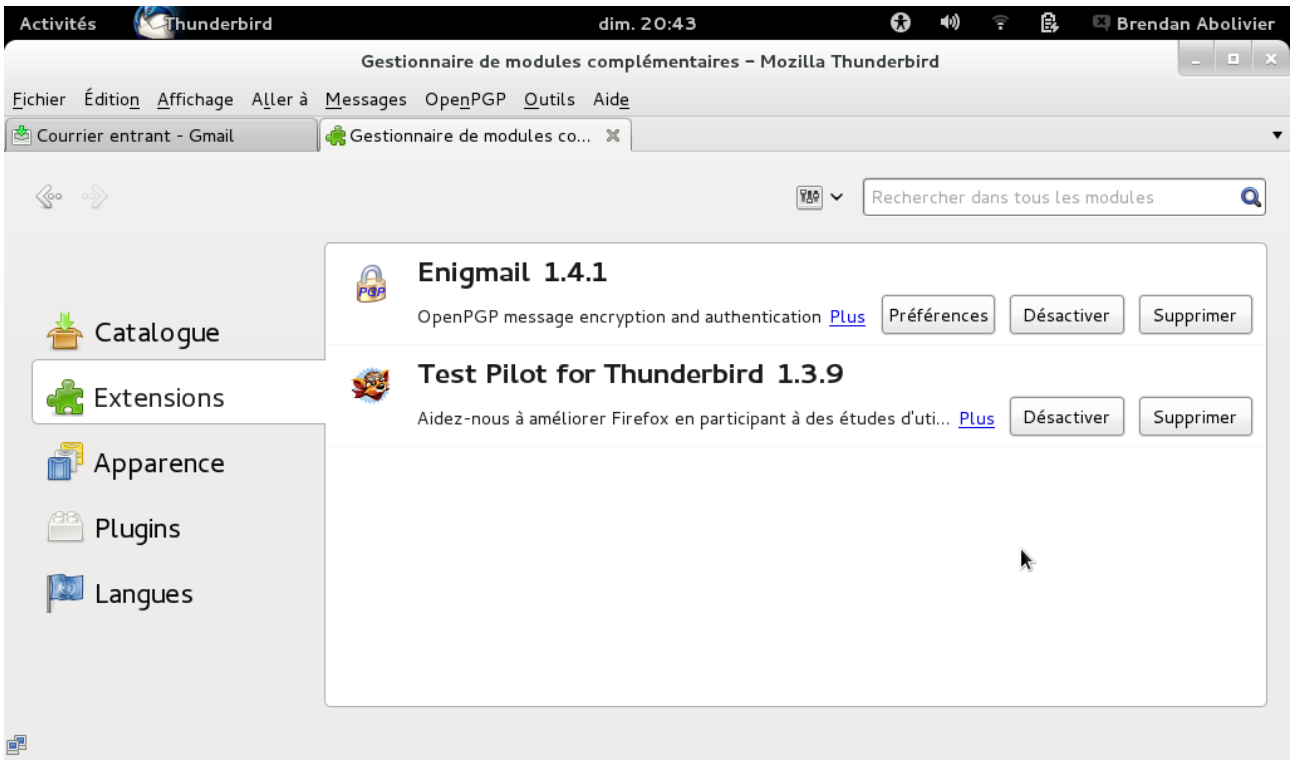


Cherchez « Enigmail » dans la barre de recherche, puis cliquez sur « Installer »

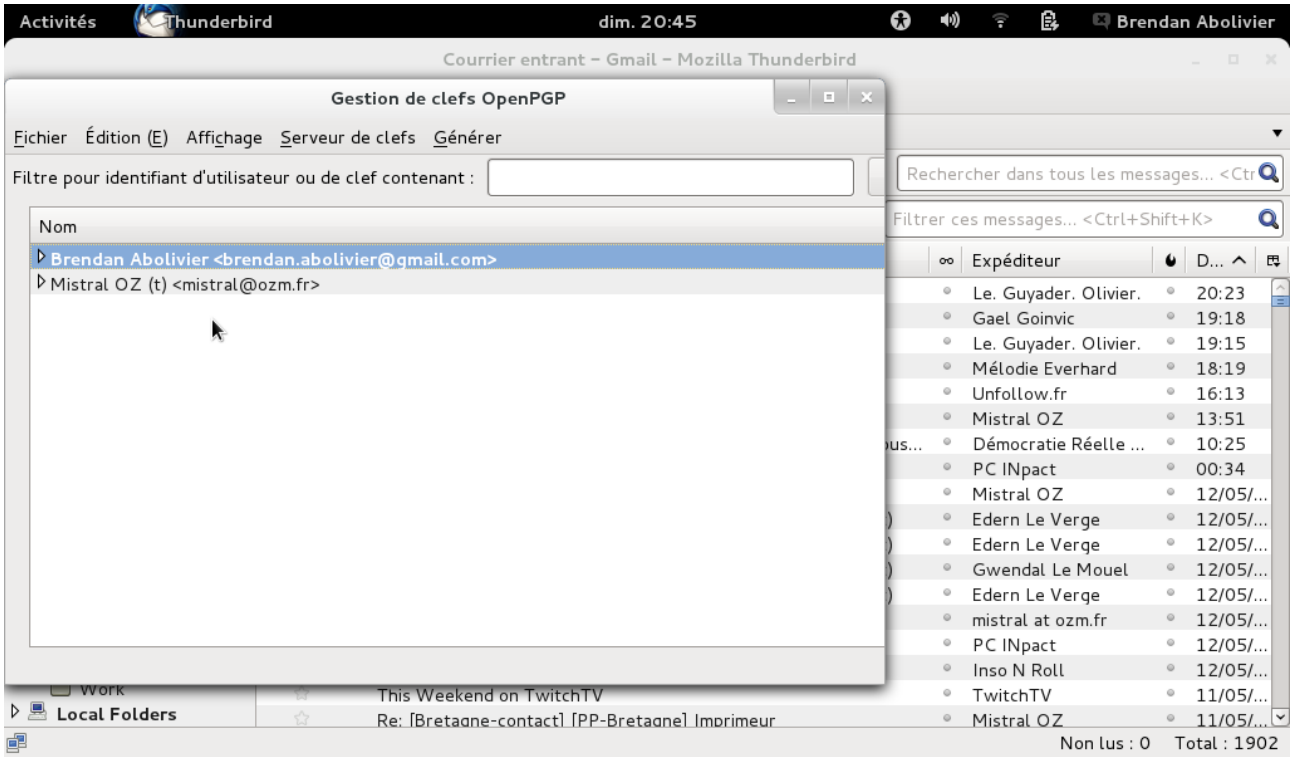




Thunderbird vous demande alors de redémarrer le logiciel. Cliquez sur « Redémarrer maintenant ». En arrivant sur l'onglet des modules complémentaires (plug-ins), vous pouvez voir qu'Enigmail a été installé et activé.

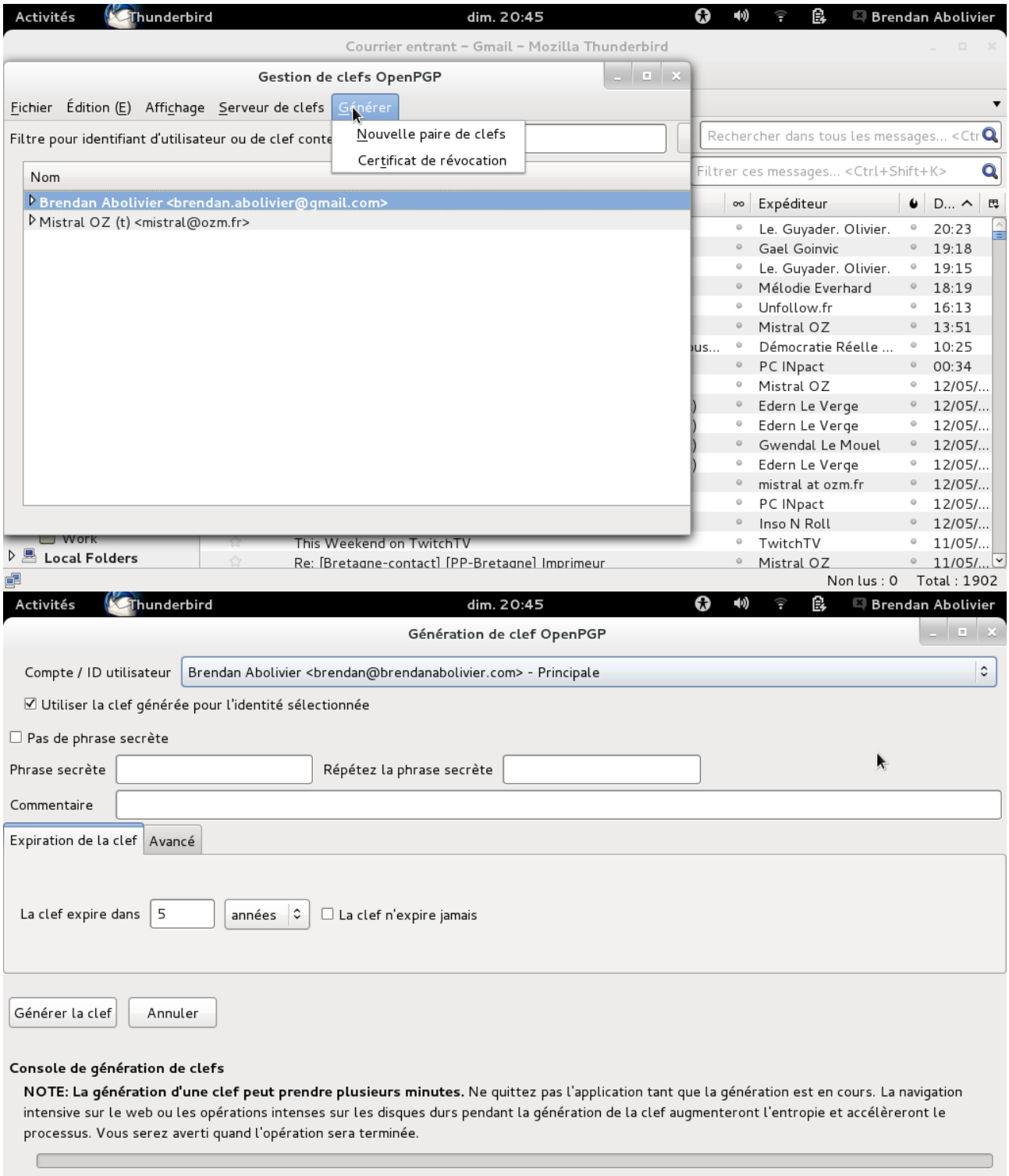


Vous pourrez aussi remarquer la présence d'un menu « OpenPGP » en haut de la fenêtre, qui permet de configurer le chiffrage PGP. Ouvrez-le puis cliquez sur « Gestion de clefs ». Vous avez alors cette fenêtre qui s'ouvre :



Vous pouvez voir la liste des clefs PGP enregistrées sur votre ordinateur. Ici, vous pouvez voir que je n'ai que deux clefs enregistrées : la mienne et celle de Mistral.

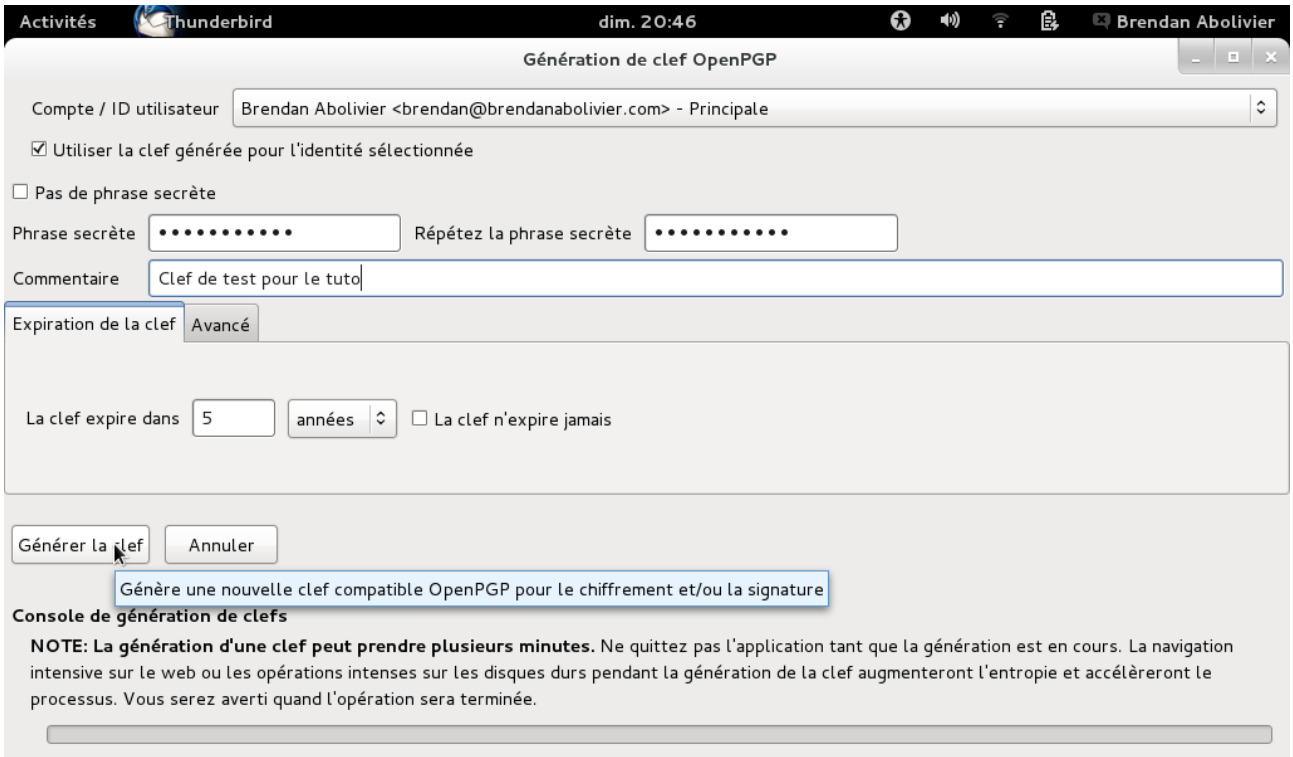
Cliquez sur le menu « Générer », puis sur « Nouvelle paire de clefs »



Vous pouvez changer l'adresse e-mail à laquelle sera attribuée cette clef avec le menu déroulant en haut de la fenêtre qui s'affiche alors. Rentrez votre phrase secrète. Une phrase secrète est un mot de passe nécessaire pour chaque configuration relative à la clef (comme un certificat de révocation, la suppression de la clef, etc).
Conservez-donc bien cette phrase secrète !

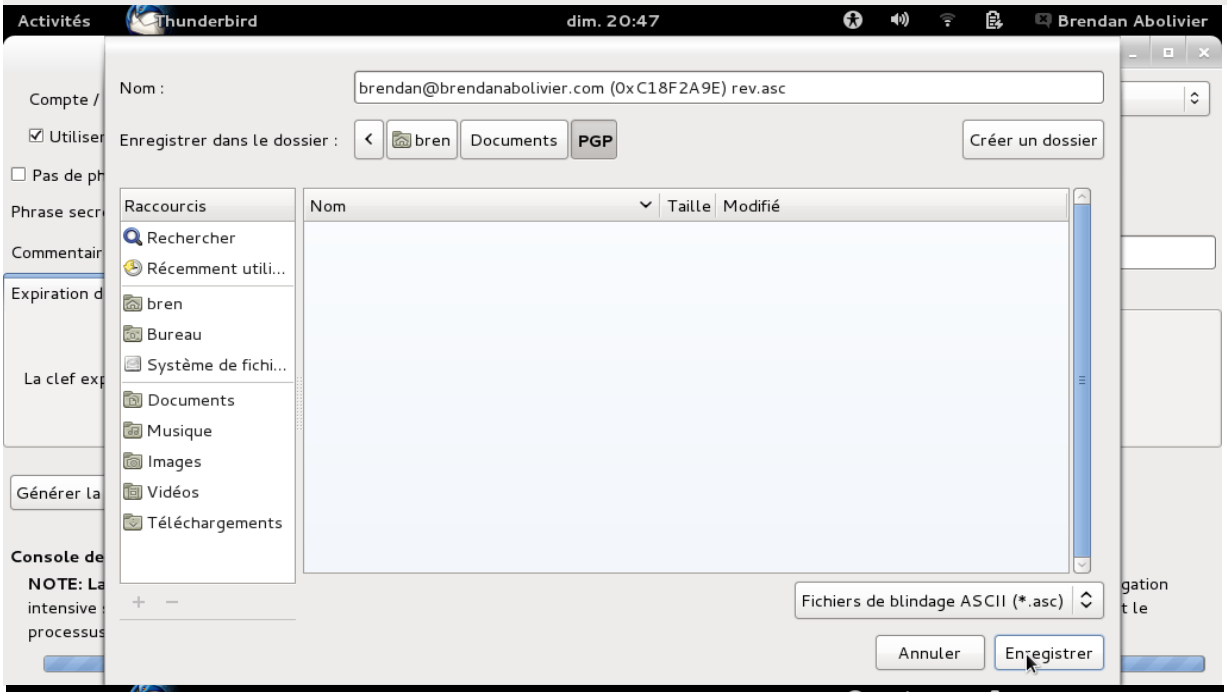
Vous pouvez également ajouter un commentaire afin d'identifier plusieurs clefs (par exemple si, pour une raison X, vous décidez de créer deux clefs pour une même adresse, vous pourrez ainsi les différencier).

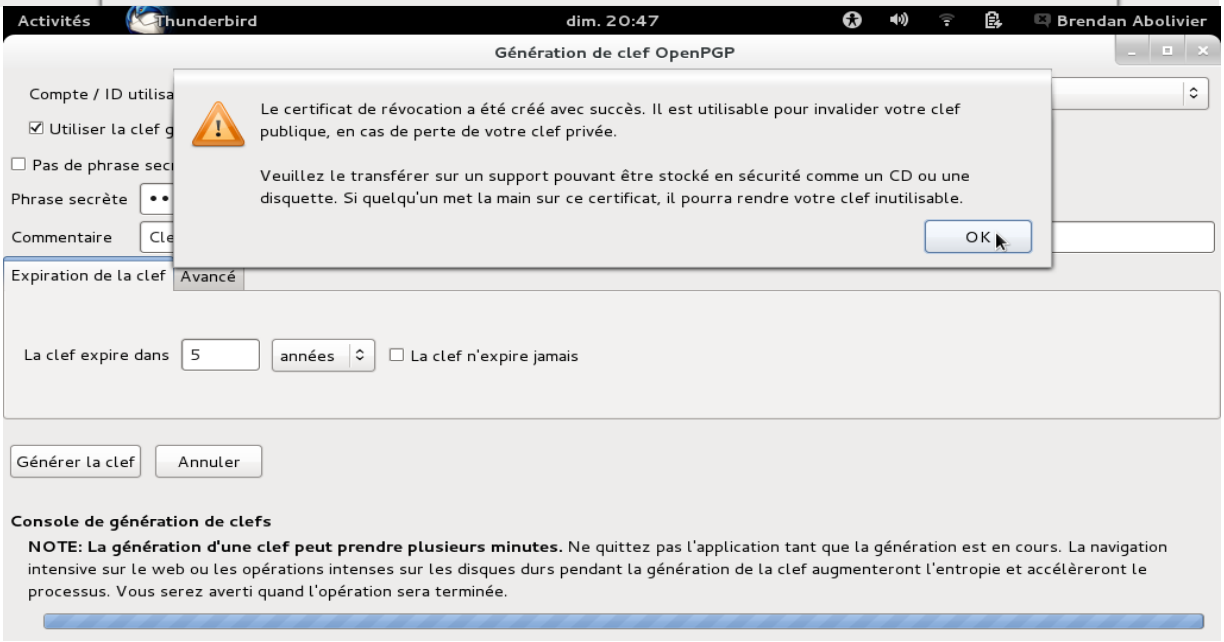
Une fois que vous aurez rempli tous les champs, cliquez sur « Générer la clef ».



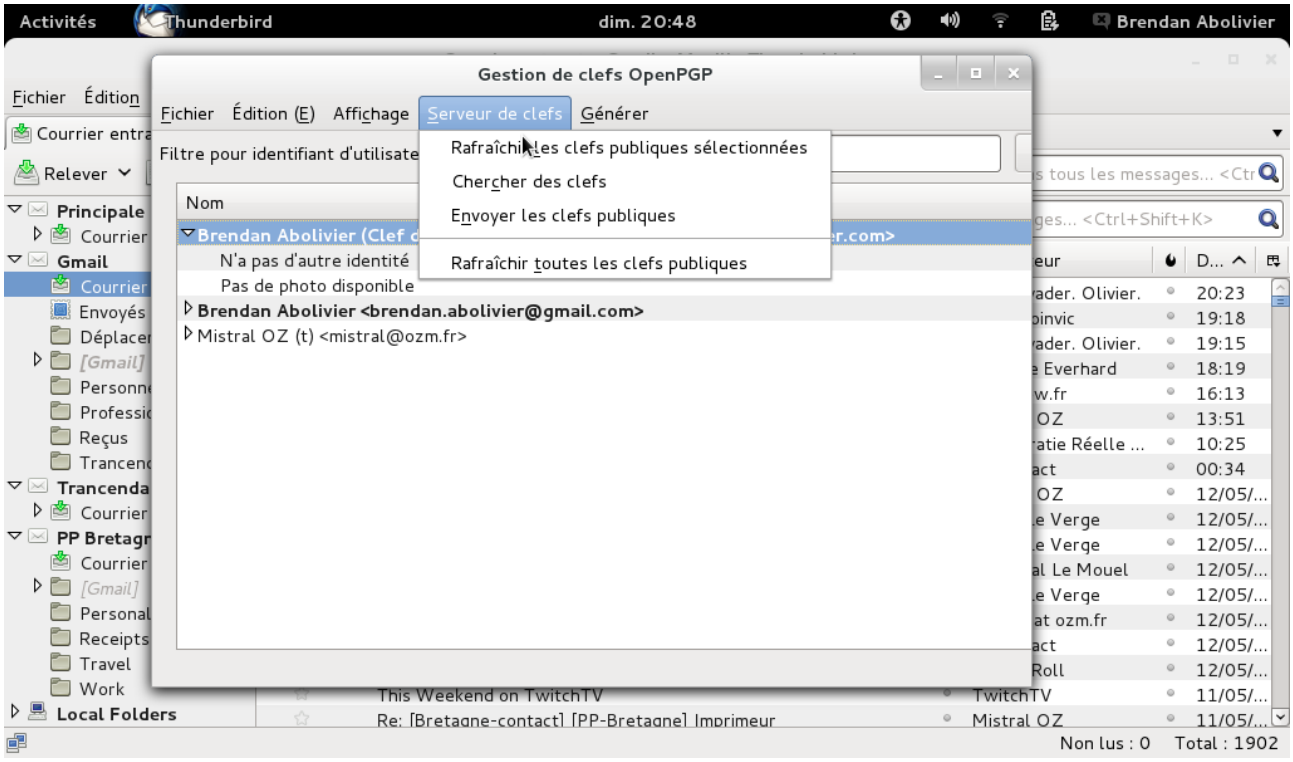
Pendant la génération de la clef, il est conseillé de faire des actions diverses comme bouger sa souris, taper au clavier, etc, pour ajouter un peu de hasard dans la génération et ainsi augmenter le niveau de sécurité de la clef.
A la suite de la génération, il est conseillé de générer un certificat de révocation de la clef. Celui-ci sert à « désactiver » la clef et est utile si, par exemple, la sécurité de la clef est compromise.
Si vous voulez générer ce certificat, cliquez sur « Générer le certificat ».
Enregistrez-le alors où vous voulez. Il vous sera ensuite demandé d'entrer la phrase secrète correspondant à la clef.


Activités
Thunderbird
dim. 20:46
Brendan Abolivier
Génération de clef OpenPGP
Génération de la clef terminée! L'identifiant <brendan@brendanabolivier.com> sera utilisé pour la signature.
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 ?
Annuler
Générer le certificat
Compte / ID utilisa
Utiliser la clef g
Pas de phrase secr
Phrase secrète
Commentaire
Expiration de la clef
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.

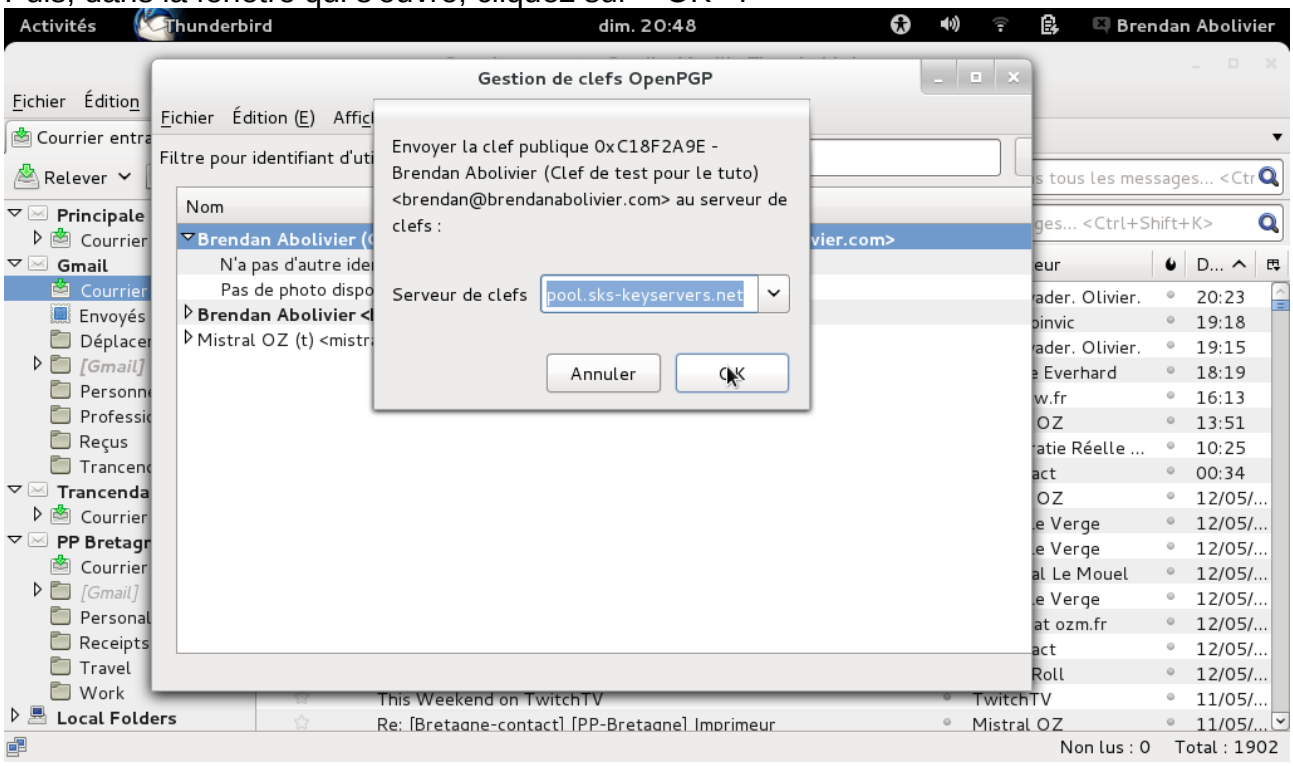

Activités
Thunderbird
dim. 20:47
Brendan Abolivier
Nom :
brendan@brendanabolivier.com (0xC18F2A9E) rev.asc
Enregistrer dans le dossier :
bren
Documents
PGP
Créer un dossier
Raccourcis
Rechercher
Récemment utili...
bren
Bureau
Système de fichi...
Documents
Musique
Images
Vidéos
Téléchargements
Nom
Taille
Modifié
Fichiers de blindage ASCII (*.asc)
Annuler
Enregistrer


Activités
Thunderbird
dim. 20:47
Brendan Abolivier
Génération de clef OpenPGP
Le certificat de révocation a été créé avec succès. Il est utilisable pour invalider votre clef publique, en cas de perte de votre clef privée.
Veuillez le transférer sur un support pouvant être stocké en sécurité comme un CD ou une disquette. Si quelqu'un met la main sur ce certificat, il pourra rendre votre clef inutilisable.
OK
Compte / ID utilisa
Utiliser la clef g
Pas de phrase secr
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.

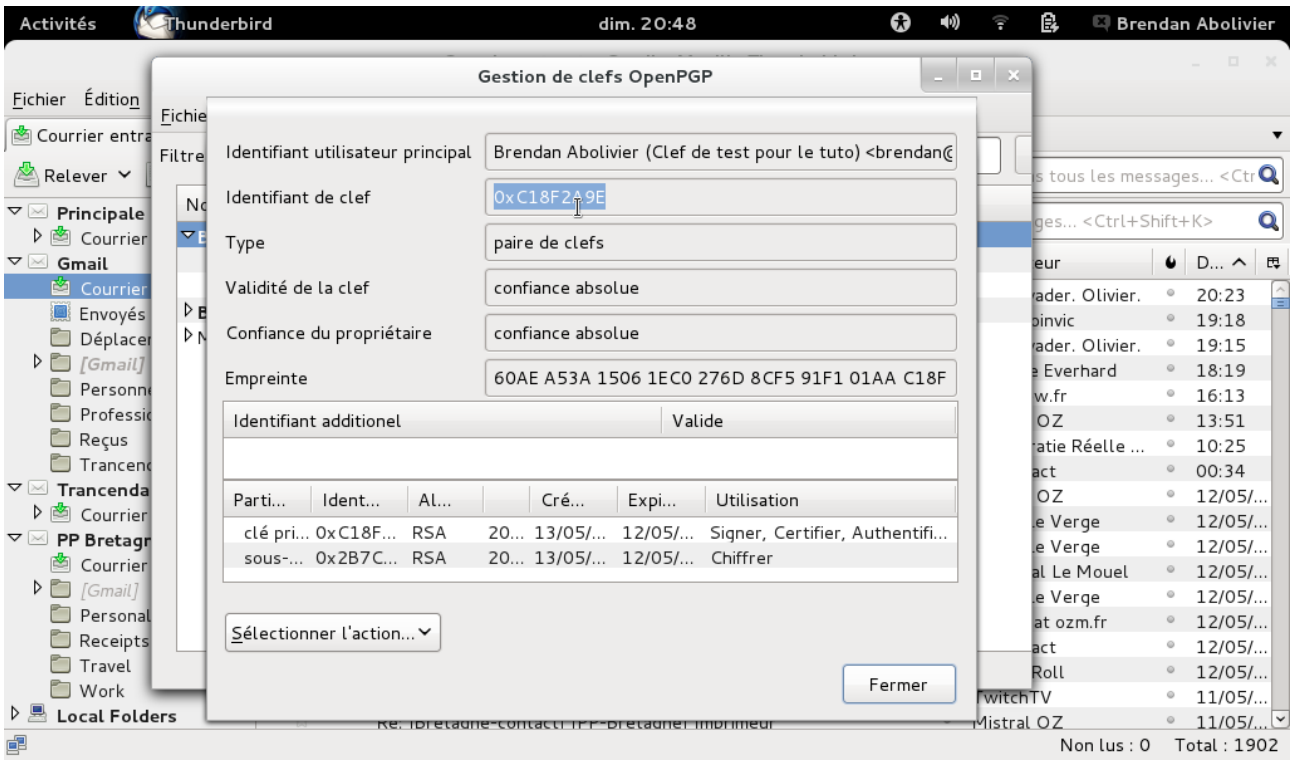
Ensuite, il vous faut envoyer votre clef sur un serveur de clefs. Pour cela, cliquez sur le menu « Serveur de clefs », puis sur « Envoyer les clefs publiques ».



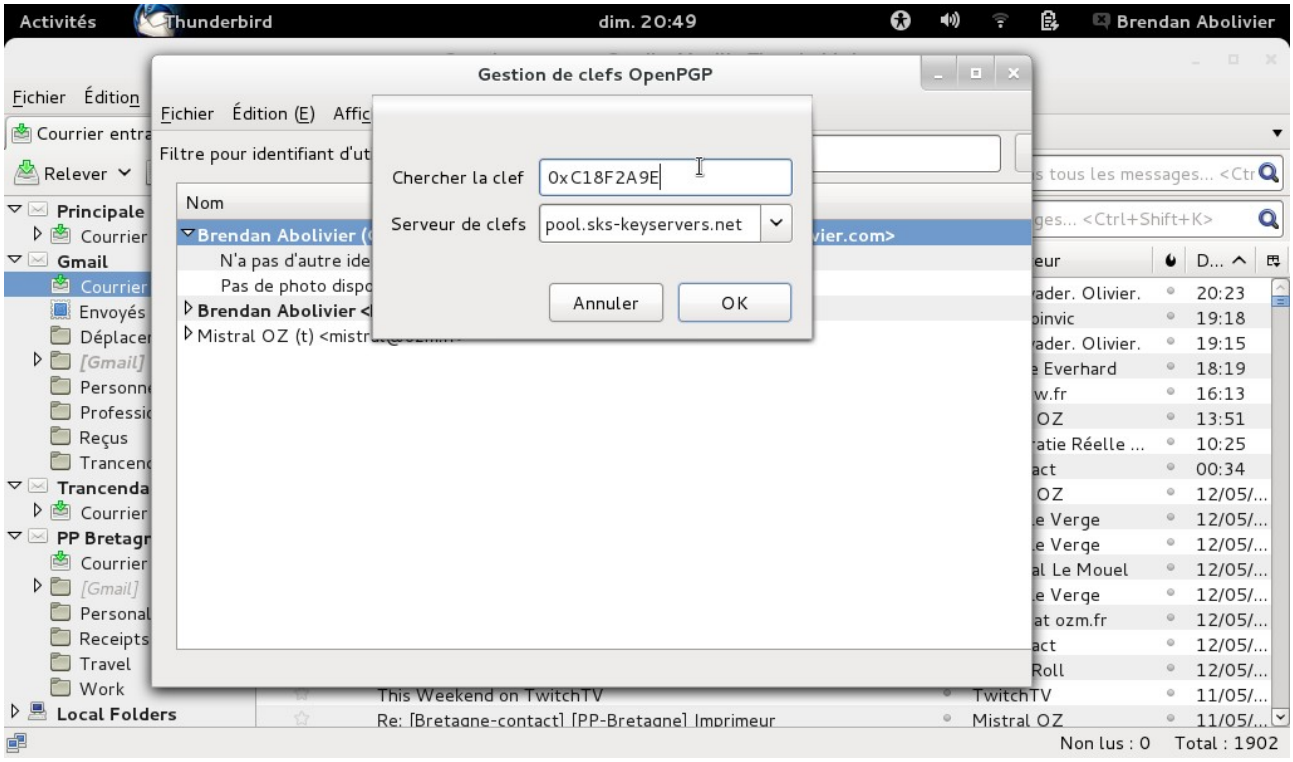
Puis, dans la fenêtre qui s'ouvre, cliquez sur « OK ».



Vous venez donc de créer votre propre clef PGP et d'envoyer la clef publique sur un serveur, à disposition de tous. Maintenant, toute personne ayant l'identifiant de votre clef pourra aller la récupérer sur le serveur de clefs et l'utiliser pour déchiffrer vos mails.
Pour connaître l'identifiant d'une clef, il vous suffit de double-cliquer sur son nom en gras dans la fenêtre principale d'Enigmail, afin de faire apparaître ses informations, dont son identifiant, une chaîne hexadécimale commençant par « 0x ».



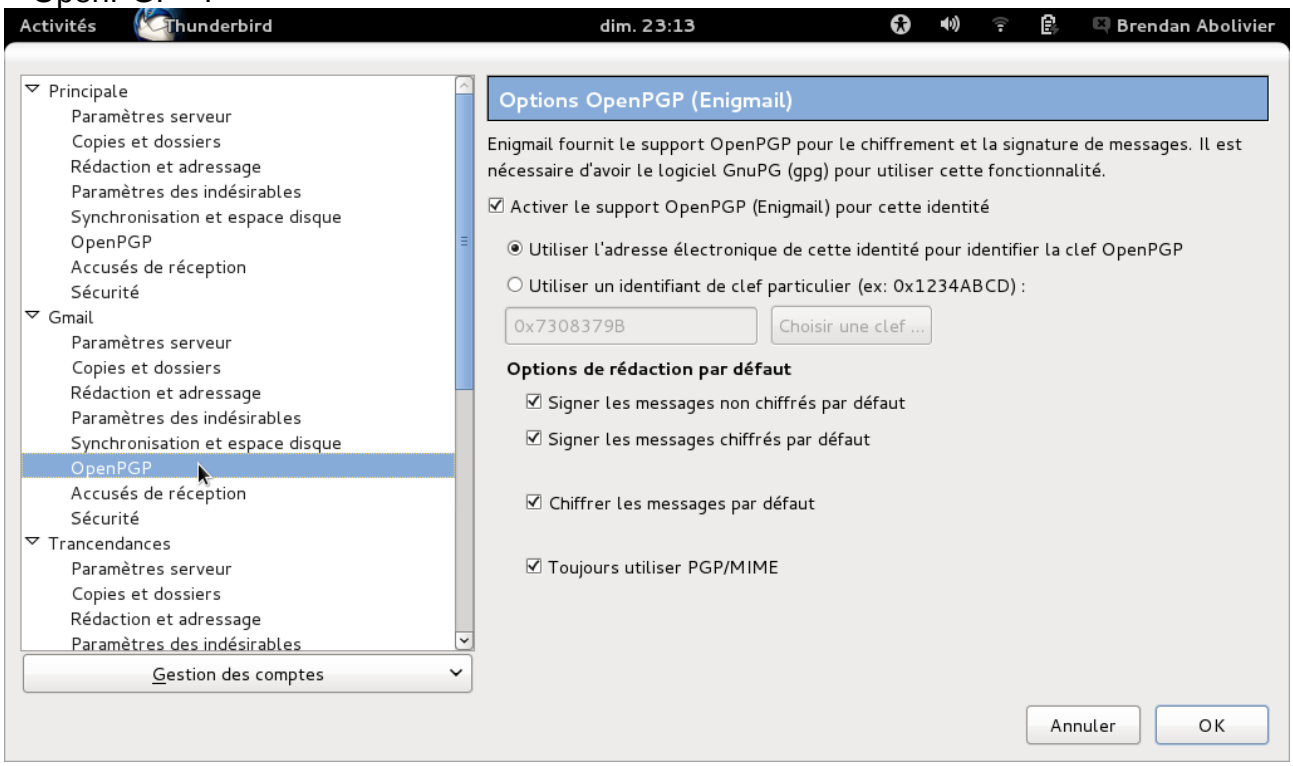
Maintenant, supposons que je vous ai envoyé ma clef PGP et que vous voulez l'ajouter à votre liste. Il vous suffit de cliquer sur « Serveur de clefs » de nouveau, puis sur « Chercher des clefs », puis de rentrer l'identifiant de la clef que vous voulez ajouter.



Cliquez sur « OK », et la clef est cherchée sur le serveur. Si elle est trouvée, elle est ajoutée à votre liste.

Maintenant, il faut paramétrer Thunderbird pour qu'il chiffre automatiquement vos e-mails sur la boîte concernée. Evidemment, cette configuration est optionnelle, et j'expliquerai plus bas comment chiffre au cas par cas (utile si les destinataires n'ont pas votre clef publique).

Rendez-vous dans le menu « Edition » de Thunderbird (sur l'écran principal), puis cliquez sur « Paramètres des comptes... ». Dans la fenêtre qui s'affiche, repérez le compte concerné par le chiffrement (si vous en avez configuré plusieurs), puis cliquez sur « OpenPGP ».

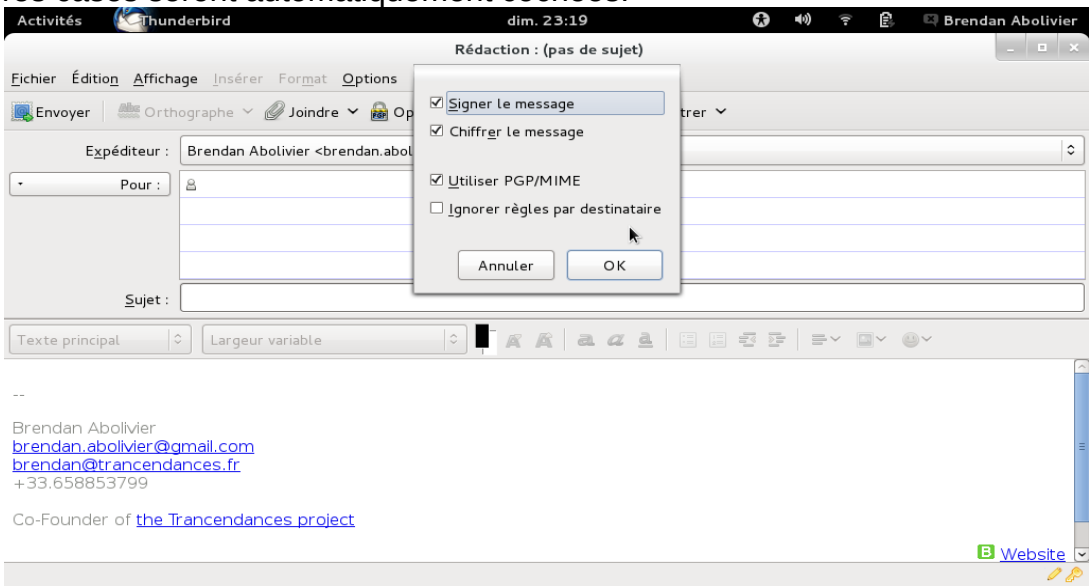


Cochez la case « Activer le support OpenPGP (Enigmail) pour cette identité », ainsi que « Utiliser l'adresse électronique de cette identit pour identifier la clef OpenPGP ». Ainsi, Enigmail comparera automatiquement l'adresse e-mail utilisée avec celles possédant une clef PGP afin de sélectionner celle qui correspond.

Personnellement, j'ai coché les quatre cases plus bas, ainsi tous mes messages envoyés via ma boîte Gmail (celle que j'utilise pour les mails du PP) seront chiffrés par défaut.

Si vous préférez chiffre au cas par cas, alors ne cochez pas ces cases. Lors de la rédaction d'un mail, cliquez sur l'icône « OpenPGP » en haut de la fenêtre de rédaction pour afficher les options de chiffrement et activer les options qui vous intéresse.

Notez que si, comme moi, vous avez sélectionné toutes les options par défaut, les trois premières cases seront automatiquement cochées.



Voilà, en espérant que ce tuto ne vous aura pas assomé :)

Bren