Fiche Pratique N°92 : Chiffrez vos e-mails avec OpenPGP dans Thunderbird V1.1

15 nov, 2026 · @Gabriel

Objectif : *envoyer et recevoir des e-mails chiffrés de bout en bout avec Thunderbird, quel que soit votre fournisseur de messagerie, pour que seuls vous et votre correspondant puissiez les lire.*

- ***Public visé :*** *intermédiaire à avancé*
- ***Temps estimé :*** *30 minutes pour la mise en place ; quelques minutes par nouveau correspondant*
- ***Difficulté :*** ★★★☆☆ *(Moyen)*
- ***Prérequis :*** *Thunderbird installé et configuré avec votre adresse e-mail ; un gestionnaire de mots de passe (fiche N°16) ; un correspondant prêt à essayer*
- ***Fiches associées :*** *N°10 (mail éthique), N°56 (alias de courriel), N°37 (vérifier l'intégrité avec GPG), N°16 (mots de passe), N°26 (chiffrer ses fichiers), N°19a à N°19e (sauvegardes), N°89 (sauvegarde hors site)*

PARTIE 1 : LES BASES (pour débutants)

1. Le problème : un e-mail ordinaire se lit comme une carte postale

Un e-mail classique est stocké en clair chez votre fournisseur et chez celui de votre correspondant. Même chez un fournisseur respectueux, il est lisible par le serveur, et donc exposé en cas de piratage, de réquisition ou de fuite. Proton Mail et Tuta chiffrent les échanges entre leurs propres utilisateurs, mais un message envoyé vers Gmail ou Orange redevient ordinaire, sauf précautions (section 8).

Situation	Conséquence
Vous envoyez un document médical ou juridique par e-mail	Il reste lisible sur les serveurs des deux fournisseurs
Votre fournisseur est piraté	Vos anciens messages peuvent être lus
Vous écrivez de Proton Mail à une adresse Gmail	Le message arrive en clair chez Google
Vous échangez avec un militant, un journaliste ou un avocat	Vous exposez aussi votre correspondant
Vous recevez un e-mail « de votre banque »	Rien ne prouve qu'il vient vraiment d'elle

Une image pour comprendre : OpenPGP fonctionne avec un **cadenas** et une **clé**. Vous distribuez librement des cadenas ouverts (votre **clé publique**) : n'importe qui peut fermer une boîte avec, mais seule votre clé (votre **clé privée**, que vous gardez) peut l'ouvrir. Pour vous écrire, votre correspondant ferme le message avec votre cadenas.

Le risque : des échanges sensibles lisibles par d'autres que leur destinataire.

Le bénéfice : des messages que seuls vous et votre correspondant pouvez lire, chez n'importe quel fournisseur, avec en prime une signature qui prouve que le message vient bien de vous.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°92 : Chiffrez vos e-mails avec OpenPGP dans Thunderbird V1.1

2. Comprendre OpenPGP

Élément	Ce que c'est	À faire
Clé publique	Le « cadenas ouvert » que vous partagez	La donner à vos correspondants, la publier
Clé privée (ou secrète)	La « clé » qui ouvre vos messages	La garder pour vous, la sauvegarder, ne jamais l'envoyer
Chiffrement	Seul le destinataire peut lire	Nécessite la clé publique du destinataire
Signature	Prouve que le message vient de vous et n'a pas été modifié	Joint automatiquement votre clé publique dans Thunderbird
Empreinte	Suite de caractères qui identifie une clé	La comparer de vive voix pour vérifier une clé

Ce qui n'est pas chiffré : l'expéditeur, les destinataires et la date restent visibles, comme l'adresse sur une enveloppe. L'objet peut l'être selon le logiciel : écrivez un objet neutre.

Avant de commencer

- ☐ Thunderbird est **à jour** et mon compte e-mail fonctionne
- ☐ J'ai un **gestionnaire de mots de passe** pour la phrase secrète de sauvegarde (fiche N°16)
- ☐ J'ai un **correspondant** prêt à faire l'essai avec moi
- ☐ Je sais que **perdre ma clé privée, c'est perdre l'accès** à mes messages chiffrés : je la sauvegarderai

3. Pas à pas : créer votre clé dans Thunderbird

Thunderbird intègre OpenPGP : aucun module à installer.

1. Ouvrez **Paramètres des comptes**, choisissez votre compte, puis la rubrique **Chiffrement de bout en bout**.
    - Vous devez voir : une section **OpenPGP** avec un bouton **Ajouter une clé…**
2. Cliquez sur **Ajouter une clé…** › **Créer une nouvelle clé OpenPGP**. Gardez les réglages proposés et choisissez une date d'expiration (2 ou 3 ans ; elle se prolonge facilement).
    - Vous devez voir : votre nouvelle clé, avec votre adresse e-mail, sélectionnée comme clé personnelle de ce compte.
3. **Sauvegardez la clé privée** : dans **Outils** › **Gestionnaire de clés OpenPGP**, sélectionnez votre clé, puis **Fichier** › **Sauvegarder la ou les clés secrètes dans un fichier**. Choisissez une phrase secrète et notez-la dans votre gestionnaire de mots de passe.
    - Vous devez voir : un fichier `.asc` protégé, à ranger avec vos sauvegardes (fiches N°19a à N°19e et N°89).
4. **Activez la signature par défaut** dans **Chiffrement de bout en bout** (option de signature des messages non chiffrés).

gabriel.ananda@mailo.com
CC BY SA

- Vous devez voir : vos messages partent signés, avec votre clé publique jointe : vos correspondants la reçoivent ainsi automatiquement.

4. Pas à pas : échanger un premier message chiffré

1. **Envoyez un message signé** à votre correspondant (il contient votre clé publique), et demandez-lui de faire de même.
   - Vous devez voir : un message reçu avec une mention OpenPGP dans l'en-tête et une clé jointe.
2. **Acceptez sa clé** : ouvrez son message, cliquez sur la mention OpenPGP de l'en-tête, puis acceptez la clé. Idéalement, comparez l'**empreinte** de vive voix ou par téléphone, et marquez-la comme vérifiée.
   - Vous devez voir : sa clé dans le **Gestionnaire de clés OpenPGP**.
3. **Rédigez votre message** et cliquez sur le bouton **Chiffrer** de la barre d'outils de rédaction.
   - Vous devez voir : un cadenas activé ; si la clé d'un destinataire manque, Thunderbird vous le signale.
4. **Envoyez**, et demandez à votre correspondant de vous répondre chiffré.
   - Vous devez voir : sa réponse s'ouvre normalement dans Thunderbird, avec la mention « chiffré » dans l'en-tête.

5. À quoi s'attendre et dépannage

Symptôme	Cause possible	Action
Le bouton **Chiffrer** refuse d'envoyer	La clé publique d'un destinataire manque ou n'est pas acceptée	Demandez-lui un message signé, ou cherchez sa clé sur keys.openpgp.org
Mon correspondant voit des pièces jointes étranges	Son logiciel ne gère pas OpenPGP	Il doit utiliser Thunderbird, Proton Mail ou un outil compatible
Je ne peux plus lire mes anciens messages chiffrés	Clé privée perdue (réinstallation, nouvel ordinateur)	Réimportez la sauvegarde `.asc` ; sans elle, ces messages sont perdus
Ma clé a expiré	Date d'expiration atteinte	Prolongez-la dans le Gestionnaire de clés, puis renvoyez votre clé publique
Le webmail affiche un message illisible	Le déchiffrement se fait dans Thunderbird, pas dans le webmail	Lisez-le dans Thunderbird

PARTIE 2 : ALLER PLUS LOIN (pour intermédiaires et avancés)

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°92 : Chiffrez vos e-mails avec OpenPGP dans Thunderbird V1.1

6. Publier votre clé et trouver celle des autres

1. **Publiez votre clé publique** sur le serveur `keys.openpgp.org` : il vous envoie un e-mail de vérification avant de la rendre trouvable par votre adresse.
    - Vous devez voir : un message de keys.openpgp.org ; après validation, votre clé est trouvable par votre adresse.
2. **Cherchez une clé** : **Gestionnaire de clés OpenPGP** › **Serveur de clés** › **Rechercher en ligne**, avec l'adresse du correspondant.
    - Vous devez voir : la clé proposée à l'import ; vérifiez son empreinte avant de lui faire confiance.

7. Sur le téléphone et dans le navigateur

Outil	Où	Points forts	Limites
Thunderbird (ordinateur)	Windows, macOS, Linux	OpenPGP intégré, libre	Il faut gérer ses clés soi-même
Thunderbird pour Android + **OpenKeychain**	Android	Libre ; cadenas vert quand le message est chiffré	Le chiffrement repose sur OpenKeychain, à installer à part
Proton Mail	Web, Android, iPhone	Clés gérées automatiquement, compatible OpenPGP	Les échanges avec Gmail restent en clair sans clé du destinataire
Mailvelope	Extension de navigateur	OpenPGP dans un webmail (Gmail, Outlook…)	Moins pratique au quotidien

Pour utiliser la même clé sur le téléphone, importez votre sauvegarde `.asc` dans OpenKeychain, puis activez **OpenPGP** dans les paramètres du compte de Thunderbird pour Android (**Chiffrement de bout en bout**).

8. Selon votre fournisseur : Proton, Tuta, Mailo

Fournisseur	OpenPGP	Thunderbird (IMAP)	Chiffrer vers une adresse ordinaire
Proton Mail (Suisse)	Oui, compatible	Seulement avec Proton Mail Bridge (offres payantes)	Avec la clé OpenPGP du destinataire, ou un message protégé par mot de passe
Tuta (Allemagne)	Non : chiffrement propre à Tuta	Non : pas d'IMAP	Message protégé par un mot de passe partagé
Mailo (France)	Oui, intégré au webmail	Oui, en IMAP	Avec la clé OpenPGP du destinataire

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°92 : Chiffrez vos e-mails avec OpenPGP dans Thunderbird V1.1

Proton Mail

Proton chiffre automatiquement les échanges entre ses utilisateurs et sait échanger avec les utilisateurs OpenPGP. Ouvrez un message signé de votre correspondant Thunderbird et cliquez sur **Faire confiance à la clé** ; pour envoyer votre clé Proton, activez **Joindre la clé publique** dans le menu de rédaction. Proton recommande le format **PGP/MIME**.

Tuta (anciennement Tutanota)

Tuta n'utilise **pas OpenPGP** et ne propose **pas d'IMAP** : on ne peut pas s'en servir avec Thunderbird. Sa logique est différente :

- **Entre utilisateurs de Tuta**, tout est chiffré automatiquement, objet compris, avec des algorithmes conçus pour résister aux futurs ordinateurs quantiques.
- **Vers une adresse ordinaire** (Gmail, Orange…) : rédigez le message dans Tuta ; au moment de saisir l'adresse externe, Tuta vous propose de créer un **mot de passe partagé**. Transmettez ce mot de passe par un autre canal (de vive voix, par Signal). Le destinataire reçoit un lien, saisit le mot de passe, lit le message et peut répondre de façon chiffrée.
    - Vous devez voir : un champ de mot de passe sous l'adresse du destinataire externe.
- **Avec un correspondant qui utilise OpenPGP** : Tuta ne peut ni lire ses messages chiffrés ni utiliser sa clé. Utilisez le message protégé par mot de passe.

Mailo

Mailo, messagerie française, intègre OpenPGP **directement dans son webmail** : génération et import de clés, envoi chiffré ou signé, lecture des messages chiffrés, sur tous vos appareils sans rien installer.

1. Dans le webmail de Mailo, ouvrez la gestion des **clés PGP** et générez une paire de clés (adresse, nom, durée de validité). **Définissez une phrase secrète** : elle est facultative chez Mailo, mais c'est elle qui protège votre clé privée ; Mailo ne la conserve pas et ne peut pas la réinitialiser.
    - Vous devez voir : votre clé dans votre trousseau PGP Mailo.
2. À la rédaction, choisissez l'option de **chiffrement PGP** et/ou de **signature**, et joignez votre clé publique au premier envoi.
    - Vous devez voir : une icône PGP sur le message envoyé.

Mailo ou Thunderbird ? Dans le webmail, Mailo gère vos clés sur ses serveurs, en tant que tiers de confiance : c'est pratique, mais moins strict qu'un chiffrement où la clé privée ne quitte jamais votre ordinateur. Si vous voulez cela, utilisez Mailo **en IMAP dans Thunderbird** (paramètres dans le webmail : **Options** › **Synchronisation**) et gérez vos clés dans Thunderbird (sections 3 et 4). Pour garder la même clé des deux côtés, exportez-la de l'un et importez-la dans l'autre. ⚠️ Dans le webmail de Mailo, l'objet du message n'est pas chiffré ; dans Thunderbird, cela dépend des réglages : écrivez de toute façon un objet neutre.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°92 : Chiffrez vos e-mails avec OpenPGP dans Thunderbird V1.1

À savoir avant de se lancer

Crainte fréquente	La réalité
« C'est réservé aux informaticiens. »	Dans Thunderbird, c'est un bouton à la rédaction ; le plus délicat est l'échange des clés, une fois par correspondant.
« Mon correspondant doit avoir le même fournisseur. »	Non : OpenPGP fonctionne entre fournisseurs différents, dès qu'il a une clé. Exception : Tuta, qui utilise son propre chiffrement (section 8).
« Tout est caché. »	Non : l'expéditeur, le destinataire et la date restent visibles.
« Si je perds ma clé, je la récupère auprès du fournisseur. »	Non : personne d'autre ne l'a. D'où la sauvegarde de l'étape 3.

Challenge 7 jours

- **Jour 1 :** mettez Thunderbird à jour et vérifiez votre compte.
- **Jour 2 :** créez votre clé OpenPGP.
- **Jour 3 :** sauvegardez la clé privée et notez la phrase secrète.
- **Jour 4 :** échangez des messages signés avec un correspondant.
- **Jour 5 :** vérifiez vos empreintes de vive voix, puis envoyez un premier message chiffré.
- **Jour 6 :** publiez votre clé sur keys.openpgp.org.
- **Jour 7 :** installez OpenKeychain et Thunderbird pour Android si vous lisez vos e-mails sur le téléphone.

Vous allez constater : une fois les clés échangées, chiffrer un message ne prend qu'un clic.

En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Créer et sauvegarder sa clé	Un chiffrement que vous contrôlez	Section 3
Échanger les clés et vérifier les empreintes	La certitude d'écrire à la bonne personne	Section 4
Signer ses messages	La preuve que vos messages viennent de vous	Section 3
Publier sa clé	Vos correspondants vous trouvent facilement	Section 6

À retenir absolument

- **La clé publique se partage, la clé privée se garde** et se sauvegarde.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°92 : Chiffrez vos e-mails avec OpenPGP dans Thunderbird V1.1

- **Chiffrer suppose la clé publique du destinataire** : commencez par un message signé.
- **Vérifiez les empreintes** de vive voix avec vos correspondants importants.
- **L'enveloppe reste visible** : expéditeur, destinataire et date ne sont pas chiffrés.

Test final :

1. J'ai créé ma clé OpenPGP dans Thunderbird.
2. Ma clé privée est sauvegardée, avec sa phrase secrète en lieu sûr.
3. J'ai échangé des clés avec au moins un correspondant.
4. J'ai envoyé et reçu un message chiffré.
5. Je sais ce qui reste visible dans un e-mail chiffré. ✅

Références

- Mozilla – Configurer votre compte pour le chiffrement de bout en bout (Thunderbird)
- Mozilla – OpenPGP dans Thunderbird pour Android
- Proton – Comment utiliser PGP avec Proton Mail
- Privacy Guides – Clients de messagerie électronique
- Tuta – Comment envoyer un courriel chiffré dans Tuta Mail gratuitement
- Tuta – Tuta vs. StartMail (absence d'IMAP, chiffrement de l'objet)
- Mailo – PGP encryption (intégration au webmail)
- Mailo – PGP keys (phrase secrète)
- Mailo – Sending PGP e-mails
- Mailo – Accès IMAP4 et POP3
- keys.openpgp.org – Serveur de clés OpenPGP

gabriel.ananda@mailo.com
CC BY SA