

## TP Signature Electronique

### Contexte

Le contexte de M@Banque, tel que détaillé dans le TP « identité numérique », s'applique aussi à ce TP.

Veuillez-vous référer au TP en question si besoin.

### Problématique

Afin d'assurer les contraintes de la preuve numérique lors de la signature d'un contrat, vous souhaitez proposer à Mme. Schmitt une solution possible. La signature des contrats se fera toujours par email mais avec une surcouche permettant d'assurer l'intégrité, l'authenticité et la confidentialité des messages.

### Table des matières

1) Installation et configuration .....	2
2) Génération de clé .....	3
3) Partage de clé .....	4
4) Signature et chiffrement .....	7

### Introduction

En suivant ce TP, vous verrez toutes les étapes nécessaires pour utiliser un logiciel permettant d'assurer l'intégrité, l'authenticité et la confidentialité des messages.

## 1) Installation et configuration

Téléchargez et installez le client mail « Thunderbird » sur votre poste de travail :

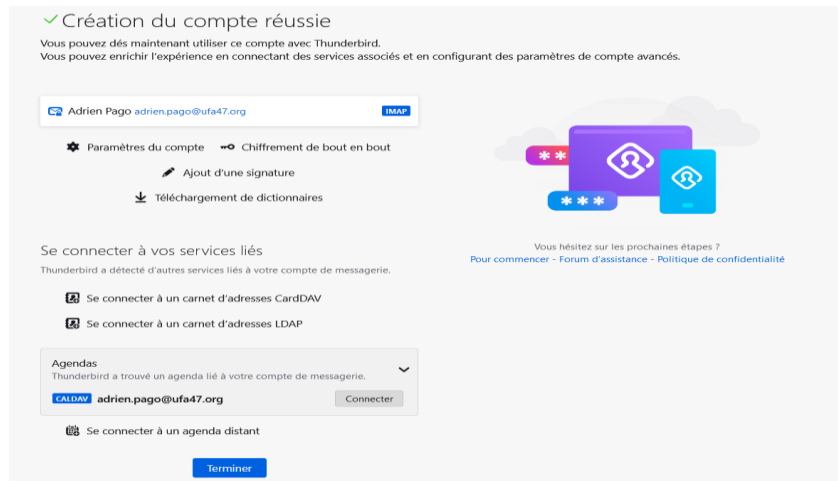
<https://www.thunderbird.net/fr/>

IMAP (Internet Message Access Protocol) est un protocole de courrier électronique qui permet aux utilisateurs d'accéder à leurs messages depuis plusieurs appareils, tout en conservant une copie des messages sur le serveur. Cela signifie que les utilisateurs peuvent lire, envoyer et supprimer des messages depuis n'importe quel appareil connecté à Internet, sans perdre les messages sur le serveur.

La configuration IMAP dans Thunderbird permet aux utilisateurs de configurer un compte de courrier électronique pour utiliser le protocole IMAP. Cela nécessite des informations telles que l'adresse du serveur IMAP, le nom d'utilisateur et le mot de passe pour se connecter au compte, et les paramètres de sécurité (comme SSL ou TLS) si nécessaire. Une fois configuré, Thunderbird peut se connecter au serveur IMAP et synchroniser les messages, les dossiers, les contacts, etc. avec ceux sur le serveur.

Dans Thunderbird, la configuration SMTP permet de configurer un compte de courrier électronique pour utiliser le protocole SMTP pour l'envoi de courriels. Cela nécessite des informations telles que l'adresse du serveur SMTP, le nom d'utilisateur et le mot de passe pour se connecter au compte, et les paramètres de sécurité (comme SSL ou TLS) si nécessaire. Une fois configuré, Thunderbird peut se connecter au serveur SMTP et envoyer des courriels en utilisant ce compte de courrier électronique. Il faut donc valider son adresse mail.

Une fois le compte validé il est ensuite créé :



## 2) Génération de clé

Ensuite il faut générer une paire de clé grâce à l'outil « Gestionnaire de clés OpenPGP »

Ajouter une clé OpenPGP personnelle pour adrien.pago@ufa47.org

### Génération d'une clé OpenPGP

**Identité** Adrien Pago <adrien.pago@ufa47.org> - adrien.pago@ufa47.org

**Expiration de la clé**  
Définissez la date d'expiration de la clé que vous venez de générer. Vous pourrez par la suite modifier cette date pour prolonger le délai d'expiration si nécessaire.

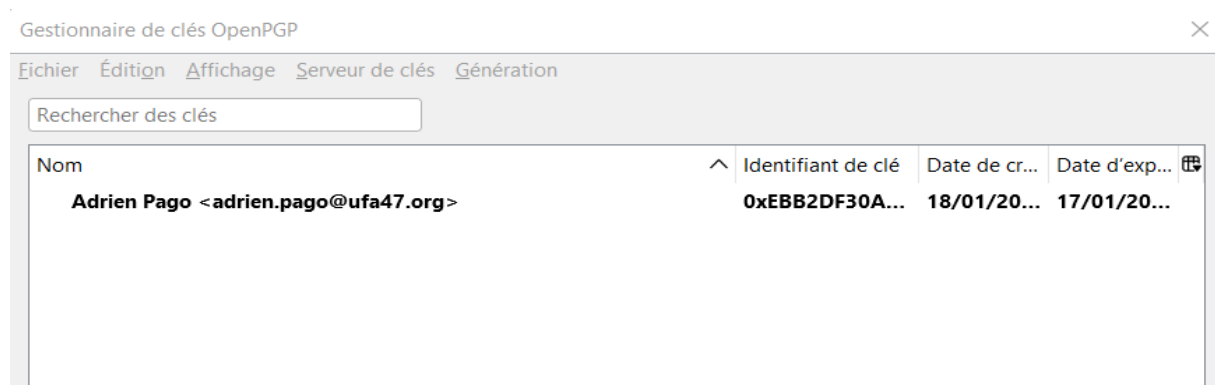
☒ La clé expire dans 3 ans  
☐ La clé n'expire jamais

**Paramètres avancés**  
Contrôlez les paramètres avancés de votre clé OpenPGP.

Type de clé : RSA  
Taille de la clé : 3072

Générer la clé Annuler Retour

Si tout s'est bien passé, votre paire de clé devrait apparaître dans le « Gestionnaire de clés OpenPGP » comme ceci :



### 3) Partage de clé

Assurez-vous que le fichier contienne seulement votre clé publique et naviguez sur <https://keys.openpgp.org/upload> et téléversez votre clé. Afin que d'autres personnes puissent retrouver votre clé publique, cliquez sur « Envoyer un courriel de confirmation » puis effectuez la validation une fois le mail reçu :

**keys.openpgp.org**

Téléverser votre clé

Adrien Pago adrien.pag...0A82758B3)-public.asc

Besoin de plus de précisions ? Consultez notre [présentation](#) et notre [guide d'utilisation](#).

**keys.openpgp.org**

Vous avez téléversé la clé **03430A66E4564847BD68650BEBB2DF30A82758B3**.

Cette clé est maintenant publiée avec seulement des renseignements qui ne permettent pas de vous identifier.  
(Qu'est-ce que cela signifie ?)

Afin qu'une recherche par adresse courriel trouve cette clé, vous pouvez confirmer qu'elle vous appartient :

**adrien.pago@ufa47.org**

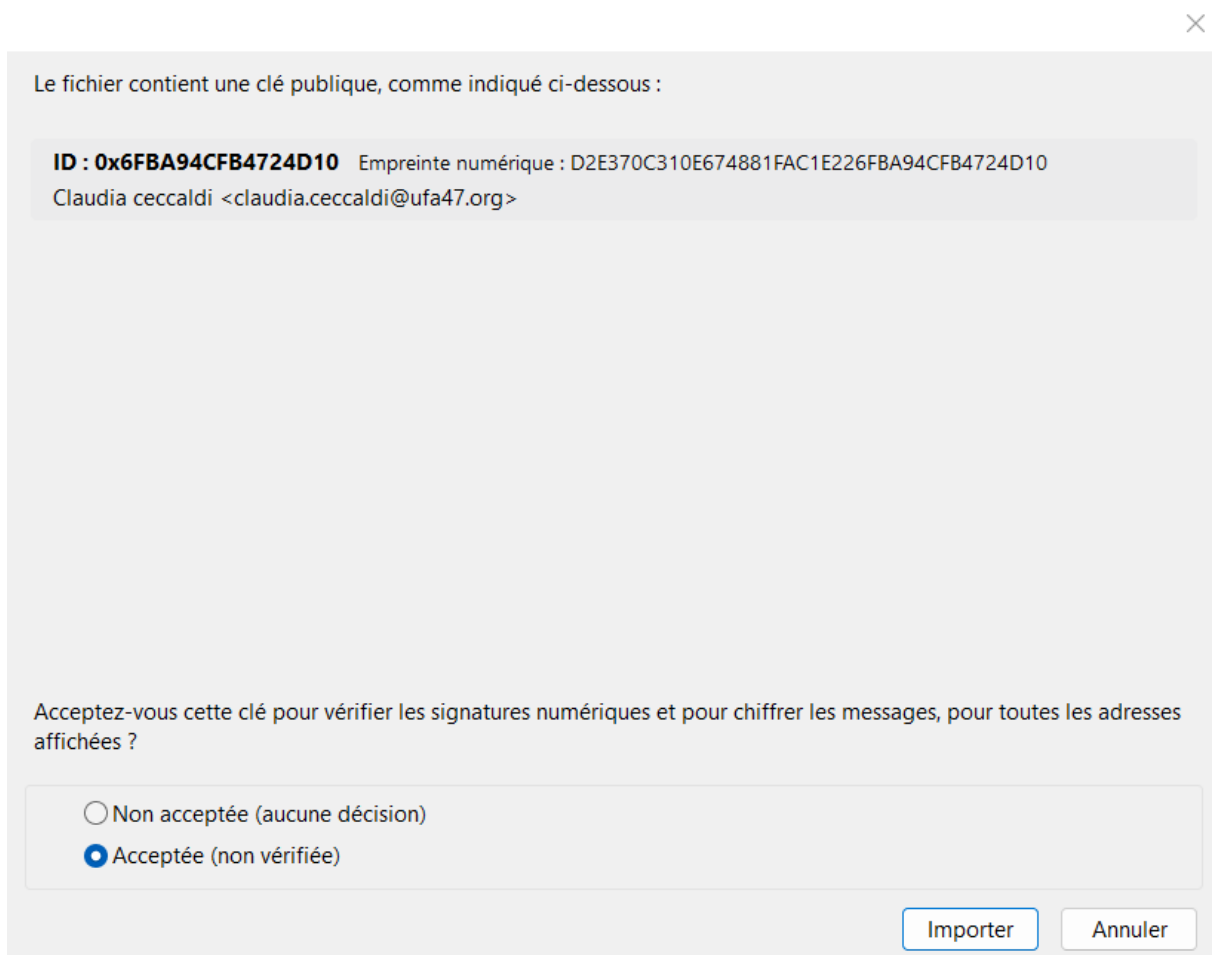
**Note :** Certains fournisseurs retardent les courriels jusqu'à 15 minutes afin de prévenir les courriels indésirables (pourriels). Veuillez faire preuve de patience.

Voici le mail de confirmation :



Afin de valider que tout fonctionne parfaitement, demandez à un de vos collègues de récupérer votre clé via le « Gestionnaire de clés OpenPGP » puis le menu « Serveur de clés » et le choix « Rechercher des clés en ligne », il devra ensuite rentrer votre adresse email.

J'ai ensuite rentrer toutes les adresses mail de mes collègues.



Si une clé a été trouvée, il faudra choisir l'option « Acceptée (non vérifiée) » comme si-dessus



Une fois la clé importée, elle doit apparaître dans votre liste de clés dans le « Gestionnaire de clés OpenPGP ». Faites un clic droit dessus puis sélectionnez « Propriétés de la clé » et validez l'empreinte de la clé.

Réalisez l'opération pour chacun de vos collègues.

Propriétés de la clé

Propriétaire de clé revendiqué

Thomas Reverdel <thomas.reverdel@ufa47.org>

Type

clé publique

Identifiant de clé

0x3D282F3D7CBD19B6

Empreinte

8427 2A8D 6307 3F84 092A 2ED1 3D28 2F3D 7CBD 19B6

Date de création

18/01/2023

Date d'expiration

17/01/2026

Actualiser en ligne

Votre acceptation

Certifications

Structure

Acceptez-vous cette clé pour vérifier les signatures numériques et pour chiffrer les messages ?

☐ Non, rejeter cette clé.

☐ Pas encore, peut-être plus tard.

☐ Oui, mais je n'ai pas vérifié qu'il s'agit de la bonne clé.

☒ Oui, j'ai vérifié en personne que l'empreinte de cette clé est correcte.

Vérifiez l'empreinte numérique de la clé à l'aide d'un canal de communication sécurisé autre que le courrier électronique pour vous assurer qu'il s'agit bien de la clé de thomas.reverdel@ufa47.org.

OK

Annuler

Réalisez l'opération pour chacun de vos collègues :

Voici maintenant mon gestionnaire de clés avec toutes les empreintes validées.

Gestionnaire de clés OpenPGP

Fichier

Édition

Affichage

Serveur de clés

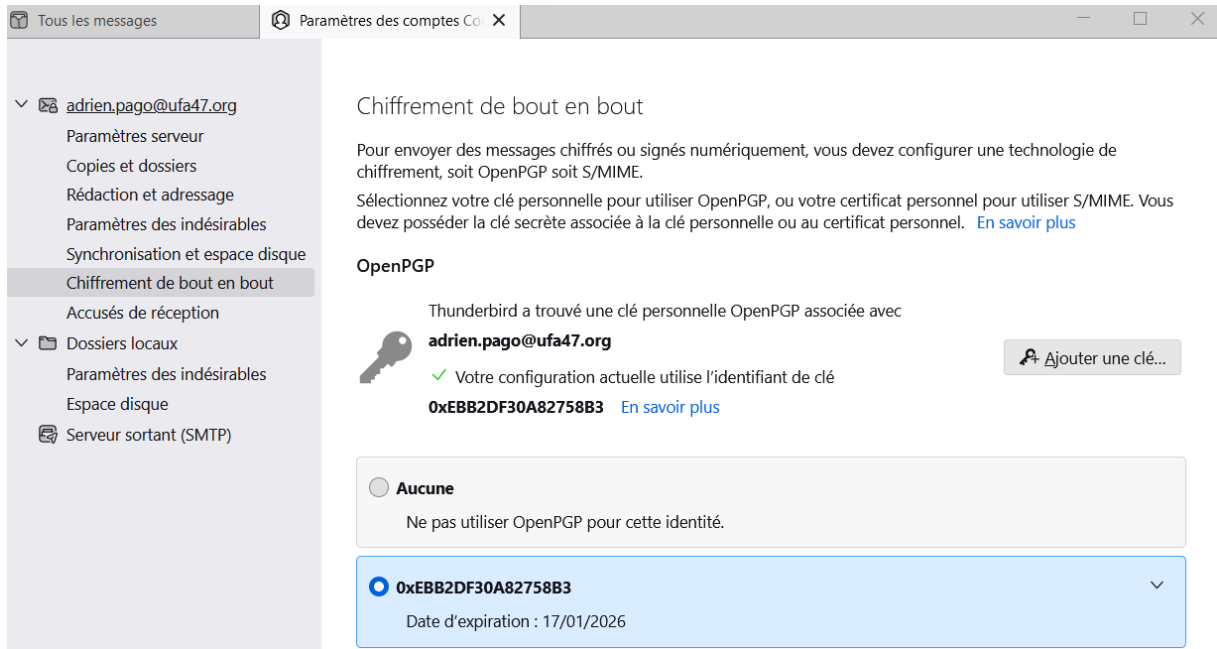
Génération

Rechercher des clés

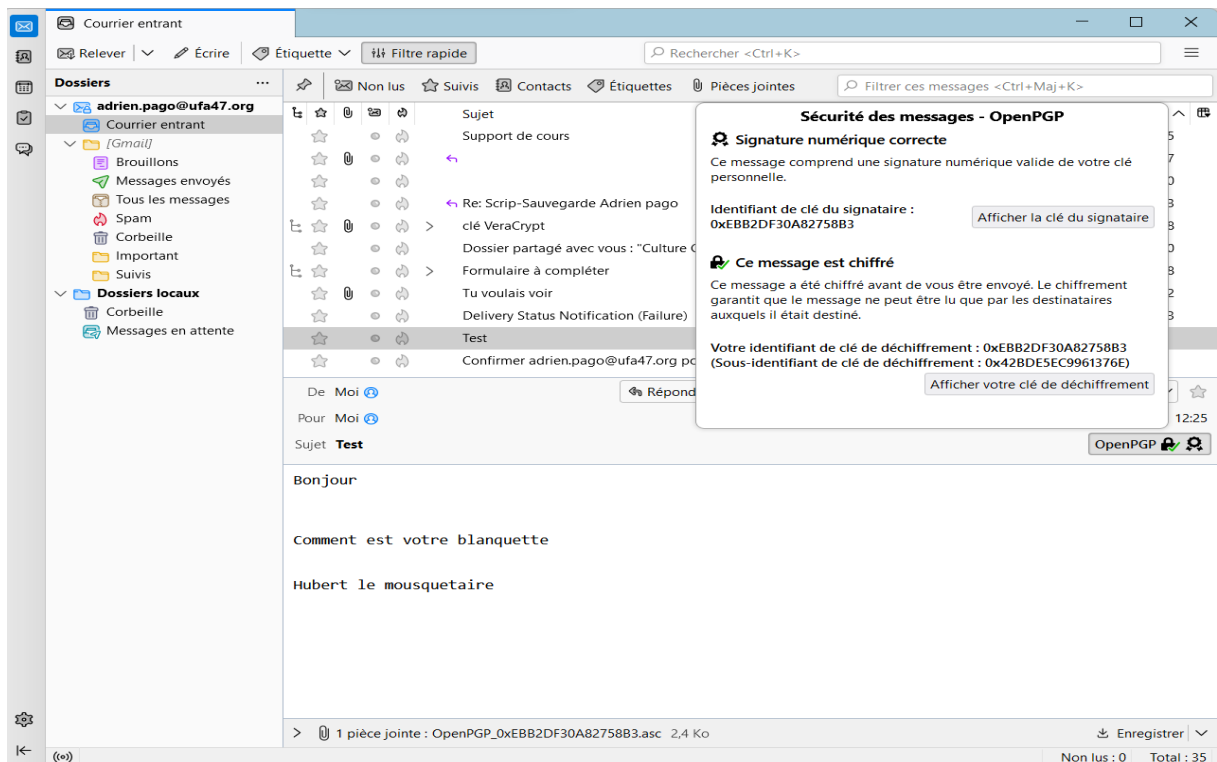
Nom	Identifiant de clé	Date de cr...	Date d'exp...
Thomas Reverdel <thomas.reverdel@ufa47.org>	0x3D282F3D7CB...	18/01/2023	17/01/2026
Louis Mallet <louis.mallet@ufa47.org>	0x1721F131590C...	18/01/2023	17/01/2026
Gabriel Pellizzari <gabriel.pellizzari@ufa47.org>	0x0687844A2DC...	18/01/2023	17/01/2026
Claudia ceccaldi <claudia.ceccaldi@ufa47.org>	0x6FBA94CFB47...	18/01/2023	17/01/2026
Bergamo Louis <louis.bergamo@ufa47.org>	0x201EF483D9F5...	18/01/2023	17/01/2026
Adrien Pago <adrien.pago@ufa47.org>	0xEBB2DF30A...	18/01/20...	17/01/20...

## 4) Signature et chiffrement

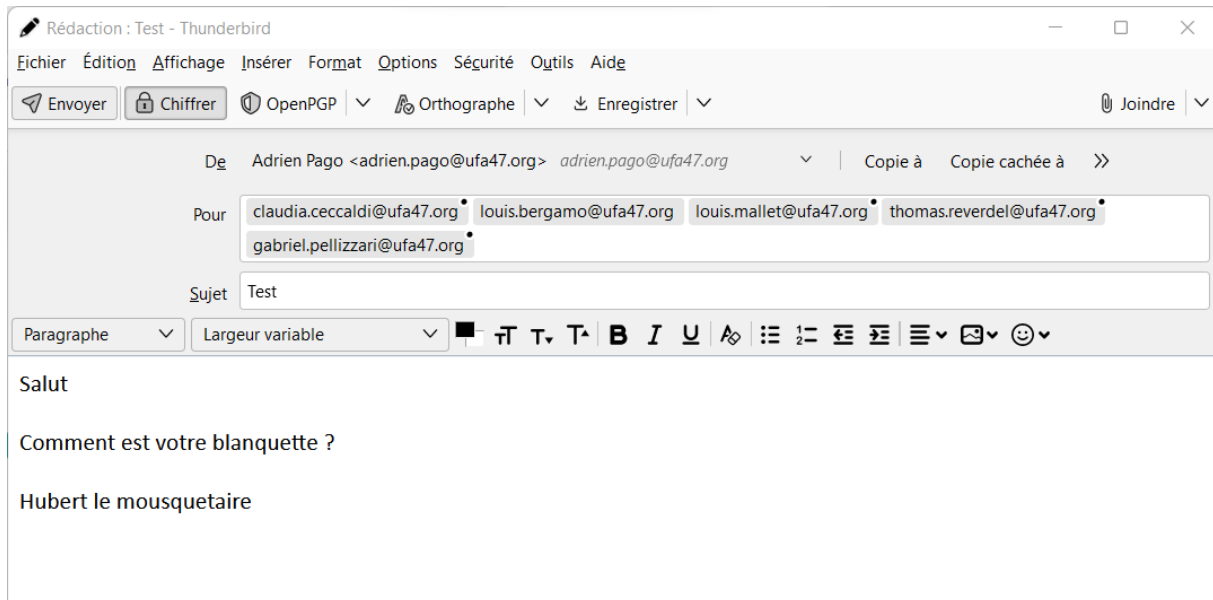
Allez dans le menu déroulant puis choisissez « Paramètres des comptes », puis sélectionnez ensuite l'onglet « Chiffrement de bout en bout » et choisissez votre clé précédemment générée pour activer OpenPGP.



Afin de valider le bon fonctionnement, rédigez un mail avec vous en seul destinataire. Cliquez sur le bouton « Sécurité » et sélectionnez le chiffrement et la signature :



On constate bien la sécurité de celui-ci via le bouton OpenPGP !  
J'ai ensuite envoyer un autre mail chiffré et avec une signature électronique à tous mes collègues pour m'assurer que tout est bien régler.



**Conclusion** : Avec mes collègues pour les quelles nous nous sommes certifiés et partager nos clés. Nous pouvons désormais nous envoyer des mails par **Thunderbird** qui assurent l'intégrité et la confidentialité du contenu et l'authenticité du destinataire.