

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

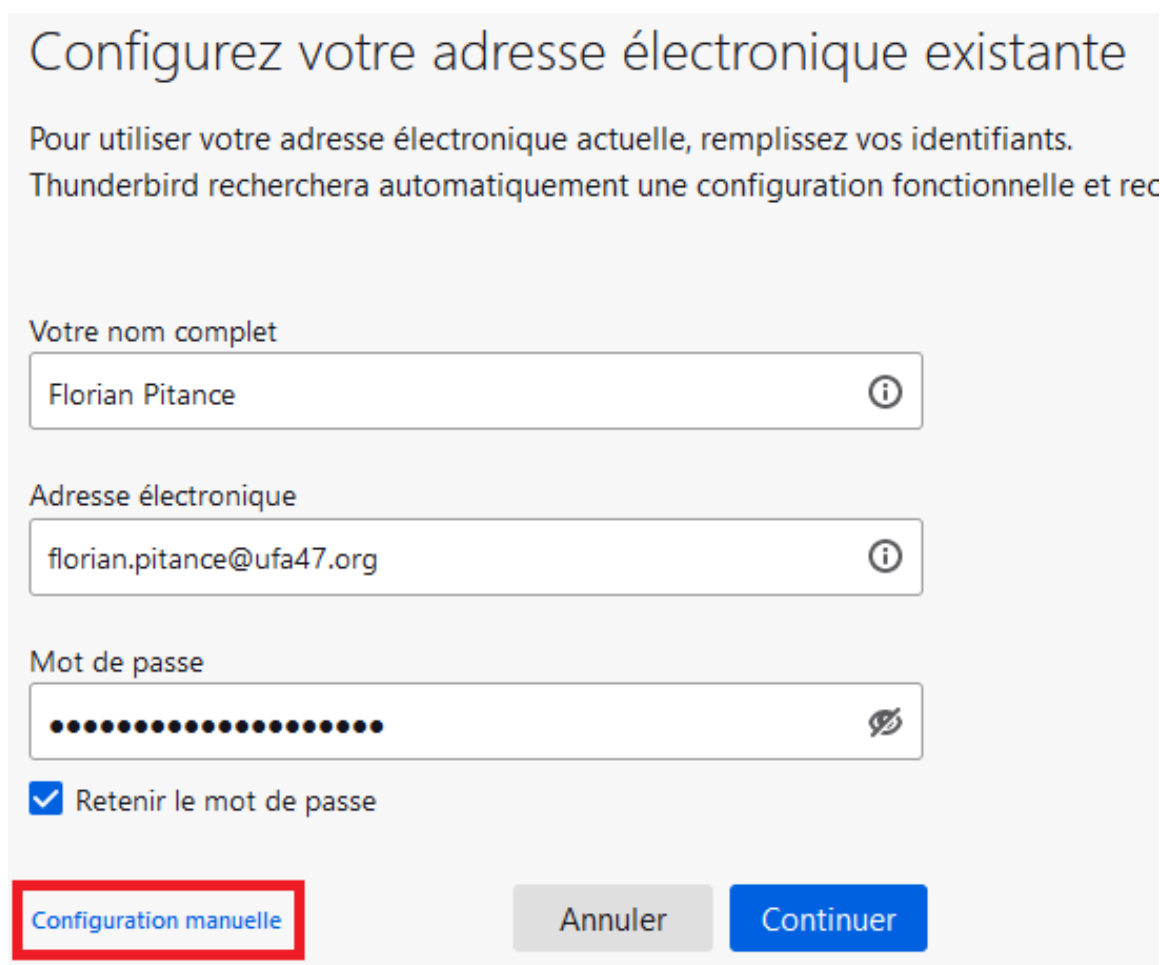
Afin d'assurer les contraintes de la preuve numérique lors de la signature d'un contrat, vous souhaitez proposer à Mme. Schmitt une solution possible. La signature des contrats se fera toujours par email mais avec une surcouche permettant d'assurer l'intégrité, l'authenticité et la confidentialité des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

Installation et configuration

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

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

Une fois Thunderbird installé, commencez à compléter les informations de votre compte @ufa47.org et cliquez sur « configuration manuelle » :



Configurez votre adresse électronique existante

Pour utiliser votre adresse électronique actuelle, remplissez vos identifiants.
Thunderbird recherchera automatiquement une configuration fonctionnelle et rec

Votre nom complet

Florian Pitance

Adresse électronique

florian.pitance@ufa47.org

Mot de passe

Retenir le mot de passe

Configuration manuelle

Annuler

Continuer

Complétez la configuration avec les paramètres de connexion IMAP et SMTP pour Google Workplace :

Paramètres du serveur

SERVEUR ENTRANT

Protocole : IMAP

Nom d'hôte : imap.gmail.com

Port : 993

Sécurité de la connexion : SSL/TLS

Méthode d'authentification : OAuth2

Nom d'utilisateur : florian.pitance@ufa47.org

SERVEUR SORTANT

Nom d'hôte : smtp.gmail.com

Port : 465

Sécurité de la connexion : SSL/TLS

Méthode d'authentification : OAuth2




Nom d'utilisateur : florian.pitance@ufa47.org

Cliquez sur « Retester » afin de vérifier si les paramètres sont bons. Si c'est le cas, cliquez sur « Terminé ». Il faudra ensuite vous connecter sur une fenêtre de connexion et autoriser Thunderbird à accéder à vos mails :

Mozilla Thunderbird Email souhaite accéder à votre compte Google

 florian.pitance@ufa47.org

Mozilla Thunderbird Email pourra ainsi :

-  Lire, rédiger, envoyer et supprimer définitivement des e-mails dans Gmail
-  Afficher, modifier, télécharger et supprimer définitivement vos contacts
-  Afficher, modifier, partager et supprimer définitivement tous les agendas auxquels vous pouvez accéder dans Google Agenda

En cliquant sur "Autoriser", vous autorisez cette application et Google à utiliser vos données conformément à leurs [Règles de confidentialité](#) respectives. Vous pouvez à tout moment modifier ces paramètres, ainsi que d'autres [autorisations associées à votre compte](#).

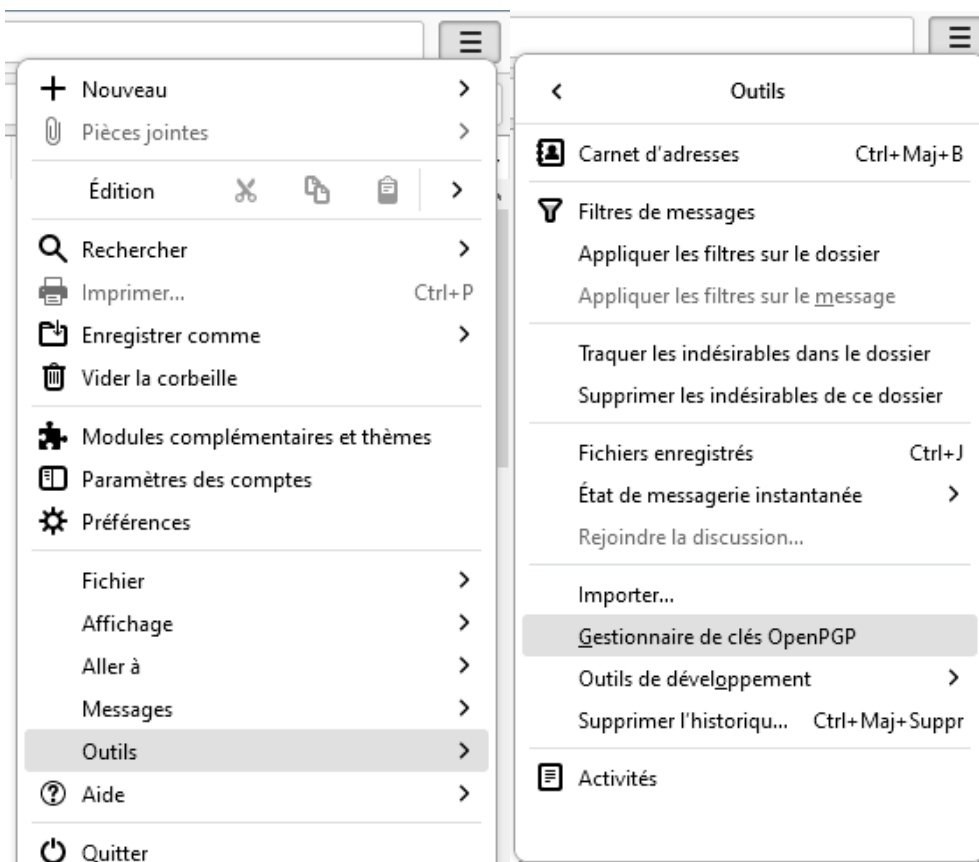
Refuser

Autoriser

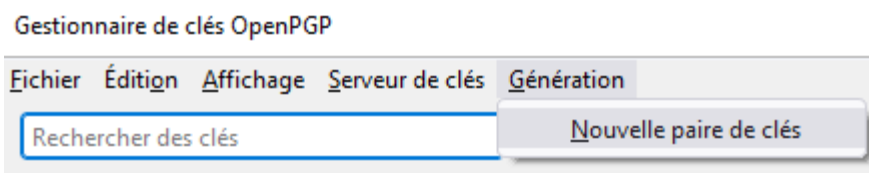
Testez le bon fonctionnement en envoyant un mail à un de vos collègues et inversement.

Génération de clé

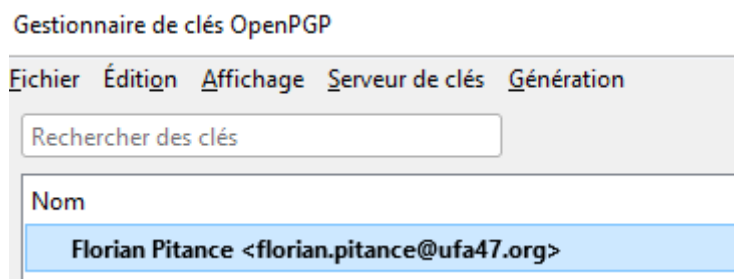
Cliquez sur le menu déroulant puis sélectionnez « Outils » puis « Gestionnaire de clés OpenPGP » :



Générez une nouvelle clé via le menu « Génération » puis le choix « Nouvelle paire de clés » (gardez les paramètres par défaut pour les besoins du TP) :

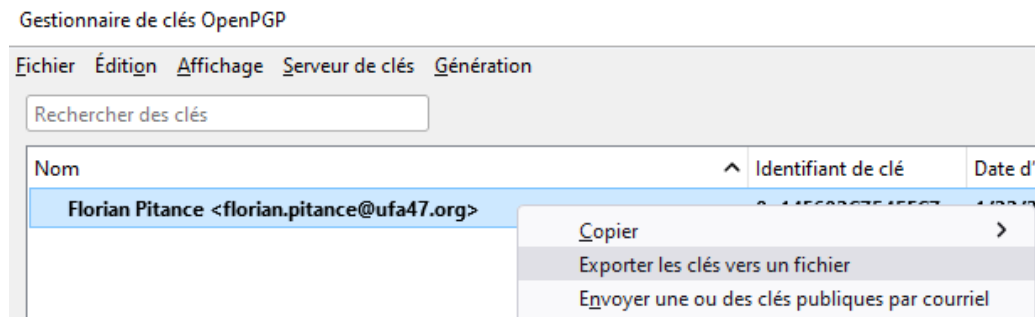


Si tout s'est bien passé votre paire de clé devrait apparaître dans le « Gestionnaire de clés OpenPGP » :



Partage de clé

Via le « Gestionnaire de clés OpenPGP », faites un clic droit sur votre clé puis choisissez « Exporter les clés vers un fichier » :



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

Vous avez téléversé la clé **810C88EDB6794B525C99F45914E602C7545EC77B**.

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

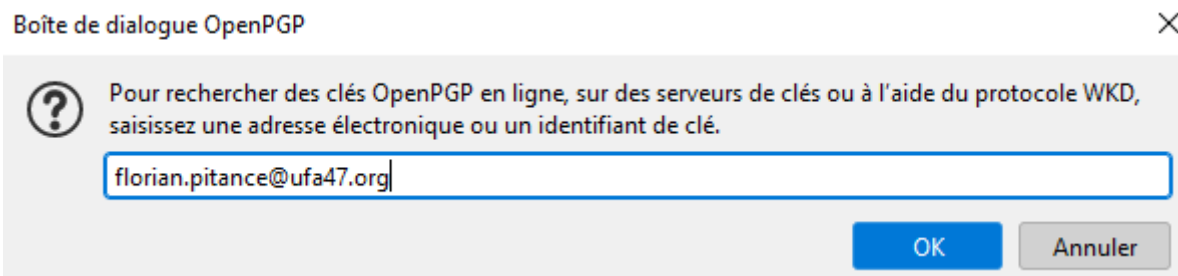
Afin qu'une recherche par adresse courriel trouve cette clé, vous pouvez confirmer qu'elle vous appartient :

florian.pitance@ufa47.org

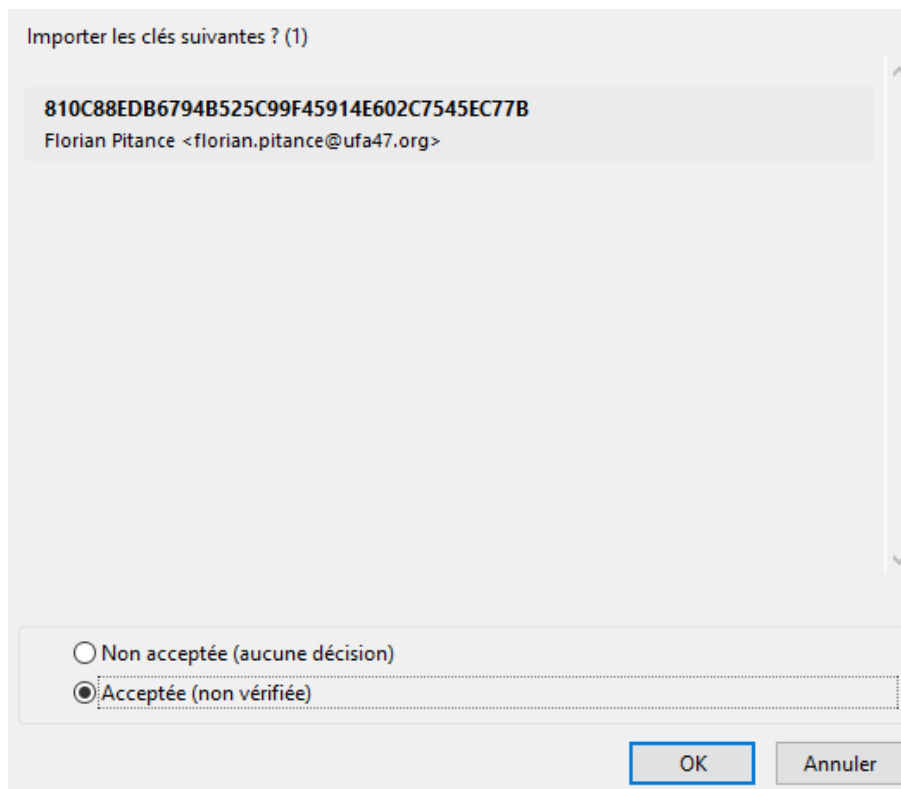
[Envoyer un courriel de confirmation](#)

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

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 :



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



Importer les clés suivantes ? (1)

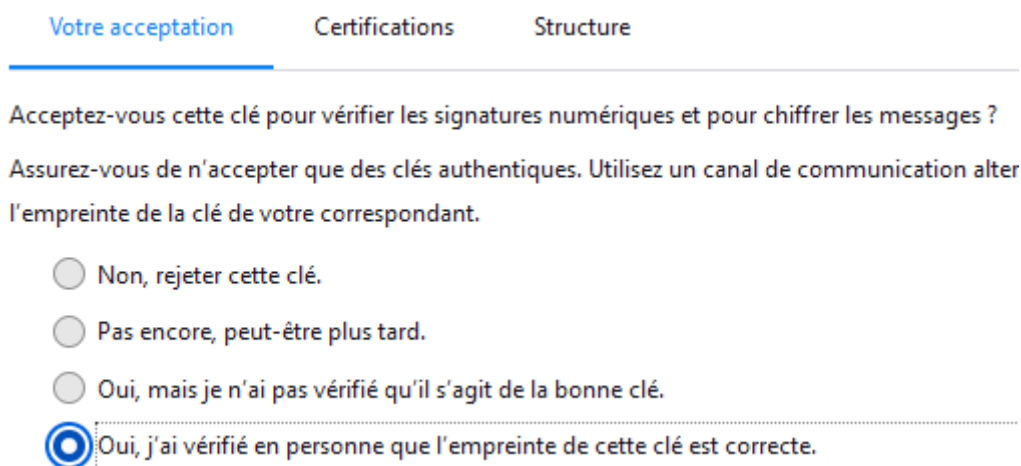
810C88EDB6794B525C99F45914E602C7545EC77B
Florian Pitance <florian.pitance@ufa47.org>

☐ Non acceptée (aucune décision)

☒ Acceptée (non vérifiée)

OK Annuler

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 :



Votre acceptation Certifications Structure

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

Assurez-vous de n'accepter que des clés authentiques. Utilisez un canal de communication alter l'empreinte de la clé de votre correspondant.

☐ Non, rejeter cette clé.

☐ Pas encore, peut-être plus tard.

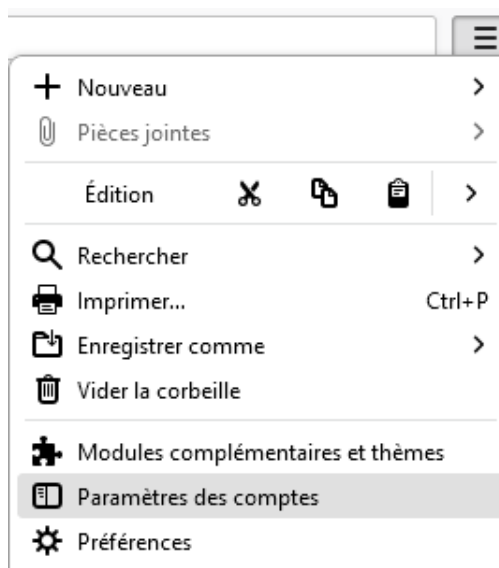
☐ Oui, mais je n'ai pas vérifié qu'il s'agit de la bonne clé.

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

Réalisez l'opération pour chacun de vos collègues.

Signature et chiffrement

Allez dans le menu déroulant puis choisissez « Paramètres des comptes » :



Sélectionnez ensuite l'onglet « Chiffrement de bout en bout » et choisissez votre clé précédemment générée pour activer OpenPGP :

OpenPGP

Thunderbird a trouvé une clé personnelle OpenPGP associée avec



florian.pitance@ufa47.org

✓ Votre configuration actuelle utilise l'identifiant de clé

0x14E602C7545EC77B [En savoir plus](#)

[Ajouter une clé...](#)

☐ Aucune

Ne pas utiliser OpenPGP pour cette identité.

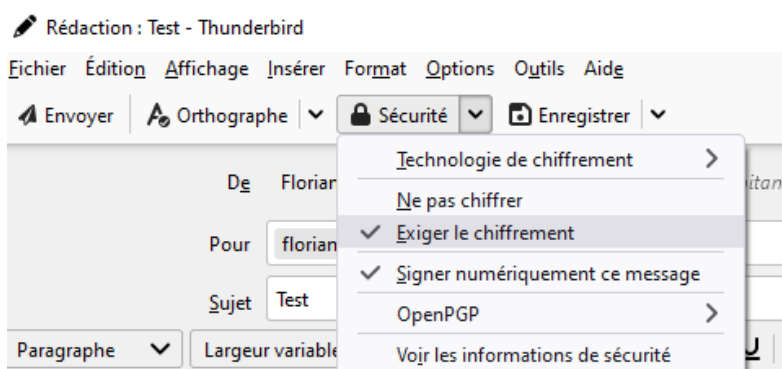


0x14E602C7545EC77B

Date d'expiration : 1/22/2025

(tournez la page svp ...)

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 :



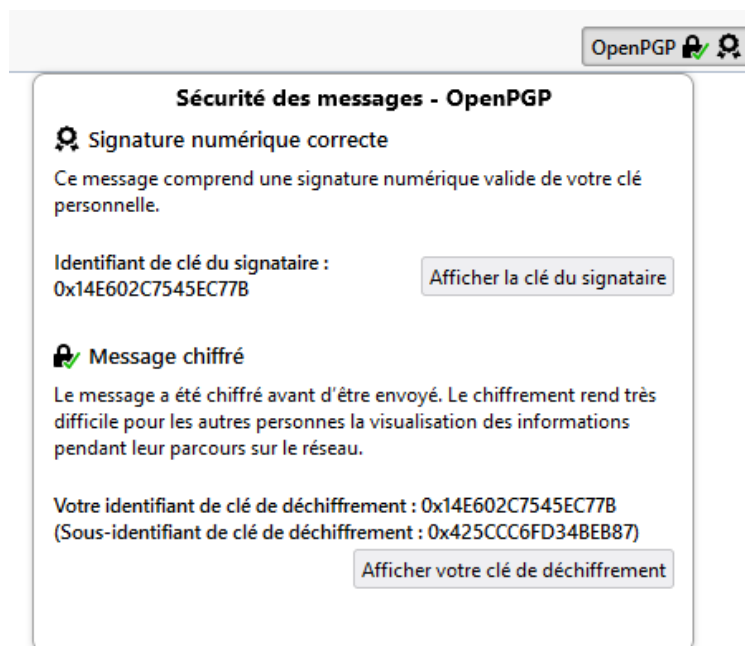
Bonjour,

Comment est votre blanquette ?

Cordialement,

Hubert Bonisseur de La Bath

Une fois le mail reçu vérifiez la sécurité de celui-ci via le bouton OpenPGP :



Refaire l'opération en envoyant un mail à chacun de vos collègues.