Bloc 3 Thème2 : Configurer une messagerie sécurisée avec Mozilla ThunderBird

Présentation

Vous travaillez dans le contexte **M@Banque**. Vous devez configurer le logiciel de messagerie Mozilla **Thunderbird** pour vous permettre d'échanger des messages sécurisés en utilisant le **format cryptographique OpenPGP** ebntre la banqeu et ses clients. OpenPGP permet le **chiffrement** et **l'authentification** du courrier électronique.

Le nom OpenPGP fait référence à l'application de cryptographie historique **PGP** (Pretty Good Privacy).

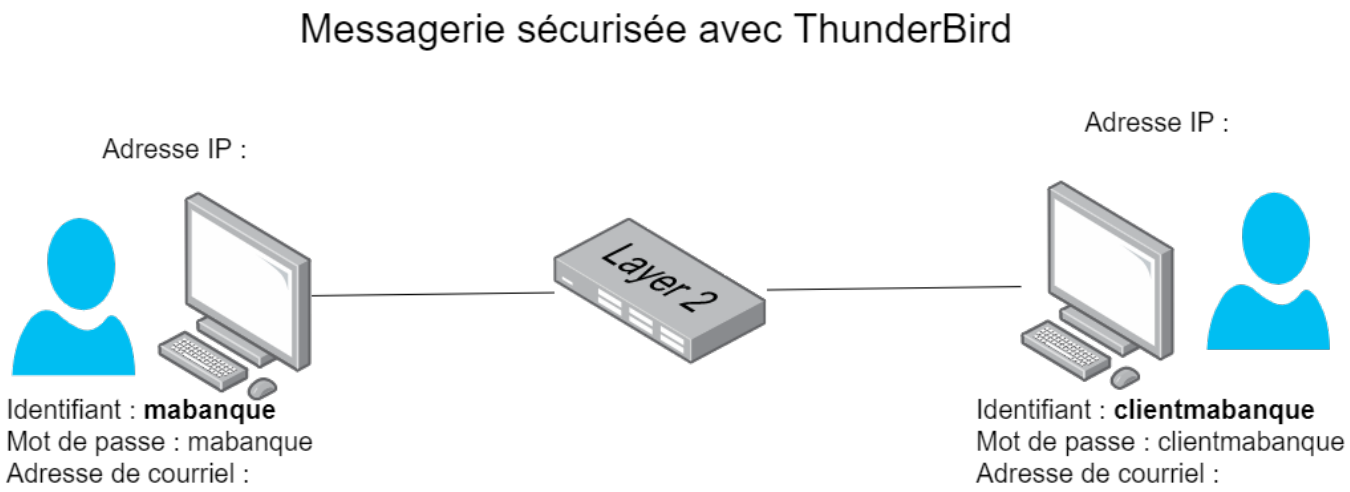
Pour en savoir plus :

- https://fr.wikipedia.org/wiki/Pretty_Good_Privacy
- https://fr.wikipedia.org/wiki/OpenPGP

Infrastructure réseau à mettre en place

Pour mettre cette solution d'échange sécurisé de courriel, vous allez utiliser la **VM** du Lab précédent afin de d'**installer et configurer les logiciels** nécessaires sans avoir besoin de modifier la configuration de votre propre ordinateur.

Voici le schéma du réseau à **mettre en place** :



Vous aurez à **travailler en binôme** afin d'assumer soit le **rôle de la banque** soit le **rôle du client** en ne **configurant qu'une seule VM** du schéma. Pour cela vous devez :

- **créer** le compte utilisateur dans votre VM ;
- **utiliser** votre adresse de messagerie ou bien en créer une pour cette activité.

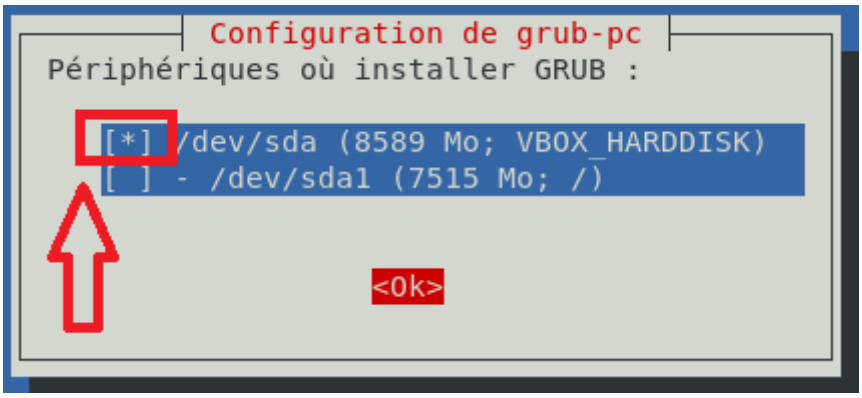
lancement et mise à jour de la VM

- Lancez VirtualBox et créez un **snapshot** de votre VM **Ch2Lab1** sous le nom **Ch3Lab3** ;
- Ouvrez une session avec le compte **centrecallbd**. Ce compte doit avoir la possibilité d'obtenir une élévation de privilèges.
- Ouvrez une **session Terminal** (dossier Utilitaires) et lancez la mise à jour de l'OS avec les commandes suivantes :

```
$ sudo apt update
$ sudo apt upgrade
```

Au message sur la configuration de **grub-pc** :

- validez **OK** (Touche TAB pour sélectionner le bouton) ;
- **sélectionnez** le premier choix avec la barre Espace. ATTENTION une **étoile** doit être affichée, puis validez



Création du compte utilisateur banque ou client

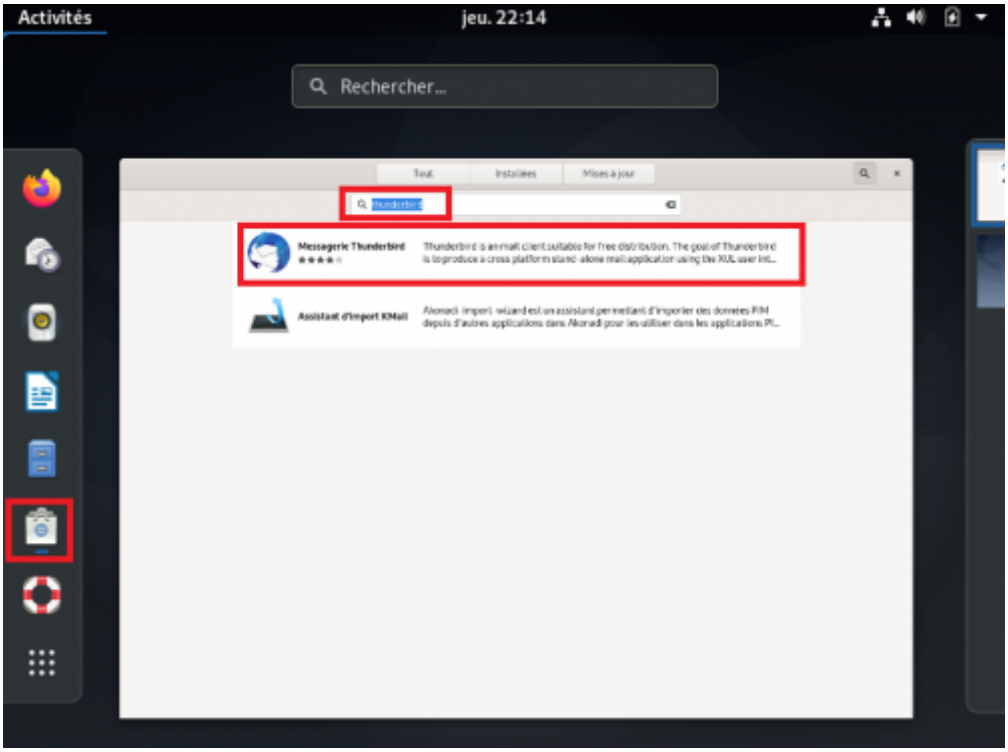
Vous devez **créer** le compte mabanque ou clientmabanque selon le rôle que vous avez à gérer.

- ouvrez une session Terminal et utilisez la commande suivante pour créer un compte avec son mot de passe :

```
$ sudo adduser mabanque
```

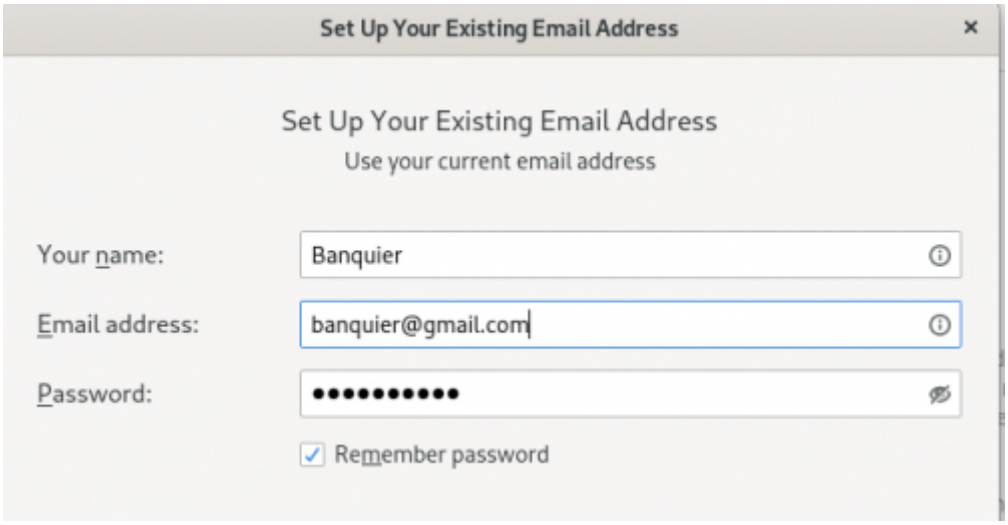
Installation et configuration de Mozilla Thunderbird

- **Lancez** le programme **Logiciels** et faite une recherche avec le mot clé **thunderbird** ;
- **Sélectionnez** le logiciel **Messagerie Thunderbird** puis lancer son installation ;
- Authentifiez-vous avec le mot de passe de **centercallbd**;

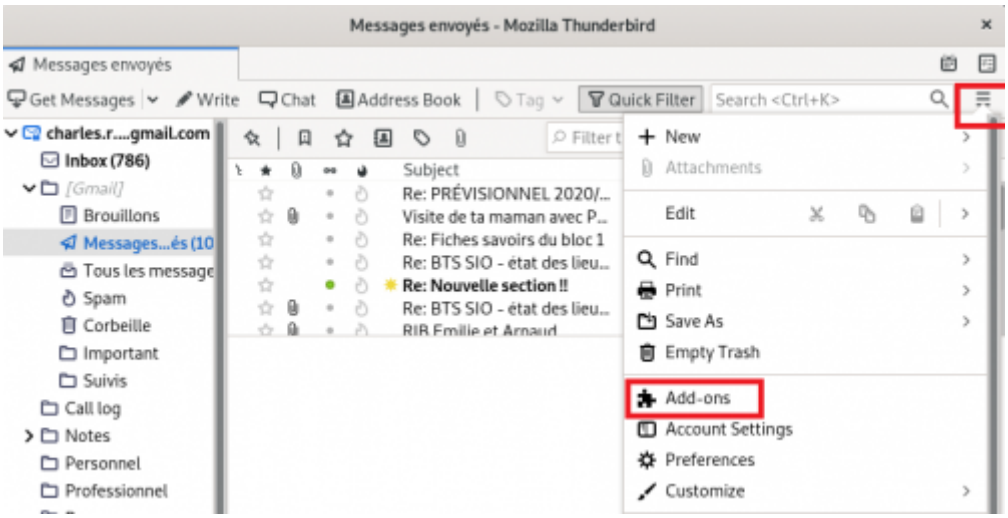


- utilisez le lien suivant pour configurer Thunderbird avec votre compte de messagerie ou un nouveau compte :

https://support.mozilla.org/fr/kb/configuration-automatique-de-compte



- Téléchargez et installez le module complémentaire **Français Language Pack** pour avoir l'interface en français (utilisez le mot clé français):



- redémarrez Thunderbird.

Testez l'envoi d'un message en clair (pas de chiffrement)

- Envoyez un message à votre binôme pour vérifier le bon fonctionnement de votre messagerie.

Configuration de l'envoi de courriel chiffrés

Lien :

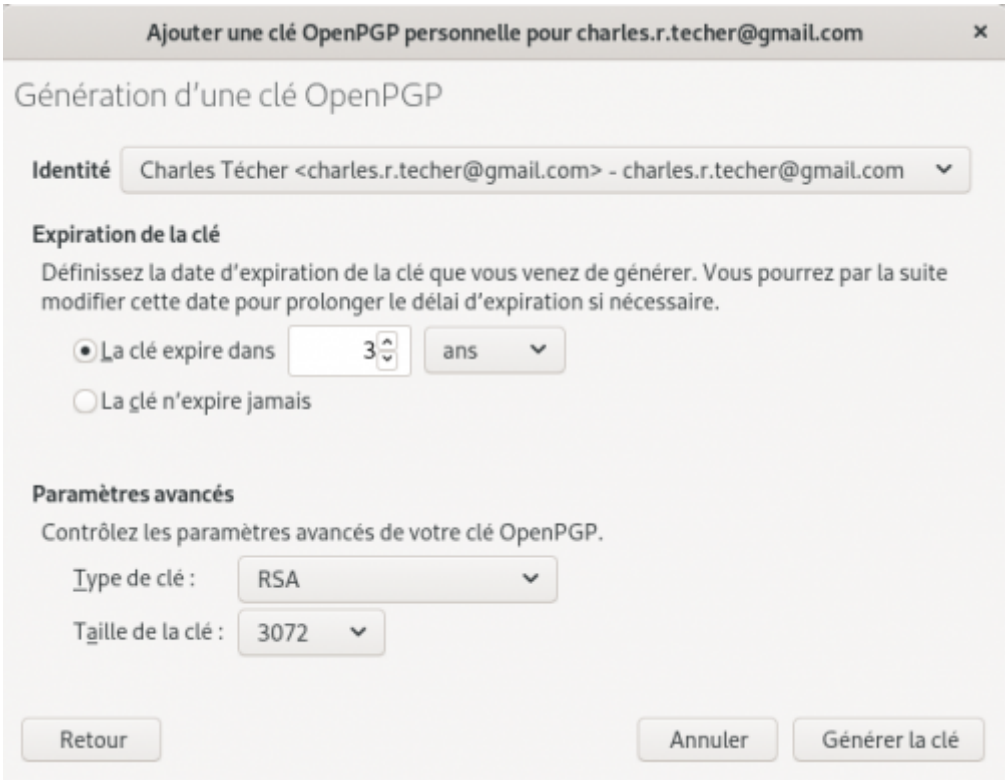
- https://support.mozilla.org/fr/kb/signature-numerique-et-chiffrement-des-messages
- https://support.mozilla.org/fr/kb/presentation-chiffrement-bout-en-bout-thunderbird

Principe de fonctionnement : Pour chiffrer les messages vous allez utiliser le **système cryptographique à clé publique** :

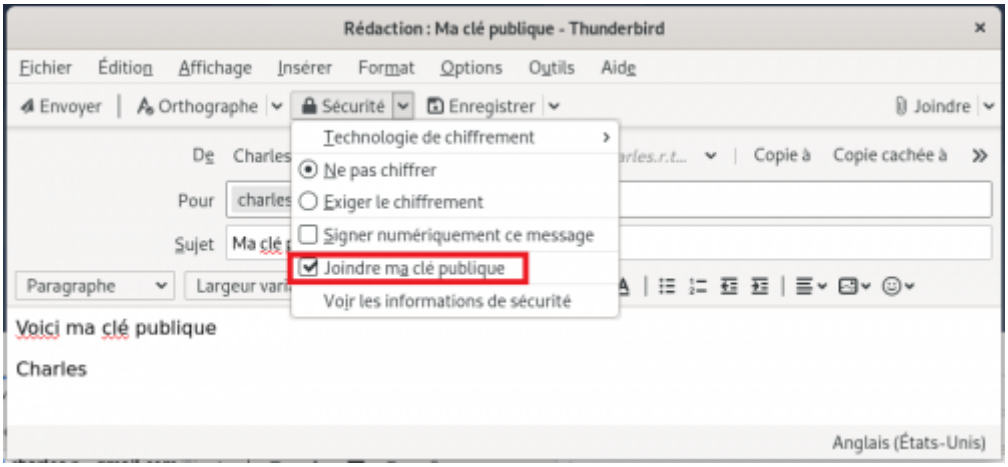
- chaque participant dispose de deux clés distinctes : une **clé de chiffrement publique** et une **clé de déchiffrement privée** ;
- Quand quelqu'un veut vous **envoyer** un **message électronique chiffré**, il utilise **votre clef publique** pour générer l'algorithme de chiffrement ;
- Lorsque vous **recevez** ce message, vous devez utiliser votre **clef privée pour le déchiffrer**.

IMPORTANT : il ne faut **jamais partager sa clef privée** avec quiconque.

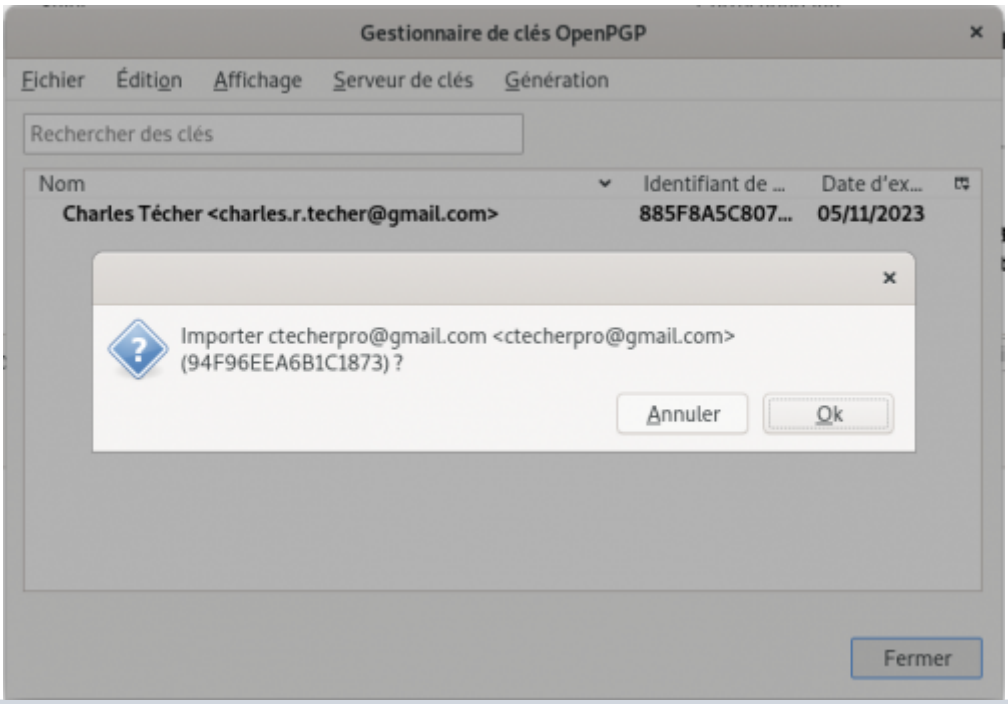
- Créez les clefs privée et publique PGP avec le **Gestionnaire de clés OpenPGP** qui se trouve dans le menu outils :
  - Utilisez le menu Génération pour générer une nouvelle paire de clés ;
  - laissez les valeurs par défaut et cliquez sur **Générez la clé** : une clé publique et une clé secrète vont être générées.
  - puis fermez le **Gestionnaire de clés OpenPGP**.



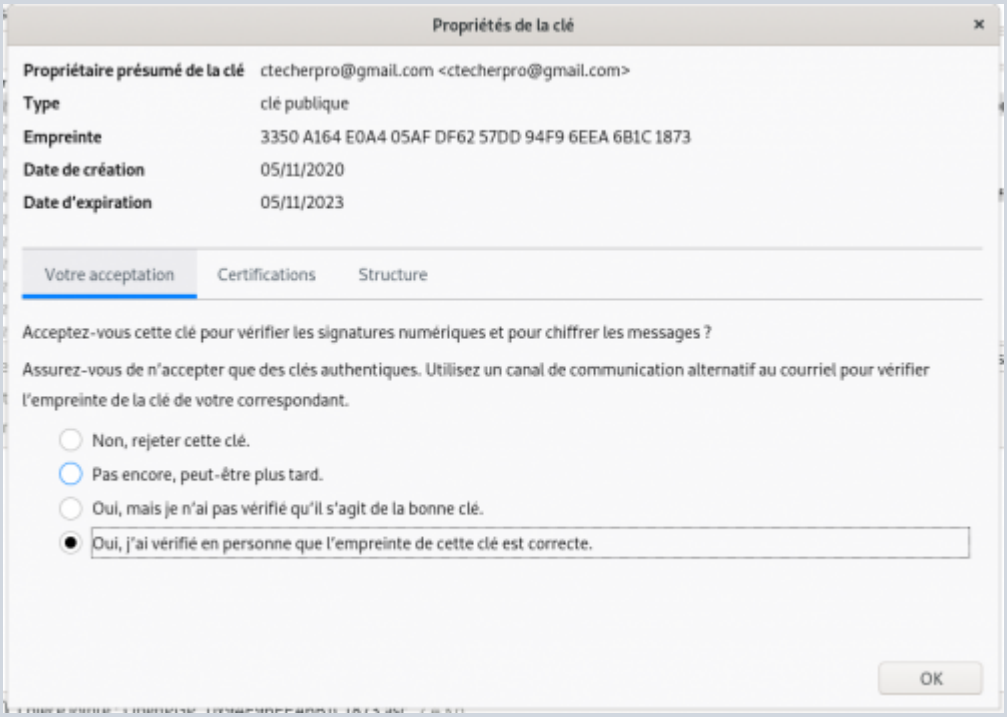
- dans le **Gestionnaire de clés OpenPGP**, cliquez sur le bouton **Gérer les clés du destinataire sélectionné…**.
- **Envoyez** dans un message **votre clé publique** à votre correspondant. Il en aura besoin pour chiffrer les messages qui vous sont destinés :



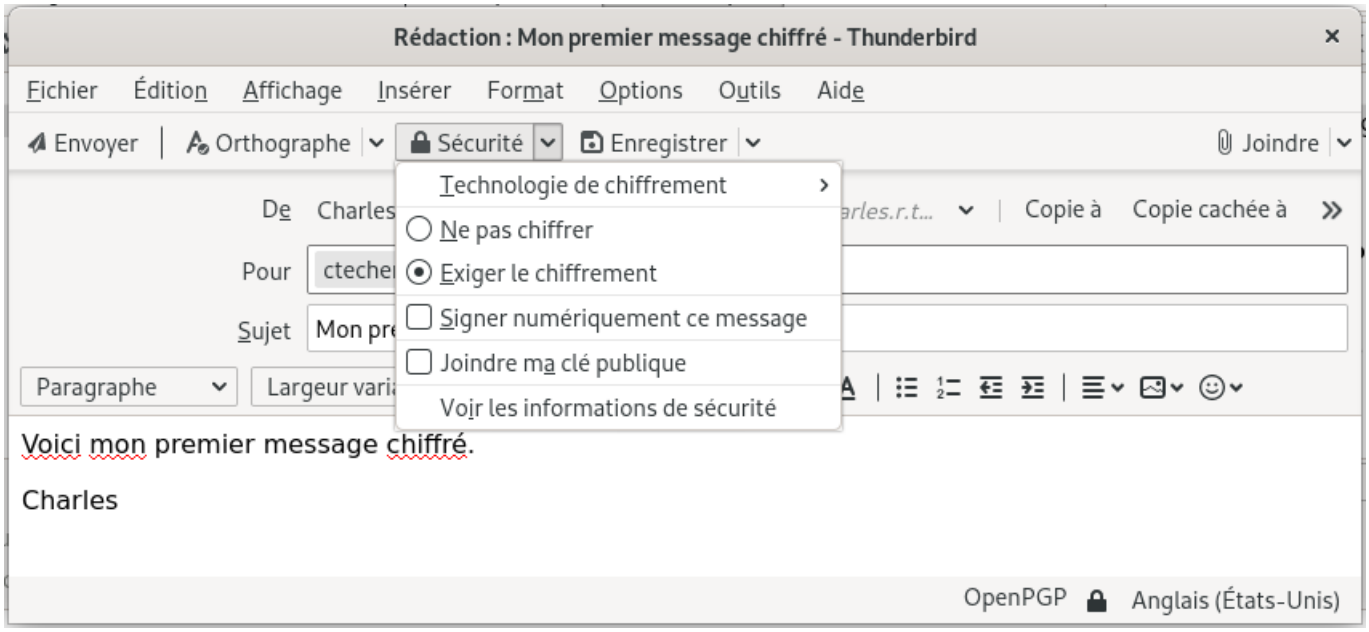
- **Attendez** de recevoir un message de votre correspondant **contenant sa clé publiqu**e. Vous en aurez besoin pour chiffrer les messages que vous souhaitez lui envoyer.
- A la **réception du message** de votre correspondant, enregistrez la piève attachée, le fichier avec l'extension **.asc** qui contient la clé publique.
- depuis **Gestionnaire de clés OpenPGP**, importez cette clé publique :



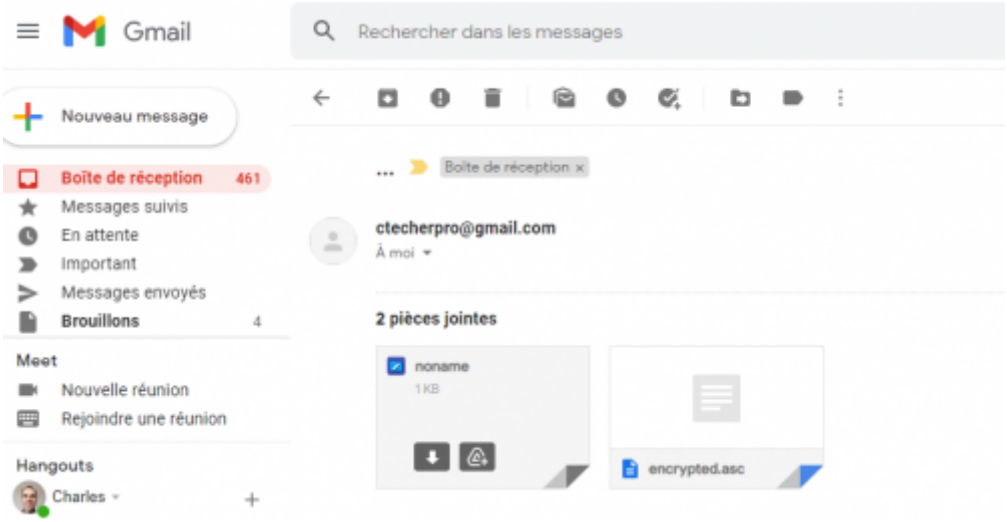
Important : après avoir importer la clé, il faut **accepter** cette clé pour qu'elle puisse servir à **signer et à chiffrer les messages**. Dans le **Gestionnaire de clés OpenPGP** double-cliquez sur la nouvelle clé publique, ce qui montre que vous êtes sur que cette clé publique est bien celle de votre correspondant et accepter là :



- créez et envoyez votre premier message chiffré en choisissant bien l'option **Exiger le chiffrement** :



- Votre message sera lisible dans la messagerie Thunderbird de votre correspondant mais illisible si le logiciel de messagerie ne possède pas la clé privée : ni l'objet ni le contenu du message ne sont interprétable :



Retour Accueil Bloc3

- Bloc3