Thème 2 Chapitre 3 : *Préserver l'identité numérique de l'organisation*

TP 2

Déployer des moyens de preuves sécurisés et conformes à la législation

Bloc 3 - Cybersécurité des services informatiques

EVALUATION DES COMPETENCES VISEES						
Compétence(s) Visée(s)	**Savoir-Faire(s)**	**Niveau d'acquisition**				
		A	B	C	D	E
B3.2 Préserver l'identité numérique de l'organisation	**Déployer les moyens appropriés de preuve électronique**					

Mission

Lors de votre mission précédente, vous avez réalisé une veille sur les technologies qui permettent de chiffrer les contenus de courriels PGP. Votre responsable vous demande maintenant de mettre en œuvre cette technologie dans un environnement prototypé. Les conclusions de vos analyses permettront de renforcer les moyens de preuves sécurisés.

Table des matières

 © Delagrave

© Delagrave

1 - Préparation de l'environnement de test

Voir schéma réseau dans Document 1

Machines virtuelles mises à votre disposition : (chemin DatacenterSIO > 1SIO > 1SIOA > TC3)

- *votrelogin*__T_fedora36_1A_TC3
- *votrelogin*__T_W10_21H2-1Proc_1A_TC3

Dans ce TP, vous allez tester une **solution d'envoi de messages sécurisés et signés**. Vous aurez besoin de 2 adresses de messagerie : celle représentant M@Banque et l'autre représentant le client. Pour effectuer les test d'envoi et de réception, nous utiliserons 2 VM dans lesquelles sera installé le **client de messagerie Thunderbird**. La VM Fedora sera la machine de la **conseillère bancaire Alice PAPIN** et la VM Windows sera la machine du **client Bruno MIKO**.

2 solutions s'offrent à vous : soit vous créez deux adresses de messagerie, soit vous utilisez 2 adresses de courriel vous appartenant à condition qu'elles puissent être intégrées dans Thunderbird.

Dans le cas où vous choisissez de créer 2 adresses email, vous pouvez choisir comme fournisseur GMX-Caramail ou Gmail de Google. Vous êtes libre de choisir vos serveurs de messagerie. Si vous optez pour un autre fournisseur que ceux cités, assurez-vous que le compte choisi puisse être intégré à Thunderbird.

Les dernières versions de Thunderbird (depuis la 78.2.1) supportent nativement les 2 chiffrements standards, **OpenPGP** et **S/MIME**. Par contre, le module complémentaire Enigmail qui les proposait de manière conviviale n'est plus maintenu. Ceci dit, l'utilisation d'OpenPGP est assez intuitive.

Dans ce TP, pour les captures d'écran d'exemples, nous avons utilisé les adresses email suivantes :

- compte de messagerie de la banque : apapin.mabanque@gmx.fr
- compte de messagerie du client de la banque : bmiko.client@gmail.com

Remarque : dans le cas où vous avez créer 2 adresses de messagerie, pensez à les supprimer lorsque le TP sera terminé si vous ne souhaitez les utiliser plus tard.

1.1 - Préparation de la station de travail Fedora36 (Banque)

1.1.1 - Renommage machine

- Renommez votre machine avec le format suivant :
  `fed-PNNNN-TC3.jolsio.net` (ex. pour Bob MORANE : **`fed-BMORA-TC3.jolsio.net`**)

1.1.2 - Vérification paramétrage VLAN et adresse IP de la VM

Figure 1: Adaptateur réseau 1 : SIO-PEDAGO. La VM se trouve bien dans le bon VLAN.

- Vérifiez que la station de travail se trouve bien dans le VLAN SIO-PEGAGO
- Vérifiez la valeur de votre adresse IP (commande **`ip a`**)

  Elle doit être comprise entre 10.15.12.1 et 10.15.15.239

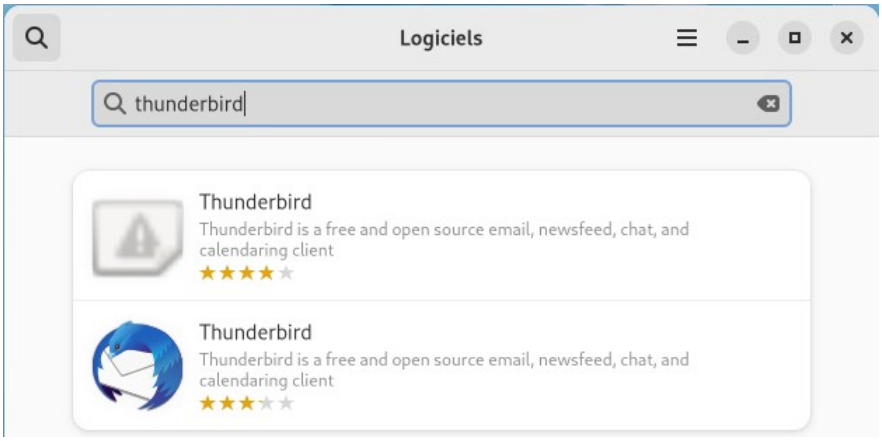
1.1.3 - Création du compte utilisateur Alice PAPIN dans la station Fedora

- Ouvrez un terminal
- Créez le compte utilisateur **Alice PAPIN** et son dossier personnel dans **`/home`**. Voir Document 1 pour le login et le mot de passe.
  - Tapez les commandes

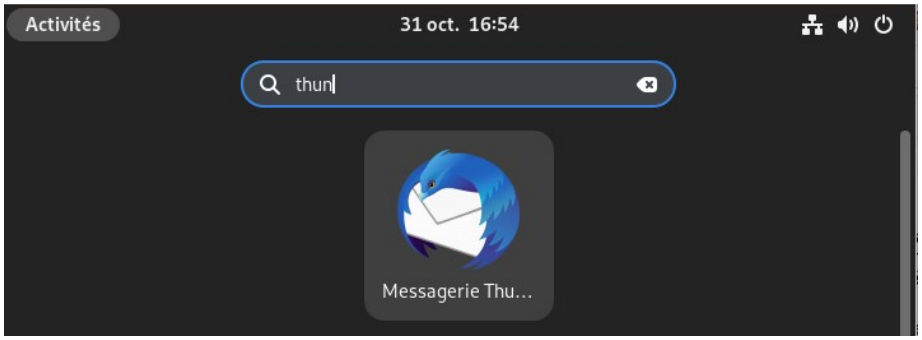
```
$ sudo useradd -m apapin
$ sudo passwd apapin
```

1.1.4 - Installation du client de messagerie Thunderbird

- Connectez-vous avec un compte administrateur (btssio par exemple)
- Connectez la VM à Internet (authentification auprès du stormshield à partir de la VM)
- Installez le logiciel Thunderbird
  - Lancez l'application Logiciels puis tapez dans la zone de recherche Thunderbird



  - Installez le premier choix proposé (celui noté 4 étoiles).
  - Vérifiez que Thunderbird a bien été installé
    - Cliquez Activités puis saisissez les premières lettres de thunderbird, l'icône doit apparaître.



1.1.5 - Intégration du compte de messagerie de M@Banque dans le client Thunderbird

- Connectez-vous avec le compte d'**Alice PAPIN** et lancez Thunderbird
- Intégrez le compte de messagerie de l'employée de M@Banque (Alice PAPIN) dans Thunderbird
  Compte de messagerie **GMX – Caramail** : voir Document 3
  Compte de messagerie **Google Gmail** : voir Document 4

© Delagrave

1.1.6 - Création de la paire de clé (banque) et questions de compréhension

La banque souhaite envoyer des messages à ses clients de manière sécurisée. Le service informatique lui conseille de chiffrer et signer numériquement tous les messages envoyés à ses clients. Pour cela, la banque doit disposer de sa propre paire de clés (une clé privée et une clé publique) et récupérer les clés publiques de ses clients.

Thunderbird dispose nativement d'un système de chiffrement asymétrique que nous allons donc utiliser.

Consulter le site suivant : (cela prend un certain temps mais cela est important)
https://support.mozilla.org/fr/kb/presentation-chiffrement-bout-en-bout-thunderbird

Répondez aux questions suivantes

Voir aussi Document 2

a) Est-ce qu'un administrateur réseau disposant de tous les droits peut lire un message d'un employé qui a été chiffré de bout en bout sur sa machine ? Pourquoi ?

b) Est-ce que les adresses de l'expéditeur et du destinataire sont protégées (rendues illisibles) par l'emploi du chiffrement de bout en bout ?

c) Quelle approche moderne est utilisée pour le chiffrement de bout en bout pour la messagerie électronique ?

d) Si un message est chiffré avec une clé publique, que doit-on posséder pour le déchiffrer ?

e) En cas de perte de sa clé privée, existe-t-il un autre moyen de déchiffrer un message chiffré par la clé publique correspondante ?

f) Pour garantir la sécurité du chiffrement de bout en bout, qu'est-il important de vérifier pour s'assurer que le message provient bien de la personne que l'on croit ?

g) Pour signer numériquement un message, quelle clé utilise-t-on ? Comment le destinataire va-t-il vérifier que la signature est valide ?

h) Est-il possible de lire le même message chiffré sur 2 machines différentes ? Si oui, à quelle(s) condition(s) ?

i) Quelle type de clé est protégée par un mot de passe ? Quel conseil pouvez-vous donner sur ce mot de passe ?

j) Est-il conseillé et prudent de diffuser sa clé publique ? Pourquoi ?

La conseillère bancaire va créer une paire de clé pour mettre en place un chiffrement de bout en bout.

k) A quoi va servir sa clé privée dans la **transmission** de messages sécurisés et signés ?

l) A quoi va servir sa clé privée dans la **réception** de messages sécurisés et signés ?

m) A quoi va servir sa clé publique dans la **transmission** de messages sécurisés et signés ?

n) A quoi va servir sa clé publique dans la **réception** de messages sécurisés et signés ?

© Delagrave

Création de la paire de clé côté banque

- Créez une nouvelle paire de clés
  Cliquez Menu (3 barres horizontales) – Outils – Gestionnaire de clés OpenPGP
  Génération – Nouvelle paire de clés
  Expiration de la clé : 3 ans Type et taille de la clé : RSA 3072

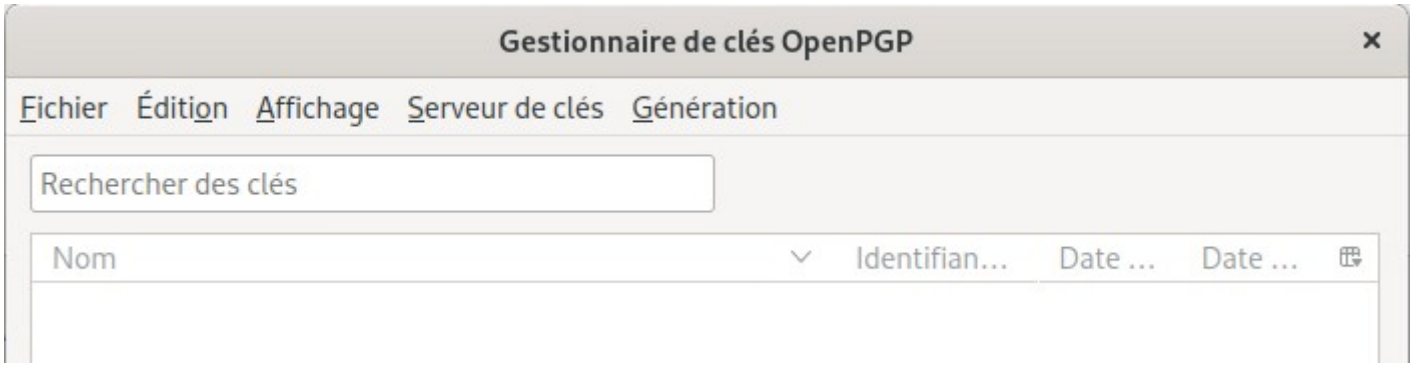


Figure 2: Gestionnaire de clés de Thunderbird

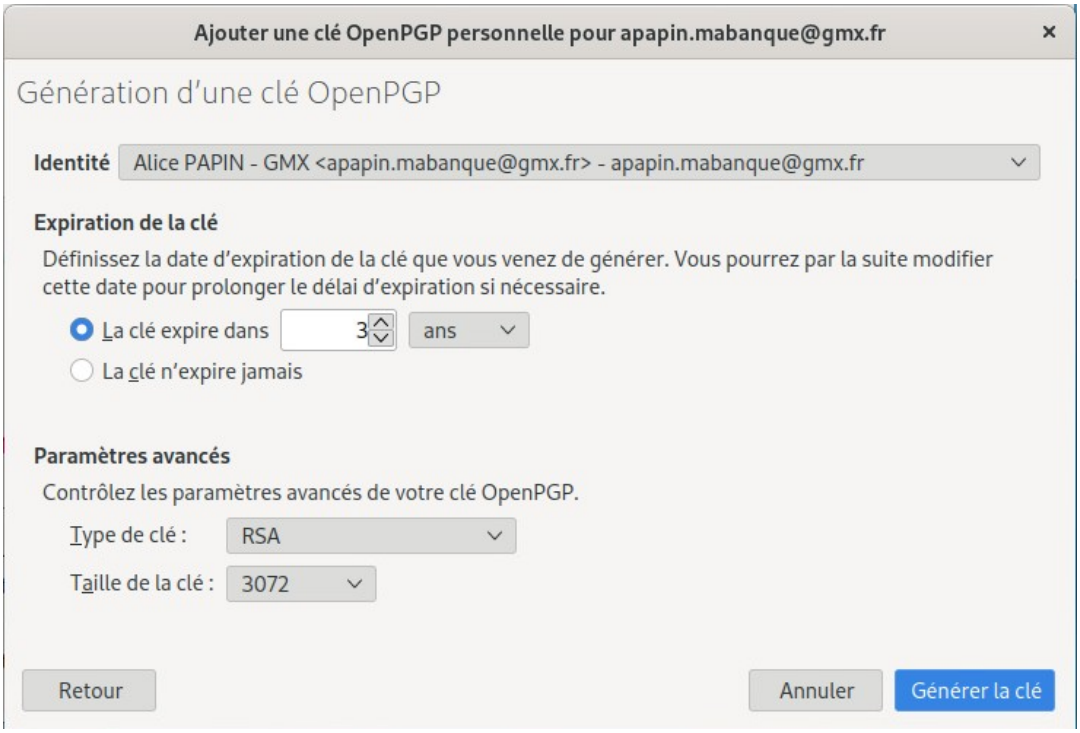


Figure 3: Génération de la paire de clé de Alice PAPIN

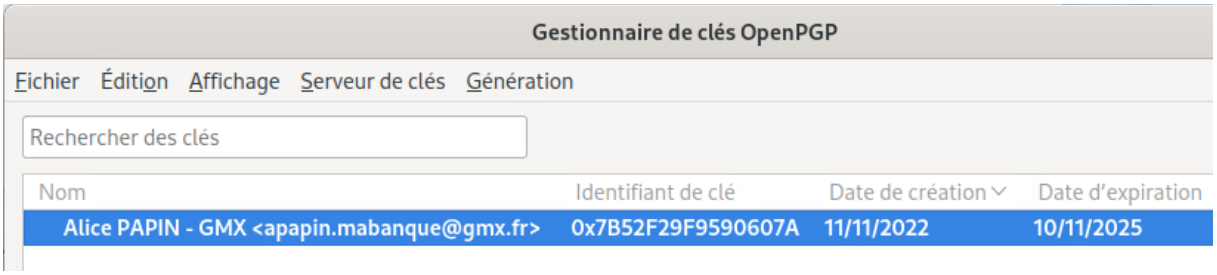
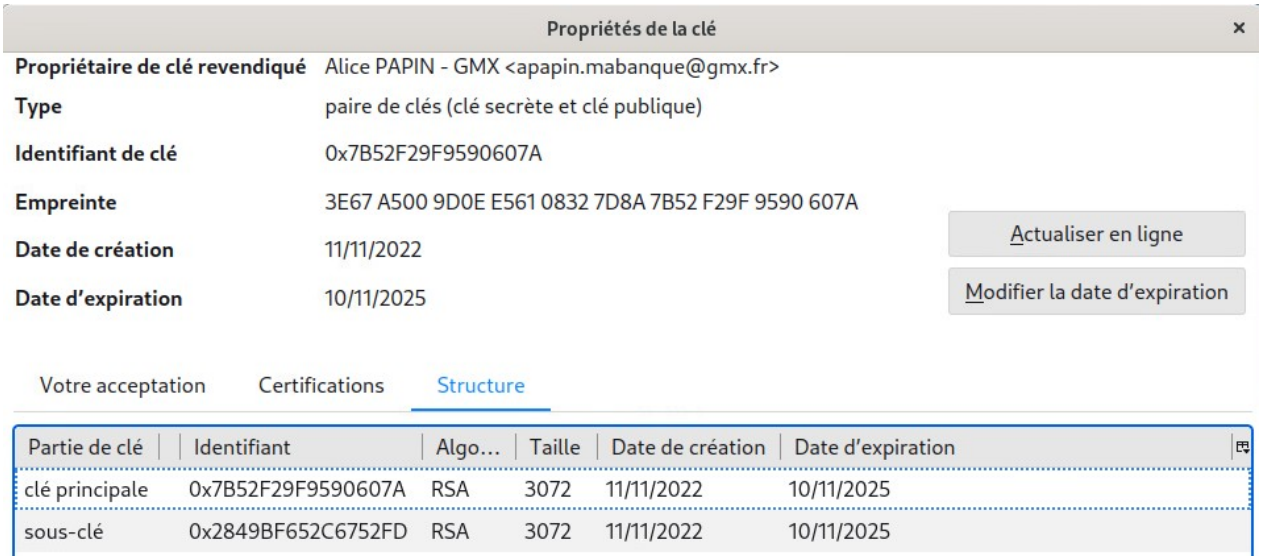


Figure 4: Alice PAPIN dispose maintenant de sa propre paire de clés.

© Delagrave

- Observez la structure des clés (Propriétés de la clé – onglet Structure) : identifiant de clé, empreinte, utilisation de chaque clé, date d'expiration



1.1.7 - Association de la clé privée au compte de messagerie

- Associez le compte de messagerie de la conseillère bancaire à la clé privée qui vient d'être créée.
  - Clic droit sur le compte de messagerie – Paramètres – Chiffrement de bout en bout
  - Sélectionner l'identifiant de la clé privée souhaitée

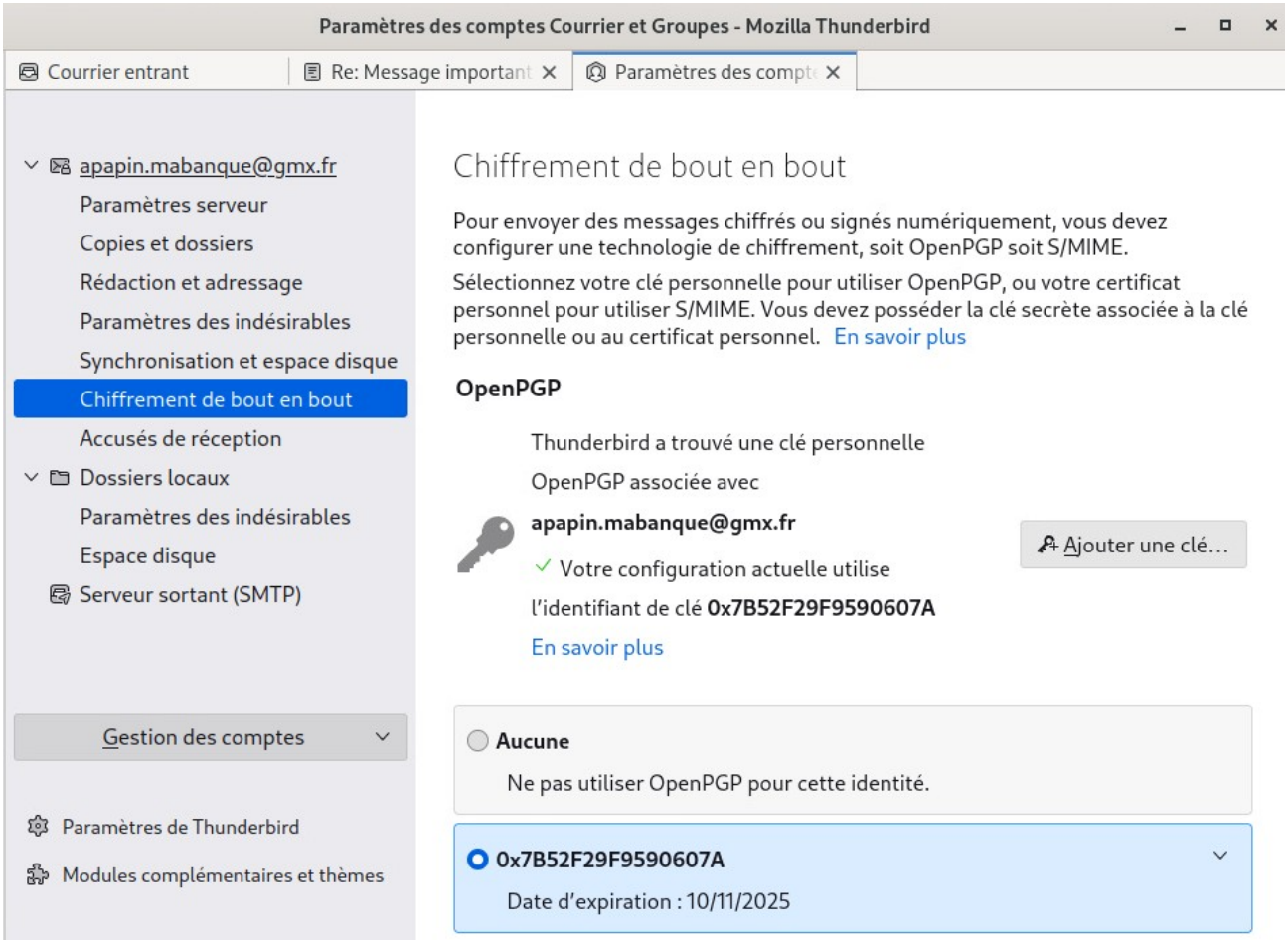


Figure 5: Activation du chiffrement de bout en bout en associant la clé privée à une adresse email

La conseillère bancaire peut maintenant utiliser le chiffrement de bout en bout.

1.1.8 - Sauvegarde de la paire de clés

Il est important de sauvegarder sa paire de clés et de la stocker dans 2 endroits sûrs éloignés géographiquement. Cela permet par exemple d'utiliser cette paire de clés sur un autre poste de travail. La paire de clés est protégée par un mot de passe. Il est conseillé de mettre une **passphrase** assez longue et difficile à deviner avec une complexité (minuscules, majuscules, chiffres, caractères spéciaux). Celle-ci doit être stockée dans un gestionnaire de mot de passe (Keypass par exemple). Si vous oubliez votre passphrase, la paire de clés sera inutilisable !

- Sauvegardez la **clé privée** (secret) dans le dossier **`Documents`** de votre espace personnel

  Gestionnaire de clés – Fichier – Sélectionner la clé à sauvegarder – Sauvegarder une ou des clés secrètes dans un fichier

  Gardez le nom donné par défaut pour la clé et proposez une passe phrase robuste.

  Exemple de passphrase : **`Leventsoufflefortdansle44!`**

- Sauvegardez la **clé publique** dans le dossier **`Documents`** de votre espace personnel

  Gestionnaire de clés – Fichier – Sélectionner la clé à sauvegarder – Exporter une des clés publiques vers un fichier

  Gardez le nom donné par défaut pour la clé

Figure 6: Exemple de fichiers de sauvegarde d'une clé publique et d'une clé privée.

Remarque : A ce stade du TP, la banque ne peut toujours pas envoyer de message chiffré. En effet, elle a besoin de la clé publique du client pour chiffrer le message qu'elle veut lui envoyer.

1.1.9 - Téléversement de la clé publique sur un serveur de clés publique

Pour cela, nous allons utiliser le serveur : https://keys.openpgp.org/

- Téléversez votre clé publique sur le serveur

  Cliquez téléverser …

Figure 7: La clé publique d'Alice Papin vient d'être téléversée sur le serveurs de clés publiques. Pour que sa clé puisse être distribuée, il faut qu'elle confirme son adresse email.

Figure 8: L'adresse email a été confirmée. Les clients pourront maintenant récupérer la clé publique de la banque.

- Essayez de téléverser votre clé privée. Que se passe-t-il ?

1.2 - Préparation de la station Windows (Client)

Lors du premier lancement de la VM Windows, définissez un compte différent de Bruno MIKO quand Windows vous le demandera (choisissez celui que vous voulez). Le compte de Bruno sera créé plus tard.

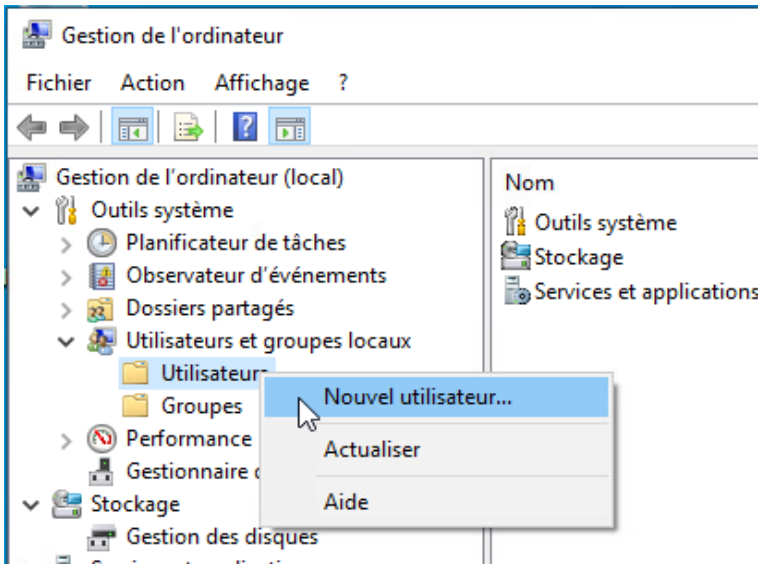
1.2.1 - Vérification paramétrage VLAN et adresse IP de la VM

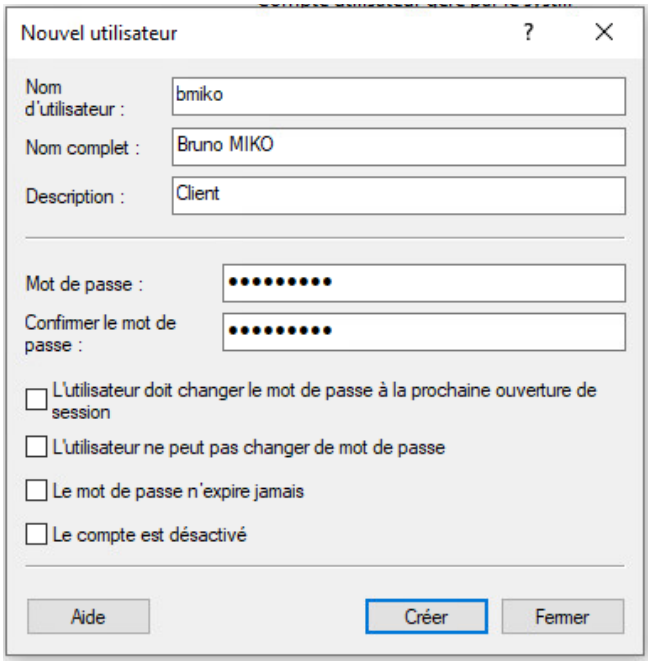
- Vérifiez que la station se trouve bien dans le VLAN SIO-PEGAGO
- Vérifiez la valeur de votre adresse IP (commande **`ipconfig`** dans une invite de commande)
  Elle doit être comprise entre 10.15.12.1 et 10.15.15.239

1.2.2 - Création du compte utilisateur local Bruno MIKO dans la station Windows

- Créez le compte utilisateur local **Bruno MIKO** et son dossier personnel. Voir Document 1 pour le login et le mot de passe.
- Clic Droit sur Menu Démarrer – Gestion de l'ordinateur

  Outils système – Utilisateurs et groupes locaux – Utilisateurs – Clic droit Nouvel utilisateur





1.2.3 - Installation du client de messagerie Thunderbird

- Connectez la VM à Internet (authentification auprès du stormshield à partir de la VM à l'aide du navigateur Internet)
- Installez le logiciel Thunderbird
  - A l'aide d'un moteur de recherche (`startpage.com` par exemple) puis tapez dans la zone de recherche Thunderbird
  - Téléchargez le fichier d'installation à partir du site officiel
  - double-cliquez sur le fichier d'installation et suivez les instructions (installation par défaut). Ne lancez pas Thunderbird.

© Delagrave

1.2.4 - Intégration du compte de messagerie du client dans Thunderbird

- Sur la station Windows, connectez-vous avec le compte de Bruno MIKO
- Intégrez le compte de messagerie du client de la banque (Bruno MIKO) dans Thunderbird
  Compte de messagerie **GMX – Caramail** : voir Document 3
  Compte de messagerie **Google Gmail** : voir Document 4

1.2.5 - Création de la paire de clé (client)

Le client a besoin de créer une paire de clés pour communiquer de manière sécurisée avec sa banque. Il a reçu les instructions à réaliser de la banque pour les créer.

- Créez une nouvelle paire de clés
- Observez la structure des clés (Propriétés de la clé – onglet Structure) : identifiant de clé, empreinte, utilisation de chaque clé, date d'expiration

1.2.6 - Association de la clé privée au compte de messagerie

- Associez le compte de messagerie de la conseillère bancaire à la clé privée qui vient d'être créée.
  - Clic droit sur le compte de messagerie – Paramètres – Chiffrement de bout en bout
  - Sélectionner l'identifiant de la clé privée souhaitée

Le client de la banque peut maintenant utiliser le chiffrement de bout en bout.

1.2.7 - Sauvegarde de la paire de clés

- Sauvegardez la **clé privée** (secret) dans le dossier **`Documents`** de votre espace personnel
  Gardez le nom donné par défaut pour la clé et proposez une passe phrase robuste.
  Exemple de passphrase : **`Lechatmangeles125souris!`**
- Sauvegardez la **clé publique** dans le dossier **`Documents`** de votre espace personnel
  Gardez le nom donné par défaut pour la clé

Remarque : A ce stade du TP, le client de la banque ne peut toujours pas envoyer de message chiffré. En effet, il a besoin de la clé publique de la banque pour chiffrer le message qu'il veut lui envoyer.

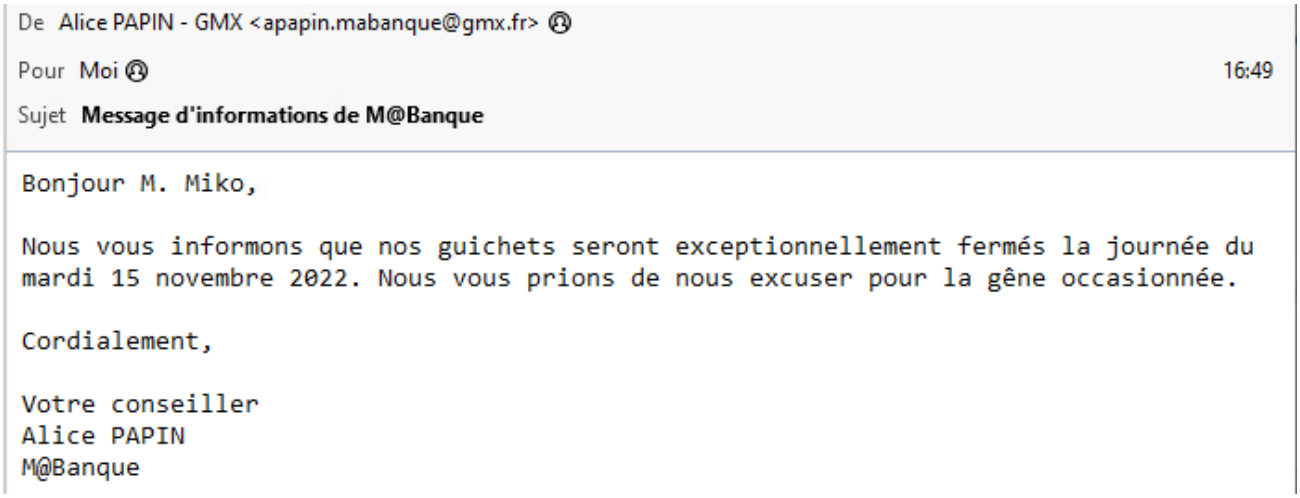
1.2.8 - Téléversement de la clé publique sur un serveur de clés publique

- Téléversez votre clé publique sur le serveur https://keys.openpgp.org/

2 - Test envoi courriel non chiffré

- Testez l'envoi de courriels entre les deux acteurs et vérifiez si le contenu du message est chiffré.
  Le test doit démontrer que le contenu du message n'est pas chiffré. Faites une capture d'écran.

© Delagrave


De Alice PAPIN - GMX <apapin.mabanque@gmx.fr>

Pour Moi 16:49

Sujet **Message d'informations de M@Banque**

Bonjour M. Miko,

Nous vous informons que nos guichets seront exceptionnellement fermés la journée du mardi 15 novembre 2022. Nous vous prions de nous excuser pour la gêne occasionnée.

Cordialement,

Votre conseiller
Alice PAPIN
M@Banque

Figure 9: Le conseiller bancaire informe un client par courriel. Le message envoyé n'est pas chiffré.


De Bruno MIKO - Gmail <bmiko.client@gmail.com>

Pour Moi 16:52

Sujet **Re: Message d'informations de M@Banque**

Bonjour Mme Papin,

Merci pour cette information.

Cordialement,

M. Miko Bruno

Le 12/11/2022 à 16:49, Alice PAPIN - GMX a écrit :

> Bonjour M. Miko,
>
> Nous vous informons que nos guichets seront exceptionnellement fermés la journée du mardi 15 novembre 2022. Nous vous prions de nous excuser pour la gêne occasionnée.
>
> Cordialement,
>
> Votre conseiller
> Alice PAPIN
> M@Banque

Figure 10: Le client répond à sa banque. La réponse n'est pas chiffrée.

3 - Test envoi chiffré et signé

- Testez l'envoi de courriels chiffrés entre les deux utilisateurs en indiquant les éléments qui permettent de vérifier si l'envoi est bien sécurisé. Voir Éléments de réponse pour vous aider un peu plus bas
  - **Étape 1** : L'expéditeur écrit un message en s'assurant que le **dispositif de chiffrement et de signature** sont présents
  - **Étape 2** : L'expéditeur **chiffre et signe** le message puis l'envoie, le sujet n'est pas chiffré. Détaillez la procédure
  - **Étape 3** : Le destinataire réceptionne le message chiffré et l'ouvre pour le lire. Expliquez ce qu'il se passe.

Éléments de réponse

3.1 - Test 1 : Conseillère bancaire envoie un message sécurisé et signé au bon client

Alice PAPIN, la conseillère bancaire, souhaite envoyer un message à un de ses clients, Bruno MIKO, pour lui signaler qu'une opération suspecte a été effectuée sur son compte.

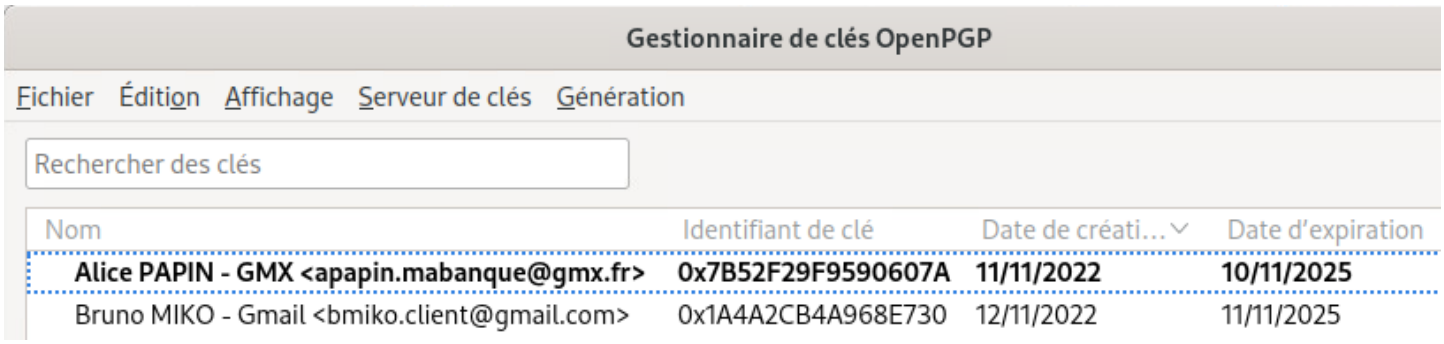
Le message doit être traité de façon à ce que :

- Seul, le client concerné puisse lire le message. Une autre personne recevant ce message ne doit pas pouvoir le comprendre, ni le déchiffrer.
- Le client concerné doit être certain que le message n'a pas été modifié lors de son transfert.
- Le client concerné doit être certain que le message provient bien de la banque.

3.1.1 - Opérations à effectuer côté Banque

- Redémarrez la machine de la conseillère bancaire Alice PAPIN
- Lancez Thunderbird
- Vérifiez que la conseillère bancaire, Alice PAPIN, possède bien la clé publique du client concerné, Bruno MIKO
  - Ouvrez le gestionnaire de clés OpenPGP, la clé de Bruno MIKO doit être présente

    Si ce n'est pas le cas, récupérez-la sur le serveur de clés publiques **keys.openpgp.org** en saisissant l'adresse email du client concerné. Ensuite, importez-la dans Thunderbird.



- Acceptez la clé de M. MIKO pour vérifier les signatures numériques et chiffrer les messages
  Propriétés de la clé – onglet Votre acceptation

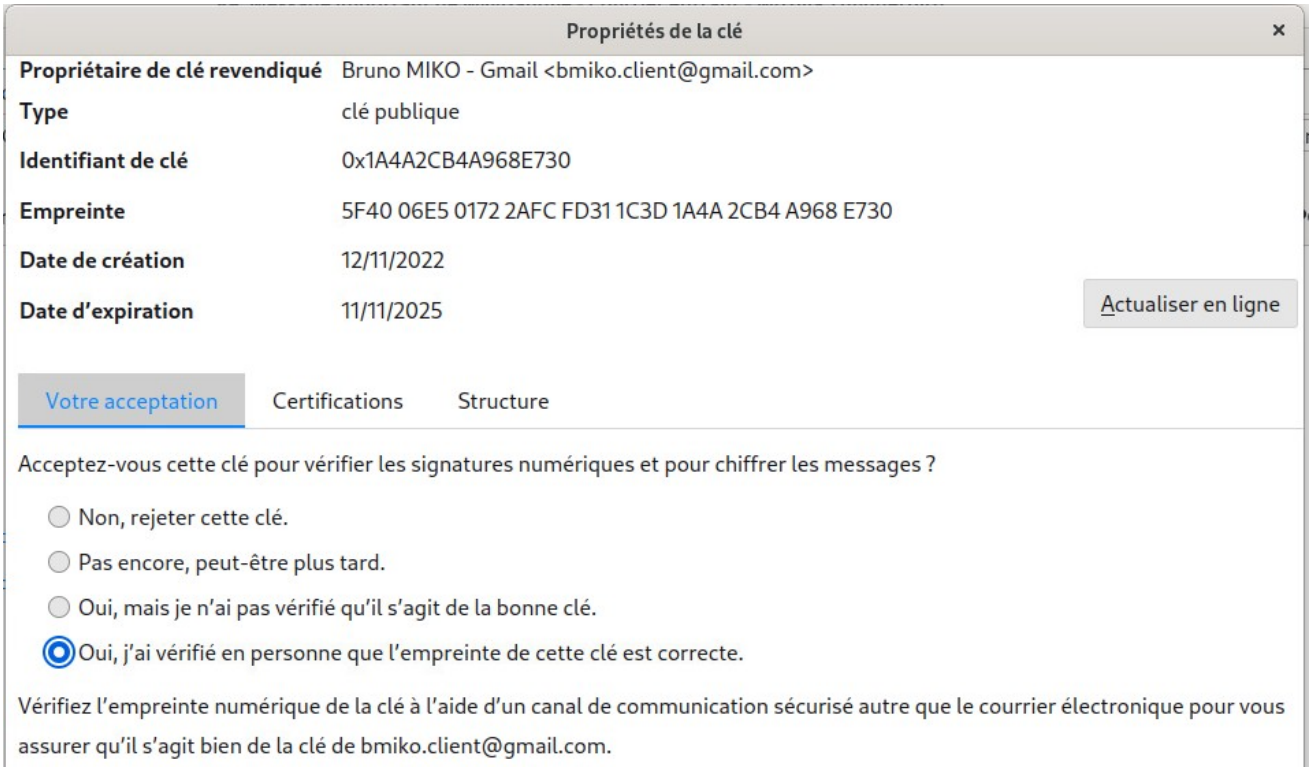


Figure 11: Acceptation de la clé de M. MIKO

- Écrivez le message que va envoyer la conseillère bancaire.

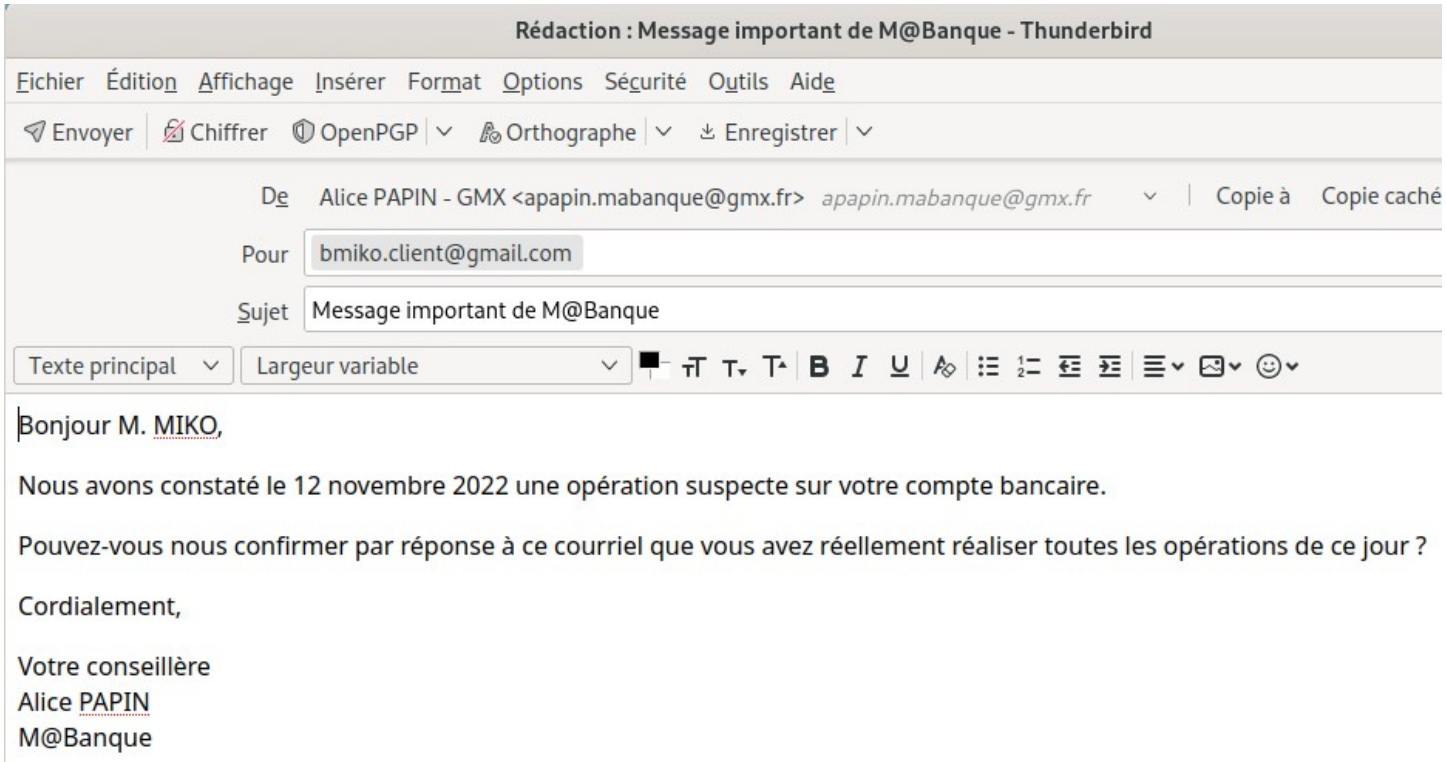
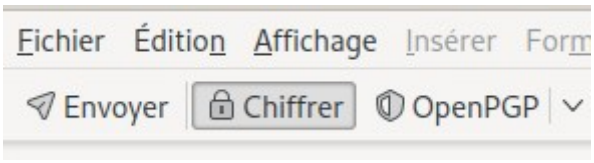
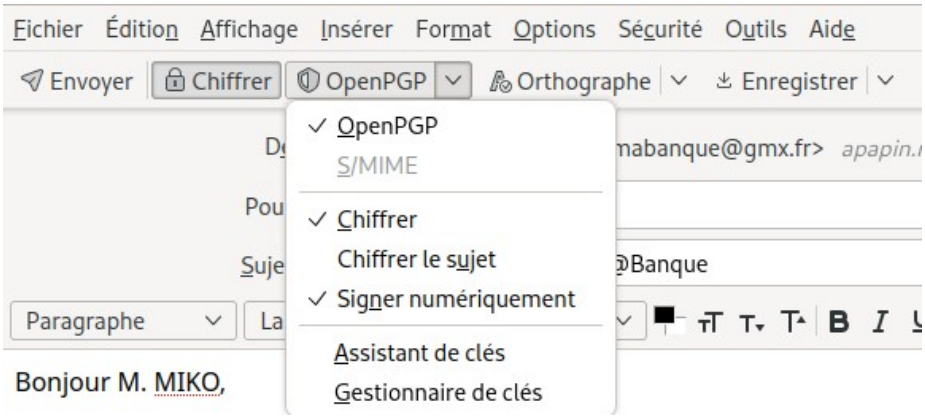


Figure 12: Rédaction du message à envoyer. Constatez que par défaut, celui-ci n'est pas chiffré (petit cadenas de l'option "Chiffrer" est barré en rouge).

- Chiffrez le message en cliquant sur le bouton **Chiffrer** (il change de couleur et le cadenas n'est plus barré)



- Ne chiffrez pas le sujet et signez numériquement
  - Ouvrez la liste déroulante **OpenPGP** à côté de l'option **Chiffrer** et cocher/décocher les options souhaitées.



- Envoyez le message

3.1.2 - Opérations à effectuer côté Client

- Redémarrez la machine du client Bruno MIKO
- Lancez Thunderbird
- Vérifiez que le client a bien reçu un message de la banque.
- Que pouvez-dire du message reçu ? Expliquez. Aidez-vous des indications données en cliquant sur l'icône OpenPGP-Cadenas-Certificat et de la pièce jointe. Faites des captures d'écran

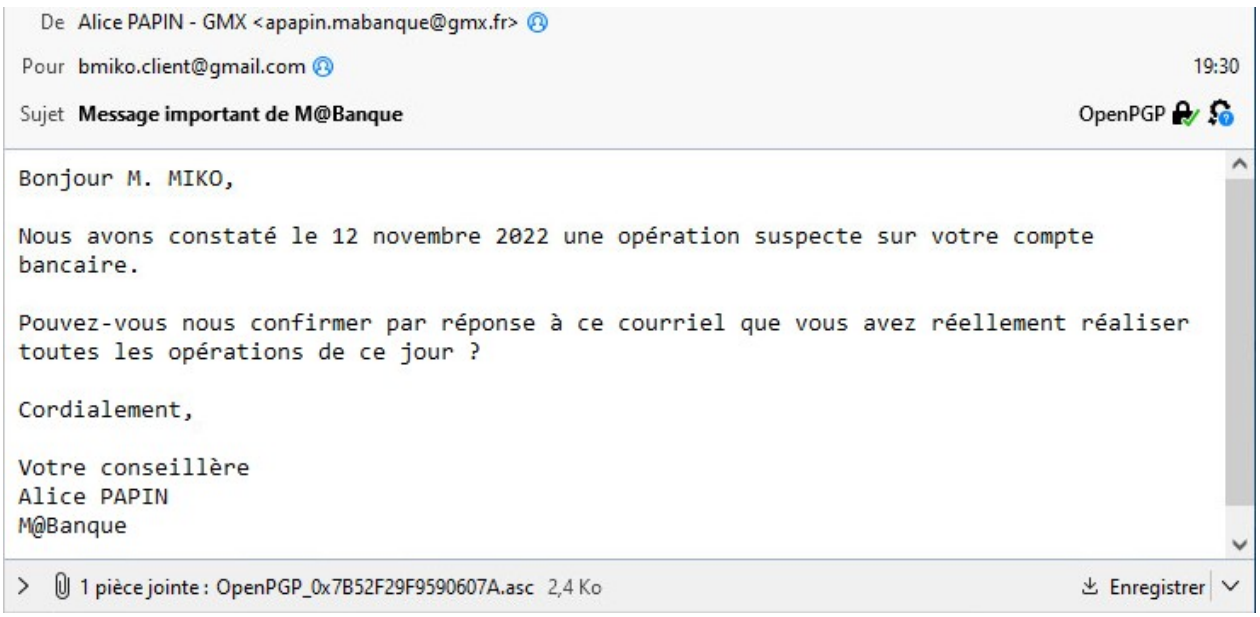
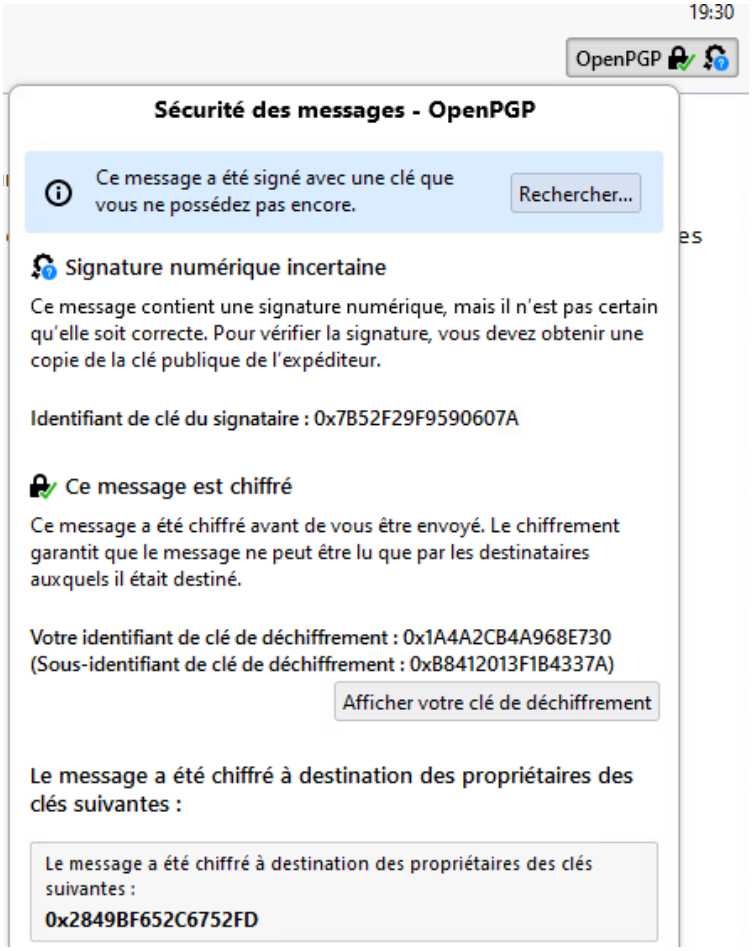


Figure 13: Message que le client a reçu de la banque. Constatez la présence de la clé publique de la banque en pièce jointe.



- Sachant que c'est le premier message que le client reçoit de sa banque, faites ce qui est nécessaire pour vérifier et valider la signature du message reçu. Expliquez en détail la procédure. Faites des captures d'écran permettant de comprendre...

  Avant de répondre, posez-vous les questions suivantes :
  - Suis-je sûr que l'expéditeur est bien la banque ?
  - La pièce jointe contenant la clé publique de la banque, suis-je sûr qu'elle appartienne bien à la banque ?

3.2 - Test 2 : Le client répond à la banque avec un message sécurisé et signé

Bruno MIKO, le client de M@Banque, vient de recevoir un courriel de la banque et va donc lui répondre avec un message sécurisé et signé.

- Répondez avec le compte du client au message de la banque avec un message sécurisé et signé. Faites des captures d'écran montrant que le chiffrement de bout en bout a bien été respecté.

  Expliquez comment est effectué le chiffrement, la signature côté client. Puis, dans un 2ème temps, comment est effectué le déchiffrement et la vérification de la signature côté banque.

3.3 - Test 3 : Le client souhaite consulter les courriels de sa banque sur son mobile par webmail

M. Miko veut consulter ses courriels de sa banque en webmail (accès messagerie via un navigateur). En effet, il est en déplacement et ne peut pas utiliser Thunderbird car il n'est pas installé sur son mobile.

- Accédez en webmail au compte de messagerie de M. Miko. Que constatez-vous ?

4 - Analyse du dispositif de chiffrement et de signature de Thunderbird

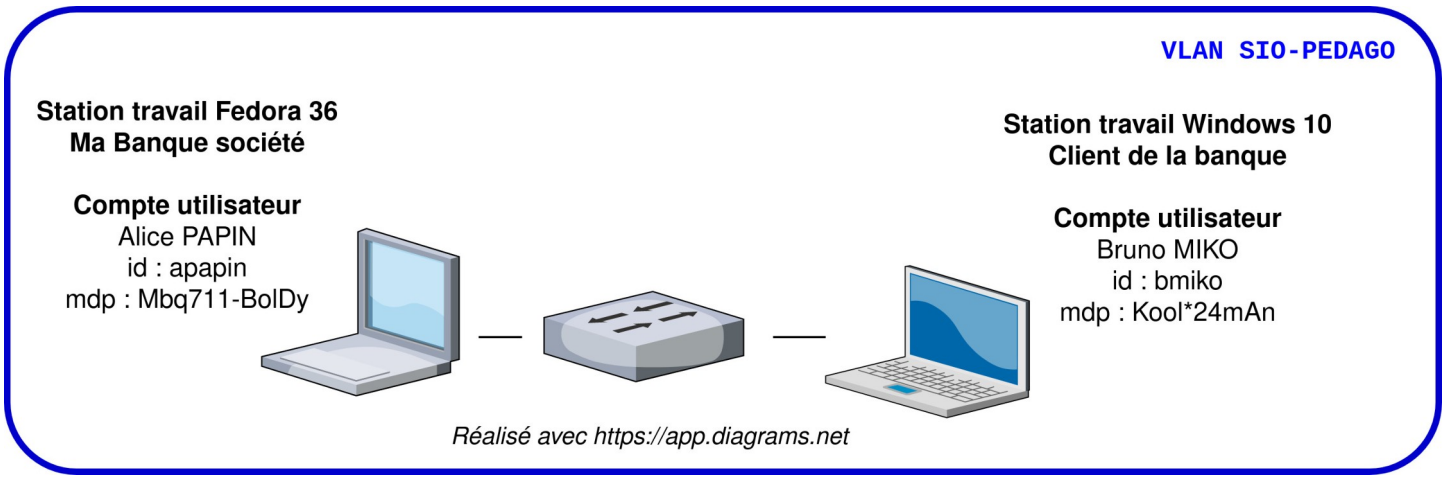
- Prouvez que le message garantit bien : la confidentialité, la preuve et l'intégrité. Expliquez en détail.
-

5 - Réalisation d'un rapport sur l'intérêt du chiffrement PGP

- Rédigez un rapport sur les tests réalisés qui démontre que l’utilisation du chiffrement PGP répond à un besoin de renforcement des moyens de preuves sécurisés.

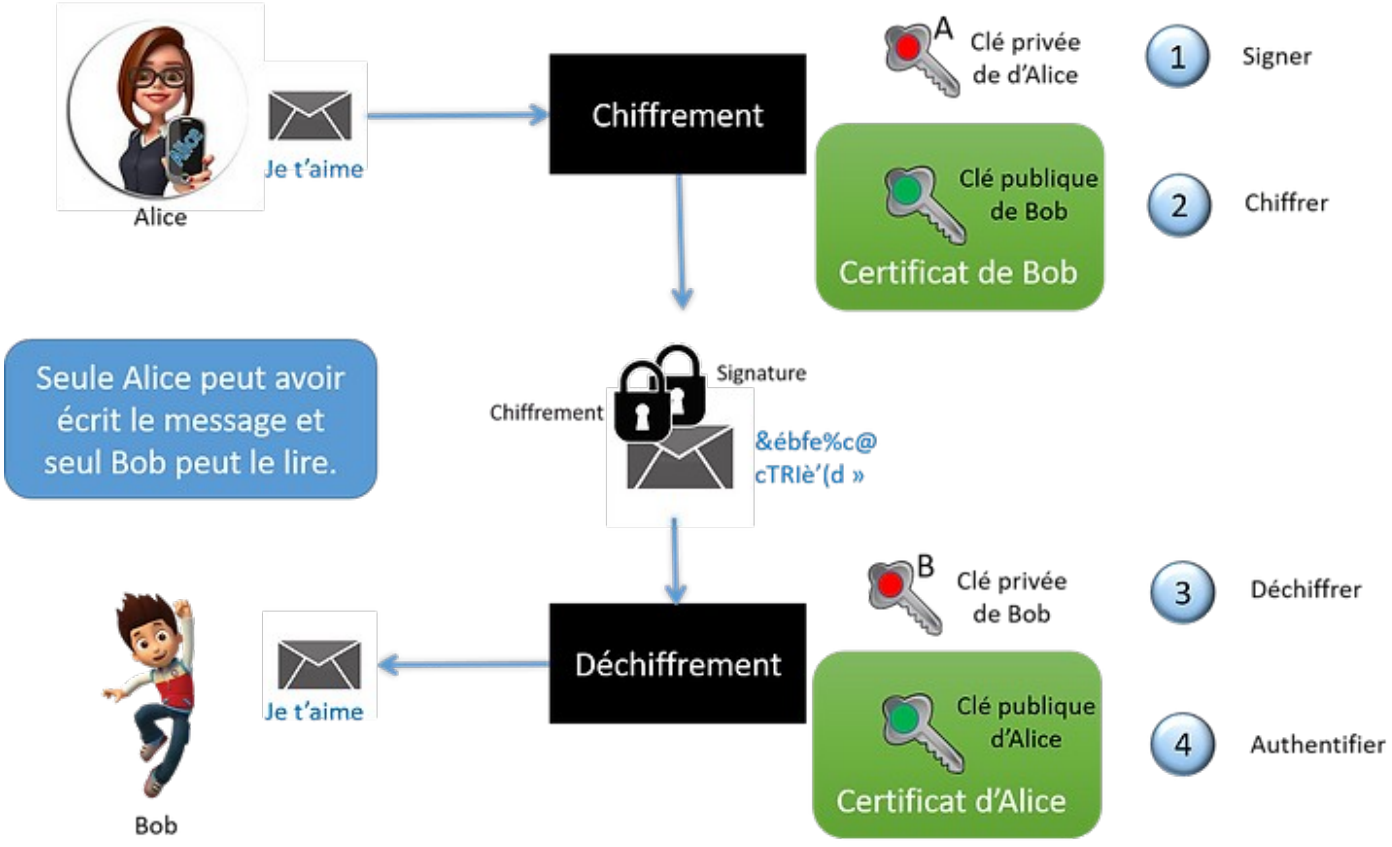
© Delagrave

Document 1 - Schéma réseau de l'environnement de test



Document 2 - Signer et Chiffrer un message

Source : https://www.sciencesculture.com/post/kezako-certificats-num%C3%A9riques



A l 'émission	A la réception
1/ Alice chiffre son message avec sa clé privée pour le signer.	3/ Bob utilise d'abord sa clé privée pour déchiffrer le message. Lui seul, est capable de le faire.
2/ Ensuite Alice utilise la clé publique de Bob pour de nouveau le chiffrer.	4/ Bob utilise ensuite la clé publique d'Alice pour s'assurer que c'est bien elle qui a envoyé le message.

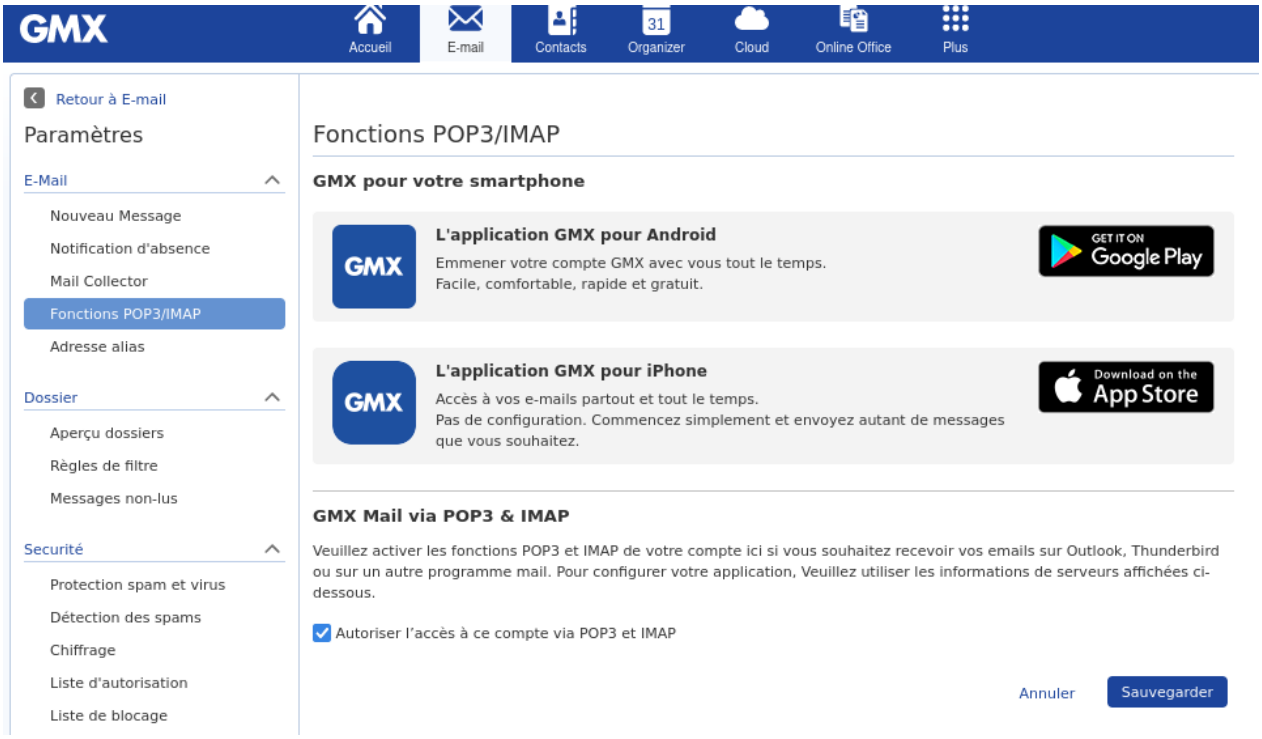
En résumé :

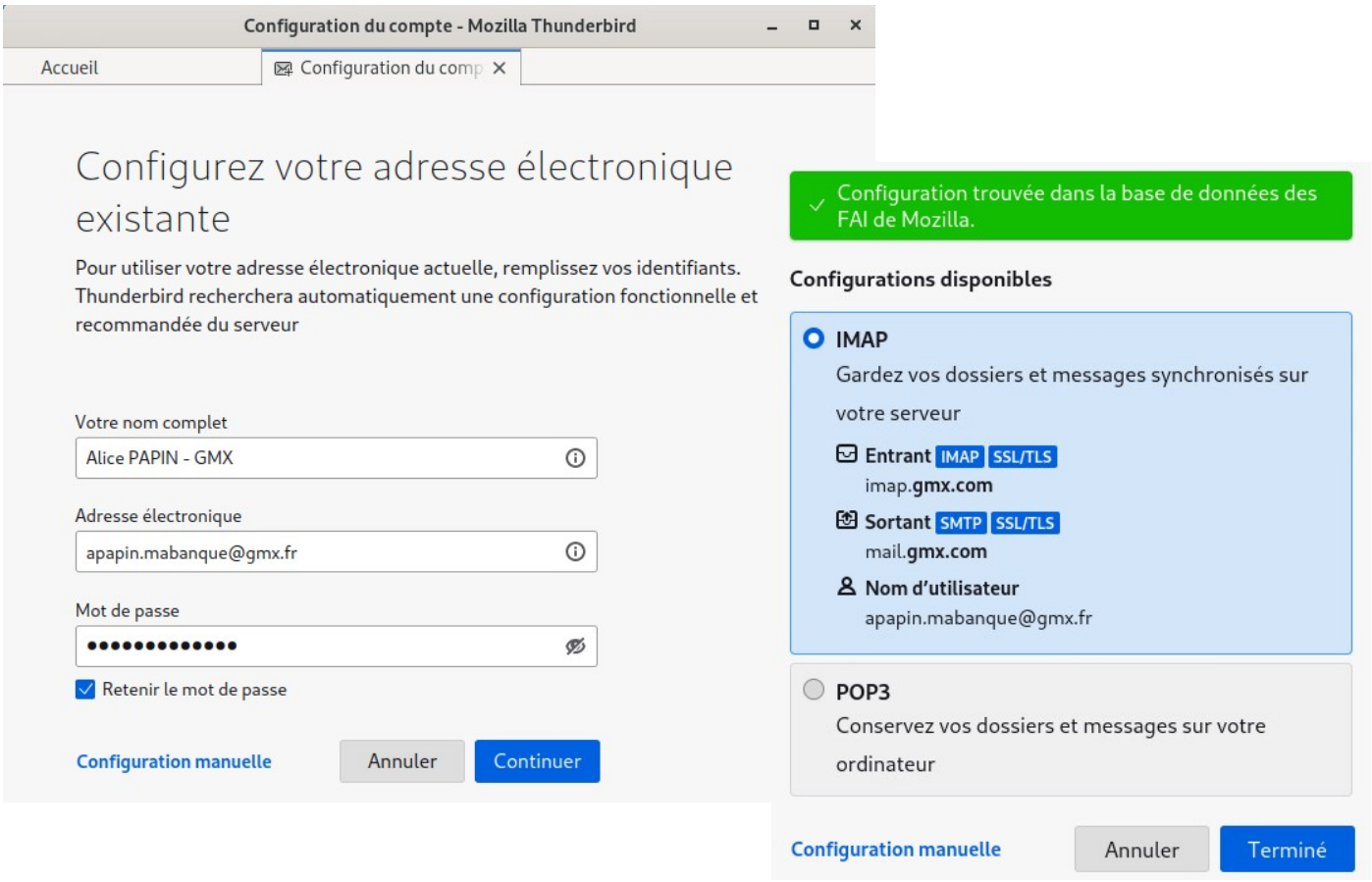
- Pour signer un message, utilisez votre clé privée.
- Pour chiffrer, utilisez la clé publique de votre destinataire.

Document 3 - Paramétrage d'un compte GMX (Caramail) dans Thunderbird

NE COPIEZ PAS bêtement cet exemple. Adaptez-le à votre adresse email.

Remarque : il faut activer l'accès via POP3/IMAP du compte GMX pour permettre à Thunderbird de se connecter au serveur de messagerie.





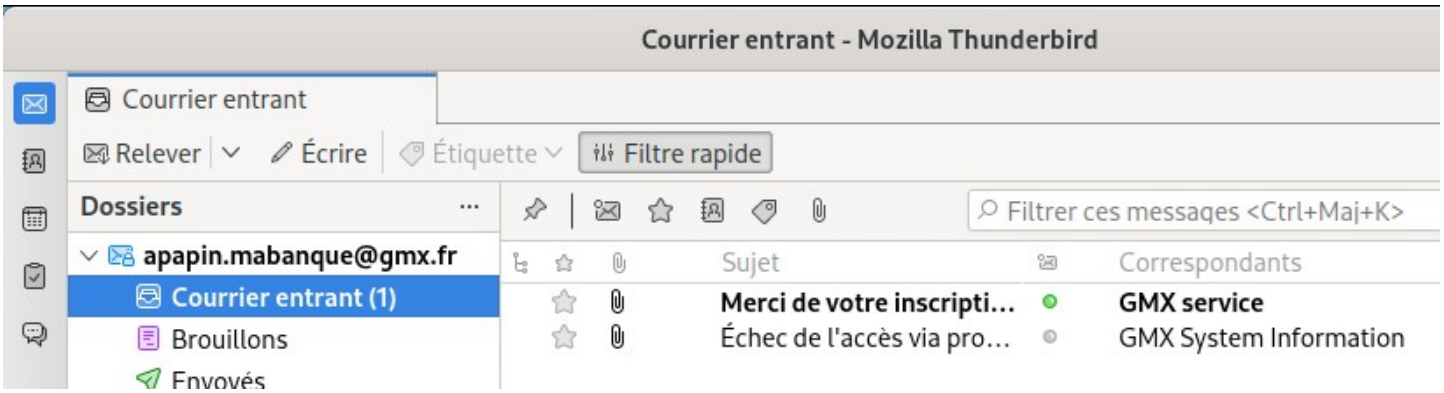
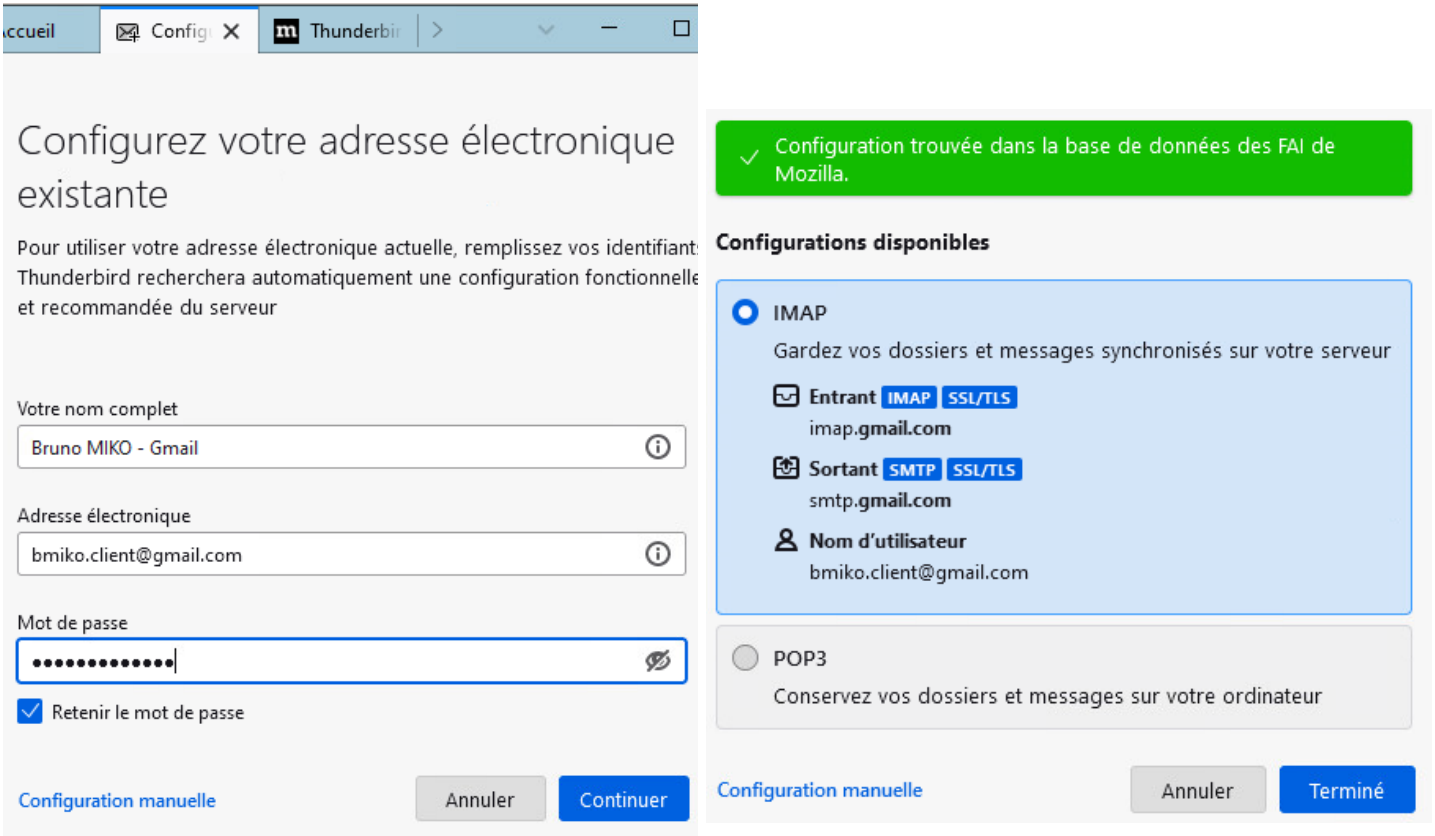


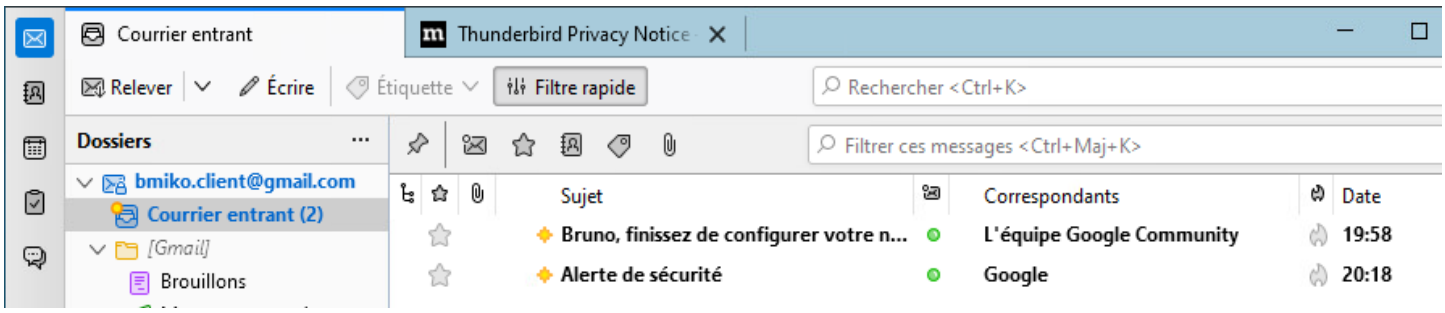
Figure 14: Le compte de messagerie **apapin.mabanque@gmx.fr** a bien été configuré dans Thunderbird.

Document 4 - Paramétrage d'un compte Gmail dans Thunderbird

NE COPIEZ PAS bêtement cet exemple. Adaptez-le à votre adresse email.

Remarque : il faut activer l'accès via POP3/IMAP du compte GMX pour permettre à Thunderbird de se connecter au serveur de messagerie.





© Delagrave