

## TP 2

# Déployer des moyens de preuves sécurisés et conformes à la législation

## Critère 1

2 captures écran commentées - Association clé privée au compte de messagerie (pour les 2 comptes).  
Paramètres des comptes - Chiffrement de bout en bout

### Compte conseillère bancaire Alice PAPIN

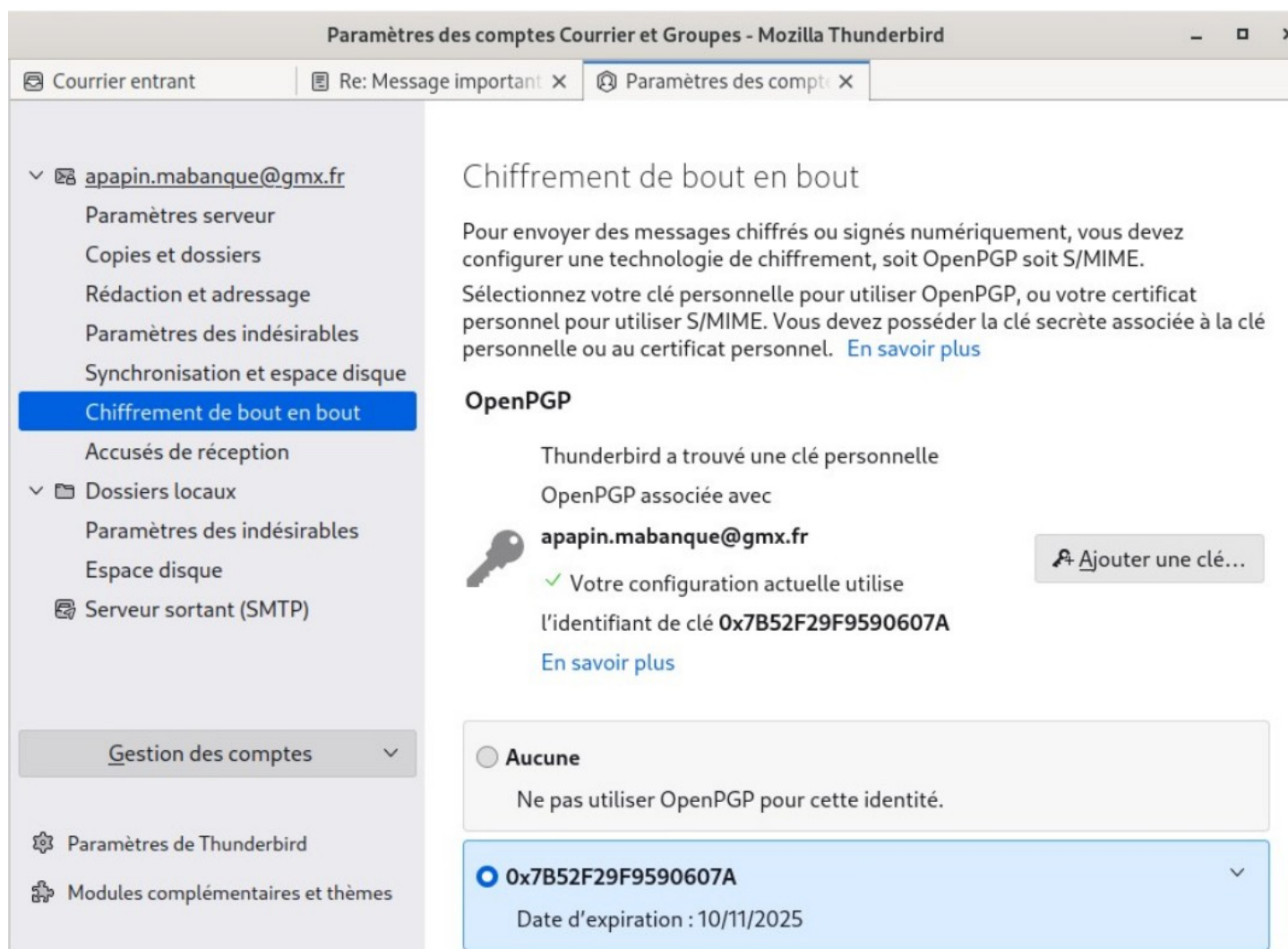


Figure 5: Activation du chiffrement de bout en bout en associant la clé privée à une adresse email

## Compte client Bruno MIKO

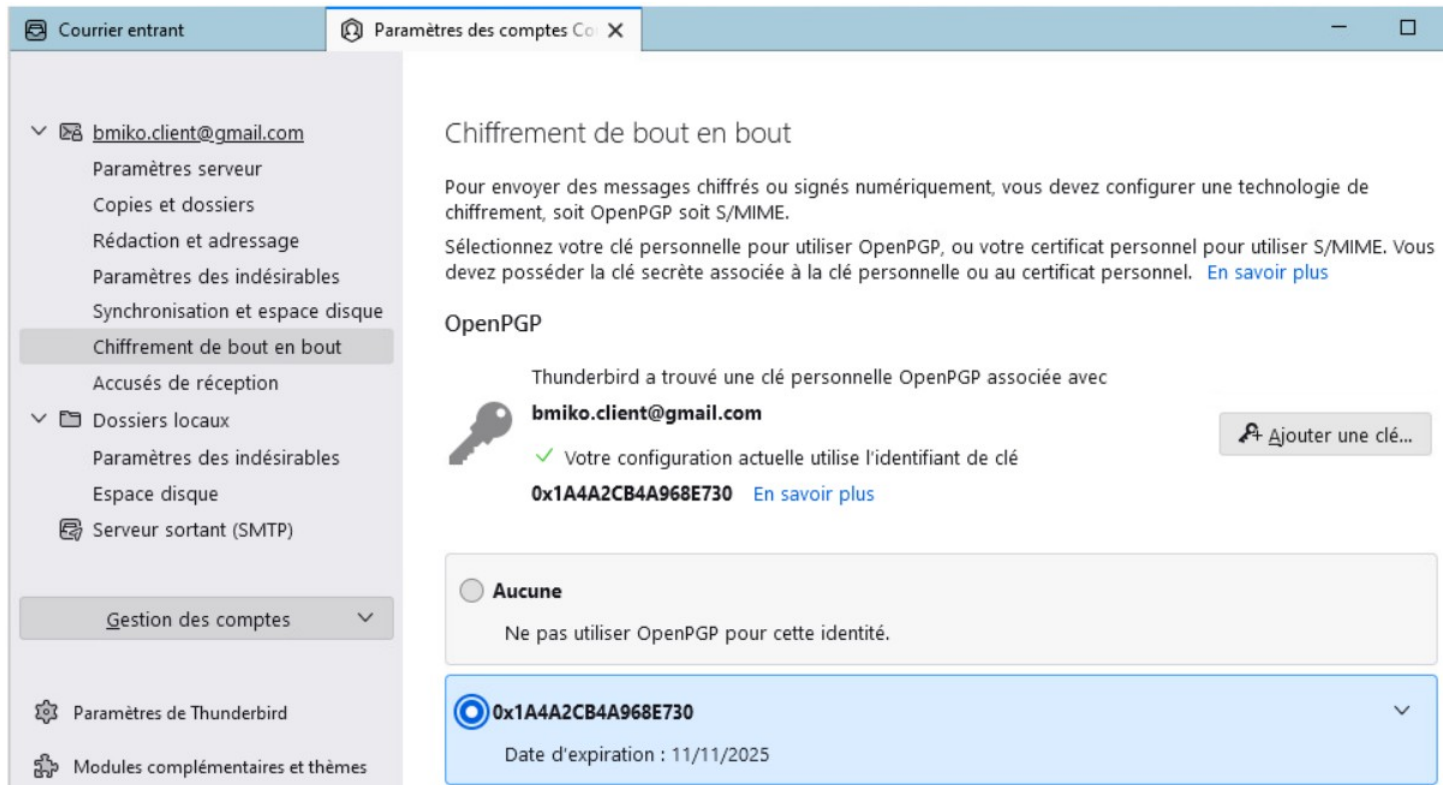


Figure 10: Activation du chiffrement de bout en bout en associant la clé privée à une adresse email

## Critère 2

Les clés publiques des 2 comptes de messagerie sont publiées sur le serveur <https://keys.openpgp.org>

# keys.openpgp.org

We found an entry for `apapin.mabanque@gmx.fr`.

<https://keys.openpgp.org/vks/v1/by-fingerprint/3E67A5009D0EE56108327D8A7B52F29F9590607A>

# keys.openpgp.org

We found an entry for `bmiko.client@gmail.com`.

<https://keys.openpgp.org/vks/v1/by-fingerprint/5F4006E501722AFCFD311C3D1A4A2CB4A968E730>

### Critère 3

La clé publique du destinataire a bien été importée dans le compte de messagerie de l'expéditeur

Gestionnaire de clés OpenPGP

Fichier Édition Affichage Serveur de clés Génération

Rechercher des clés

Nom	Identifiant de clé	Date de cr...	Date d'expiration
Alice PAPIN - GMX <apapin.mabanque@gmx.fr>	0x7B52F29F9590607A	11/11/2022	10/11/2025
Bruno MIKO - Gmail <bmiko.client@gmail.com>	0x1A4A2CB4A968E730	12/11/2022	11/11/2025

---

Propriétés de la clé

Propriétaire de clé revendiqué Alice PAPIN - GMX <apapin.mabanque@gmx.fr>

Type clé publique

Identifiant de clé 0x7B52F29F9590607A

Empreinte 3E67 A500 9D0E E561 0832 7D8A 7B52 F29F 9590 607A

Date de création 11/11/2022

Date d'expiration 10/11/2025

Actualiser en ligne

Figure 1: La clé publique du destinataire est bien importée (apapin.mabanque@gmx.fr) dans le compte de l'expéditeur (bmiko.client@gmail.com)

Gestionnaire de clés OpenPGP

Fichier Édition Affichage Serveur de clés Génération

Rechercher des clés

Nom	Identifiant de clé	Date de créati...	Date d'expiration
Alice PAPIN - GMX <apapin.mabanque@gmx.fr>	0x7B52F29F9590607A	11/11/2022	10/11/2025
Bruno MIKO - Gmail <bmiko.client@gmail.com>	0x1A4A2CB4A968E730	12/11/2022	11/11/2025

Figure 2: La clé publique du destinataire est bien importée (bmiko.client@gmail.com) dans le compte de l'expéditeur (apapin.mabanque@gmx.fr)

## Critère 4

Le client de la banque a reçu un message chiffré et signé de la conseillère de la banque

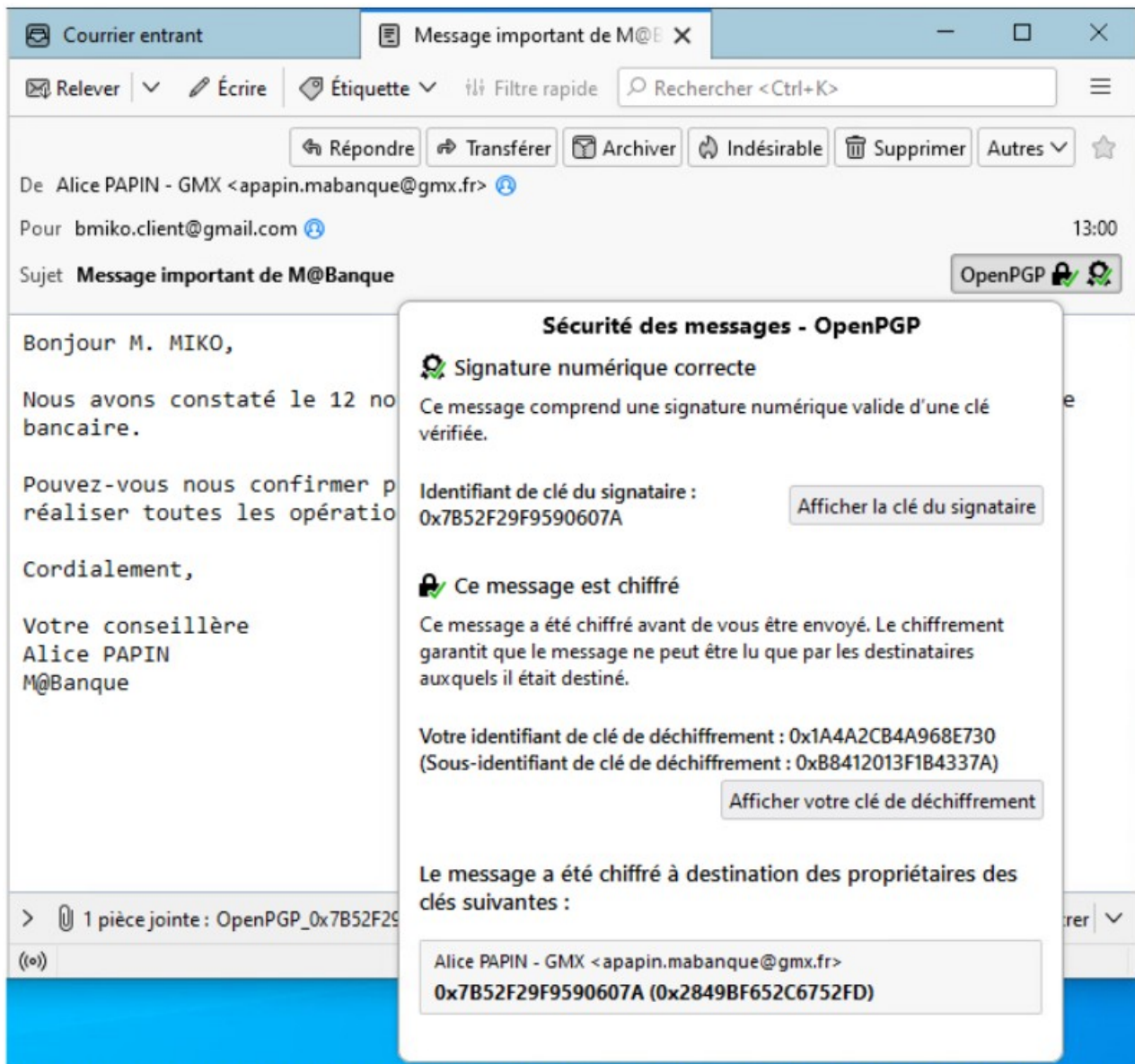


Figure 18: Le cadenas et le certificat d'OpenPGP ont une coche verte, ce qui prouve que le message est valide (non modifié) et que la signature a été reconnue. Le message chiffré par la banque a bien été déchiffré par la clé privée du client. La signature du message a été validée par la clé publique de la banque.



## Critère 5

La conseillère bancaire a reçu la réponse du client (message chiffré et signé par le client)

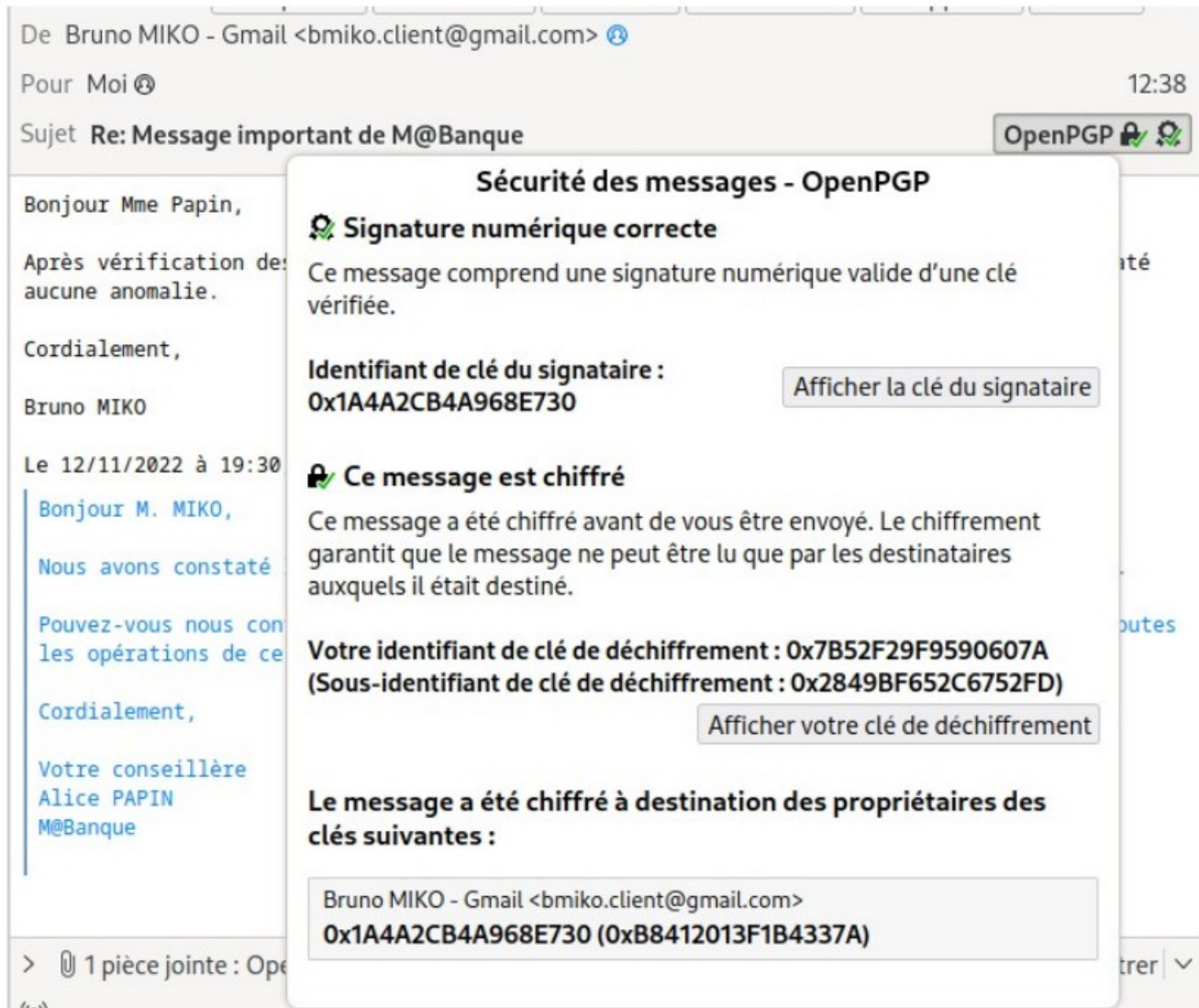


Figure 21: Le message reçu est valide et la signature est conforme

## Critère 6

Le client de la banque constate qu'il ne peut pas lire les messages chiffrés s'il utilise un client de messagerie différent de Thunderbird (son webmail par exemple)

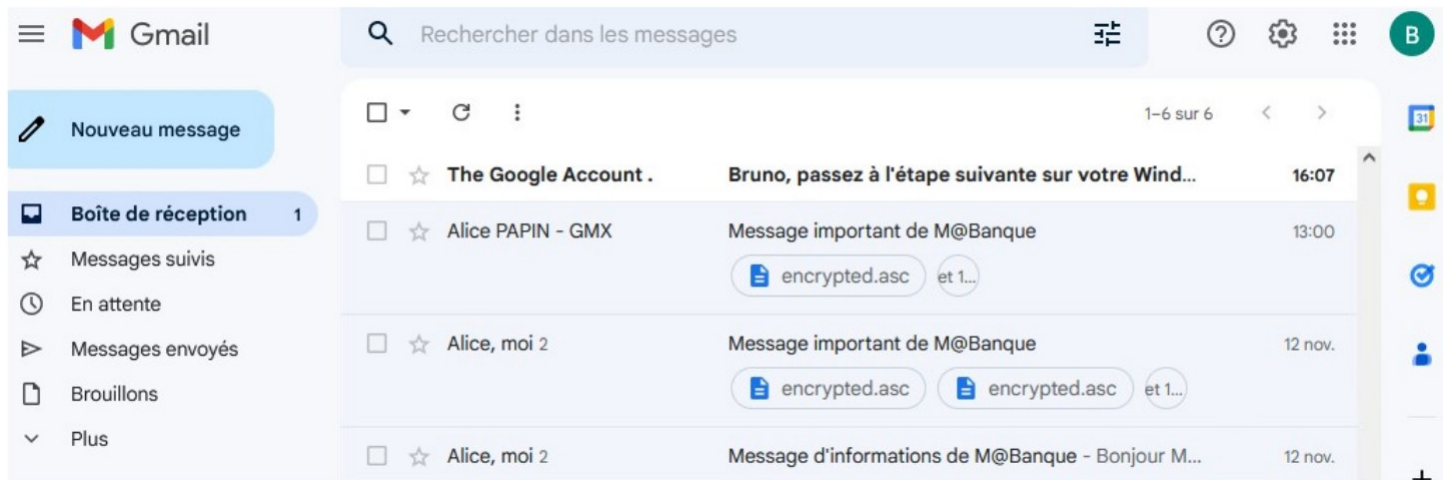


Figure 3: Le client ne peut pas lire les 2 premiers messages car ils sont chiffrés et le client de messagerie ne dispose pas des clés de déchiffrement.