Thème 2 Chapitre 3

Préserver l'identité numérique de l'organisation

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

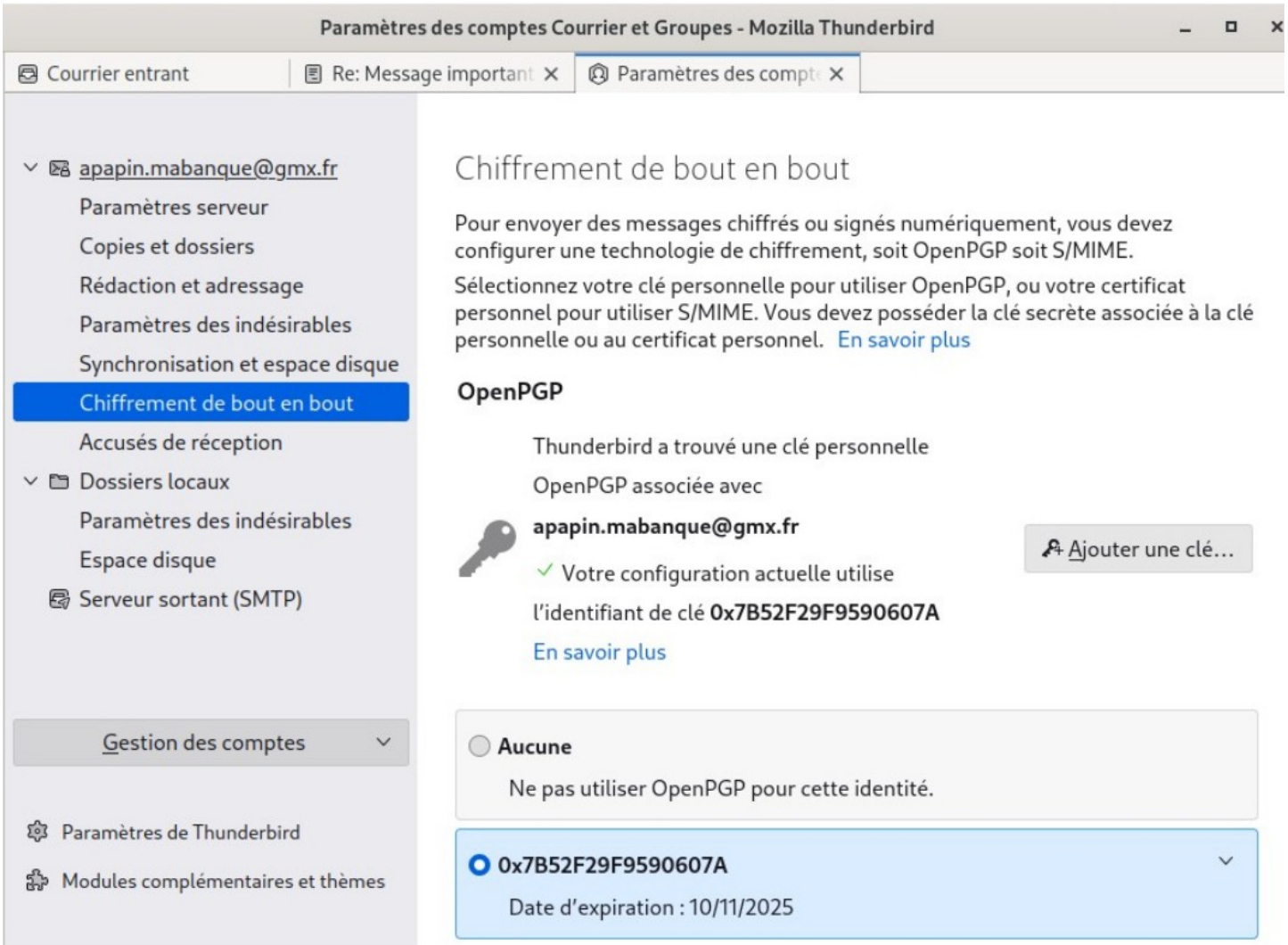

Figure 5: Activation du chiffrement de bout en bout en associant la clé privée à une adresse email

Compte client Bruno MIKO

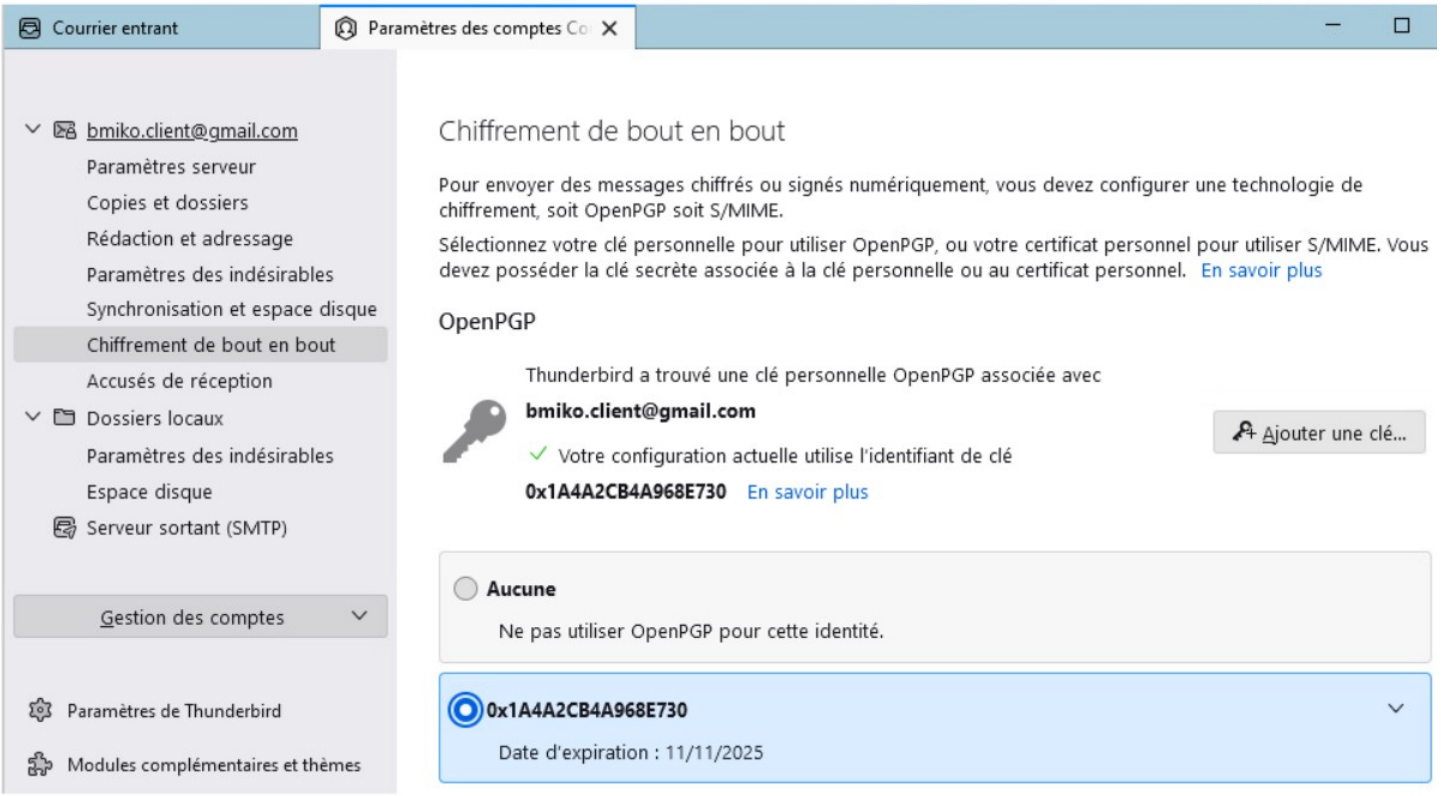

Figure 10: Activation du chiffrement de bout en bout en associant la clé privée à une adresse email

Critère 2

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

Critère 3

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

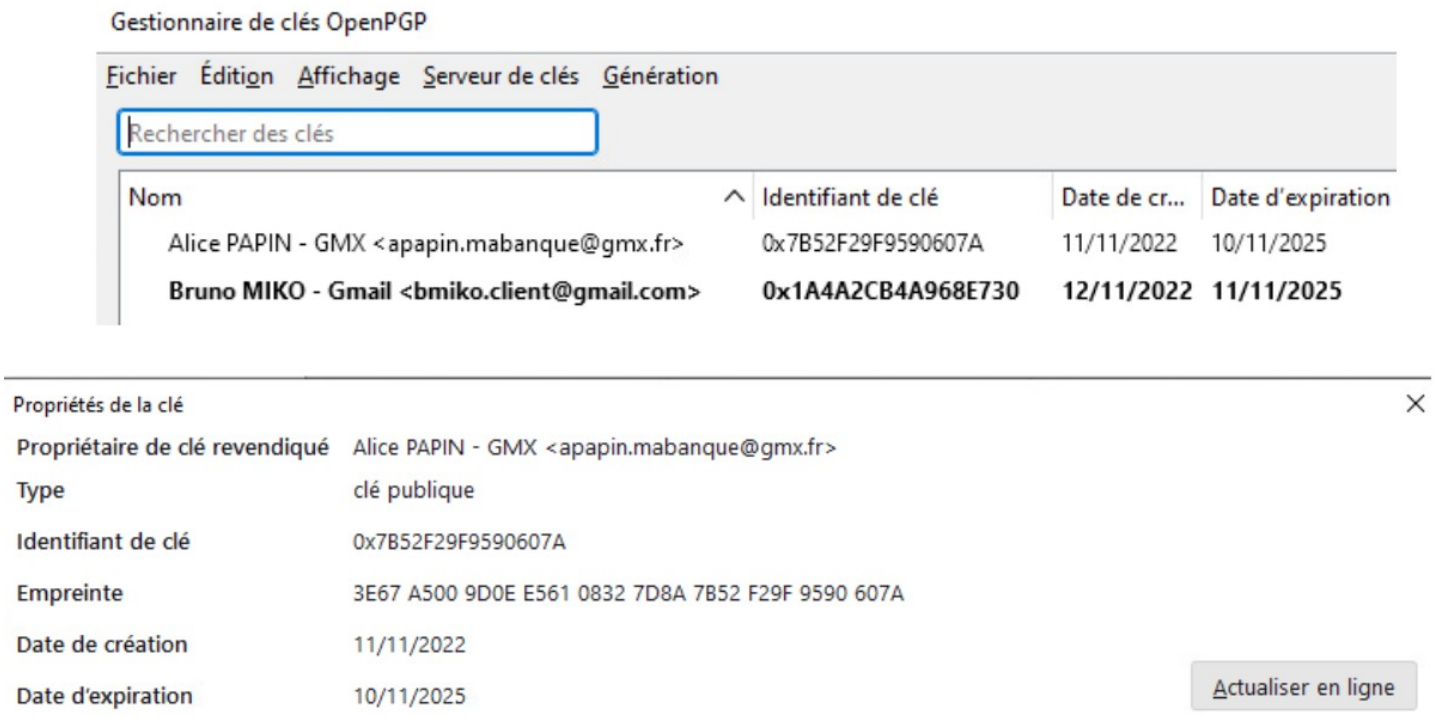

Figure 1: La clé publique du destinataire est bien importée (apapin.mabanque@gmx.fr) dans le compte de l'expéditeur (bmiko.client@gmail.com)

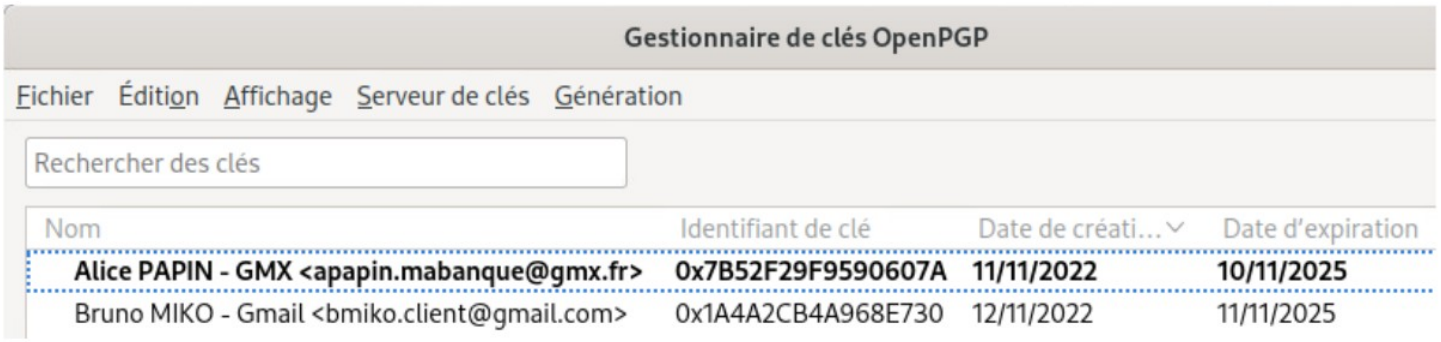

Figure 2: La clé publique du destinataire est bien importée (bmiko.client@gmail.com) dans le compte de l'expéditeur (apapin.mabanque@gmx.fr)

Critère 4

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

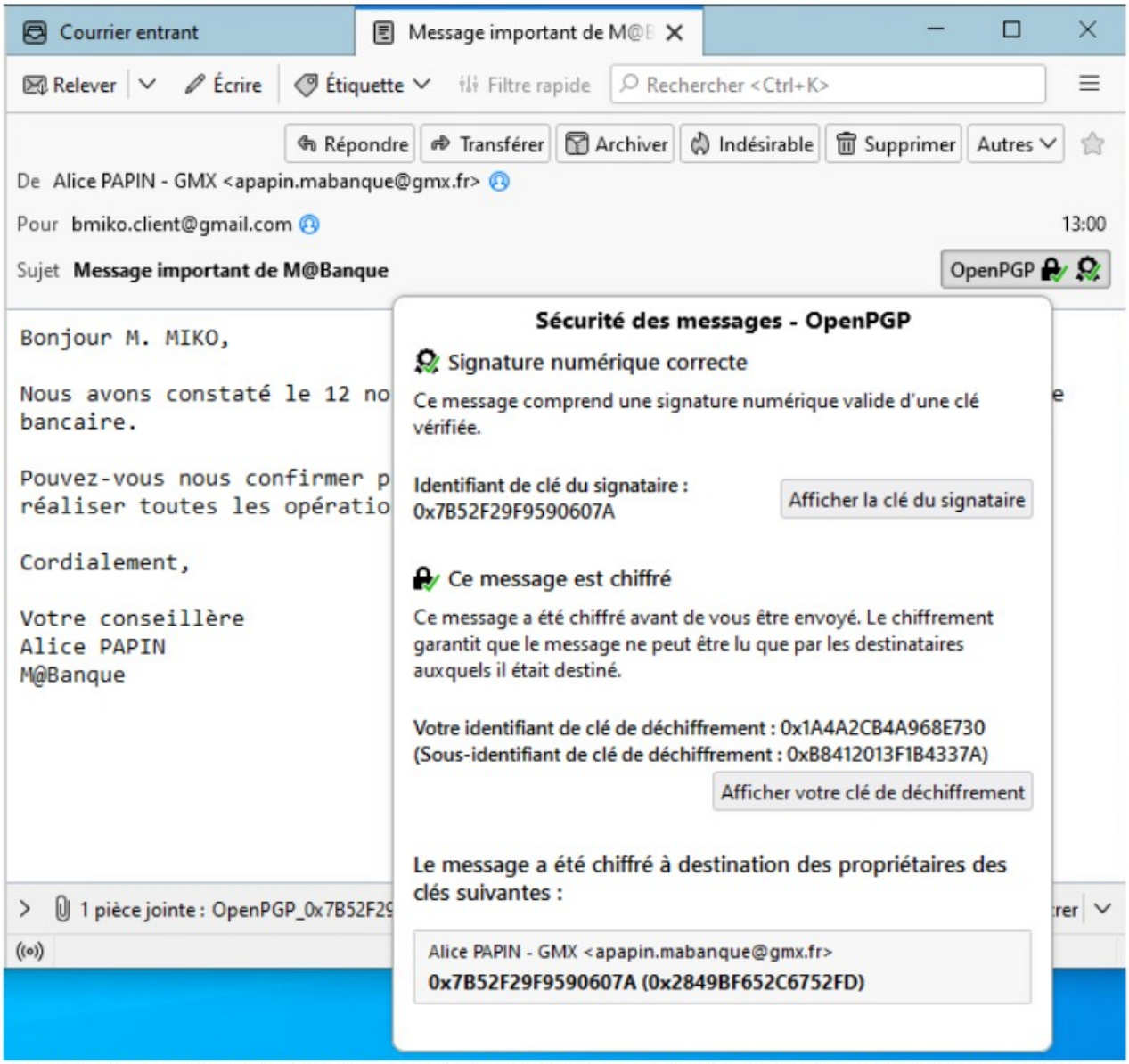

Figure 18: Le cadenas et le certificat d'OpenPGP ont une coche verte, ce qui prouve que le message est valide (non modifié) et que la signature a été reconnue. Le message chiffré par la banque a bien été déchiffré par la clé privée du client. La signature du message a été validée par la clé publique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

Critère 5

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

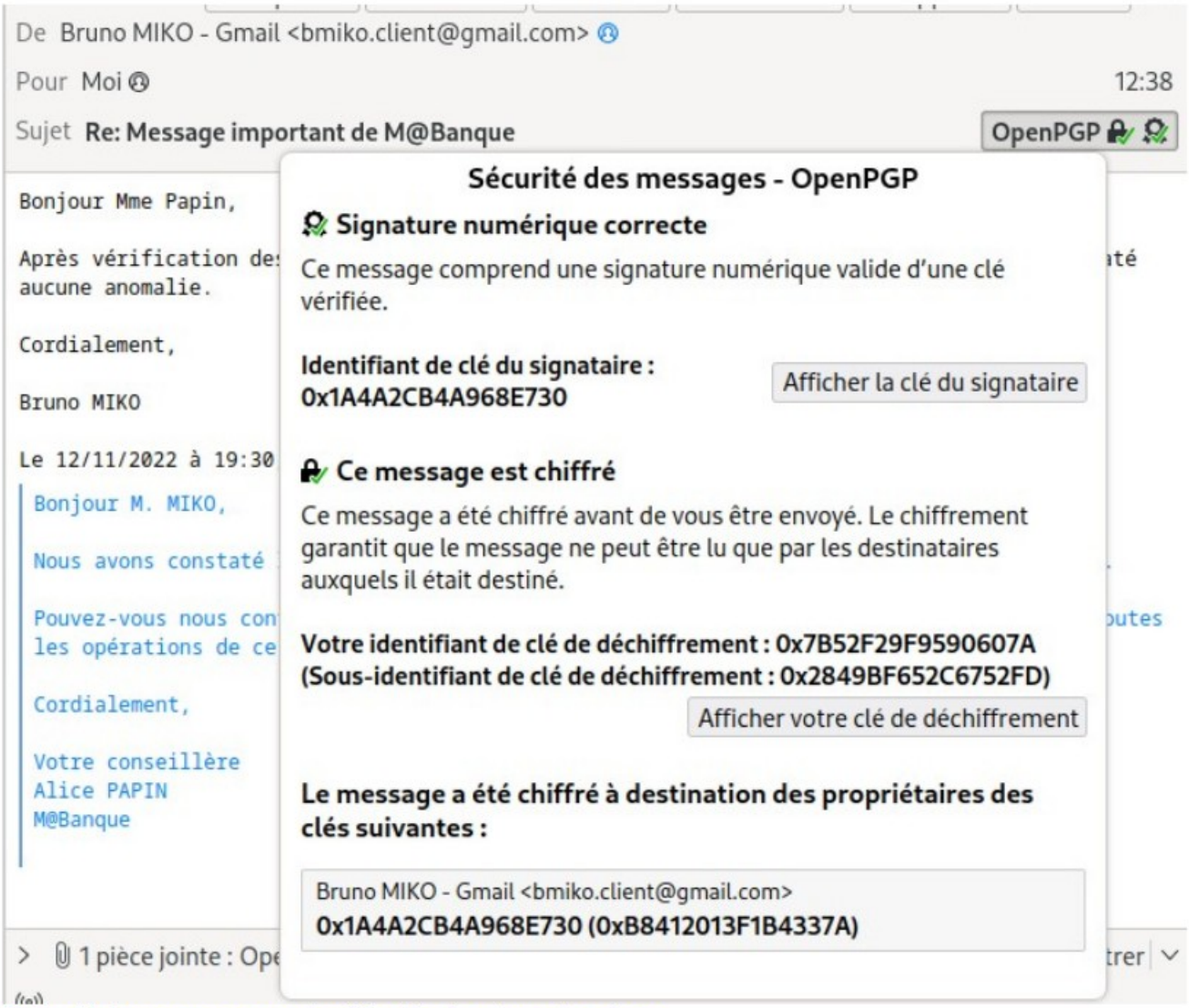

Figure 21: Le message reçu est valide et la signature est conforme

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)

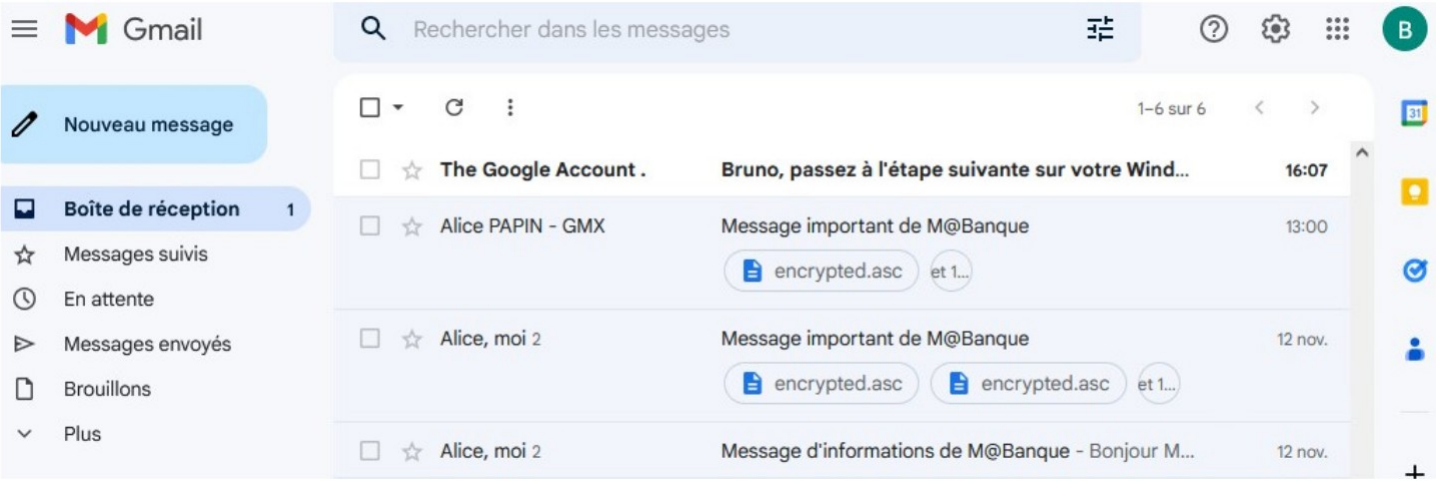

Figure 3: Le client ne peut pas lire les 2 premiers messages car ils sont chiffrés et le client de messagerie ne dispose pas des clés de déchiffrement.