Ruben Battocchio
20/01/2026

TP CH3-TD2

I. Introduction

Dans le cadre du renforcement des moyens de preuve électronique, il m'a été demandé de mettre en œuvre une solution de sécurisation des échanges de courriels. La technologie retenue est le chiffrement PGP (Pretty Good Privacy). L'objectif est de garantir la confidentialité (seul le destinataire peut lire) et l'authenticité (l'expéditeur est certifié) des messages échangés entre une banque et son client.

II. Environnement de test

Le test a été réalisé sur deux machines virtuelles Debian connectées en réseau local simulé.

Machine A (Banque) :
IP : 192.168.0.1
Compte : M@Banque

Machine B (Client) :
IP : 192.168.0.2

Compte : ClientM@Banque

III. Test de l’envoie non sécurisé

Dans un premier temps, un courriel standard a été envoyé du Client vers la Banque sans configuration PGP.

Observation : Le message est transmis en texte clair. Si ce message était intercepté sur le réseau (attaque "Man in the middle"), son contenu serait lisible immédiatement. Sur Thunderbird, aucune icône de sécurité n'apparaît.

IV. Mise en oeuvre du chiffrement PGP

Pour chaque utilisateur, j'ai accédé au menu Paramètres des comptes > Chiffrement de bout en bout. J'ai généré une nouvelle paire de clés OpenPGP (clé publique + clé privée).

- Clé M@Banque : Créée et active.
- Clé Client : Créée et active.

4.2. Échange des clés publiques

Pour que le chiffrement fonctionne, chaque interlocuteur doit posséder la clé publique de l'autre.

1. J'ai exporté la clé publique de "M@Banque" et je l'ai envoyée par mail au client.
2. Sur la machine du client, j'ai importé cette clé via le Gestionnaire de clés OpenPGP.
3. J'ai répété l'opération inverse pour le client vers la banque.

V. Test de l’envie sécurisé

J'ai réalisé un nouvel envoi de "M@Banque" vers le "Client". Lors de la rédaction, Thunderbird a détecté que je possédais la clé publique du destinataire.

Manipulations effectuées :

1. Rédaction du message.
2. Activation de l'option "Chiffrer" (Cadenas fermé) et "Signer numériquement" (Sceau/Rosette).
3. Envoi du message.

Réception côté Client : À la réception, le message affiche une bannière spécifique indiquant "OpenPGP : Chiffré".

VI. Signature numérique

La signature numérique garantit l'intégrité du message (il n'a pas été modifié) et l'authenticité de l'expéditeur (c'est bien lui qui l'a envoyé). Elle demande une démarche active (souvent la saisie d'une phrase de passe ou une validation explicite) car elle engage la responsabilité de l'expéditeur. Contrairement au chiffrement qui est une action technique de protection, la signature est l'équivalent numérique d'une signature manuscrite sur un contrat : elle valide le contenu comme étant approuvé par le détenteur de la clé privée.

VII. Conclusion

Les tests réalisés démontrent que l'utilisation du chiffrement PGP répond parfaitement au besoin de sécurisation des preuves:

1. Confidentialité : Sans la clé privée du destinataire, le message est illisible.
2. Preuve d'origine : La signature certifie que le message vient bien de la banque (non-répudiation).

L'environnement est donc conforme aux attentes pour échanger des documents sensibles.