

TD2 : Virtualisation du déploiement de moyens de preuve sécurisés et conformes à la législation

Introduction.....	2
1. Importation des machines virtuelles.....	2
2. Configuration des comptes de messagerie Thunderbird.....	3
3. Vérification du chiffrement des messages.....	4
4. Mise en place du chiffrement PGP.....	5
5. Nouvelle vérification.....	5
6. Signature numérique.....	6
Rapport.....	6

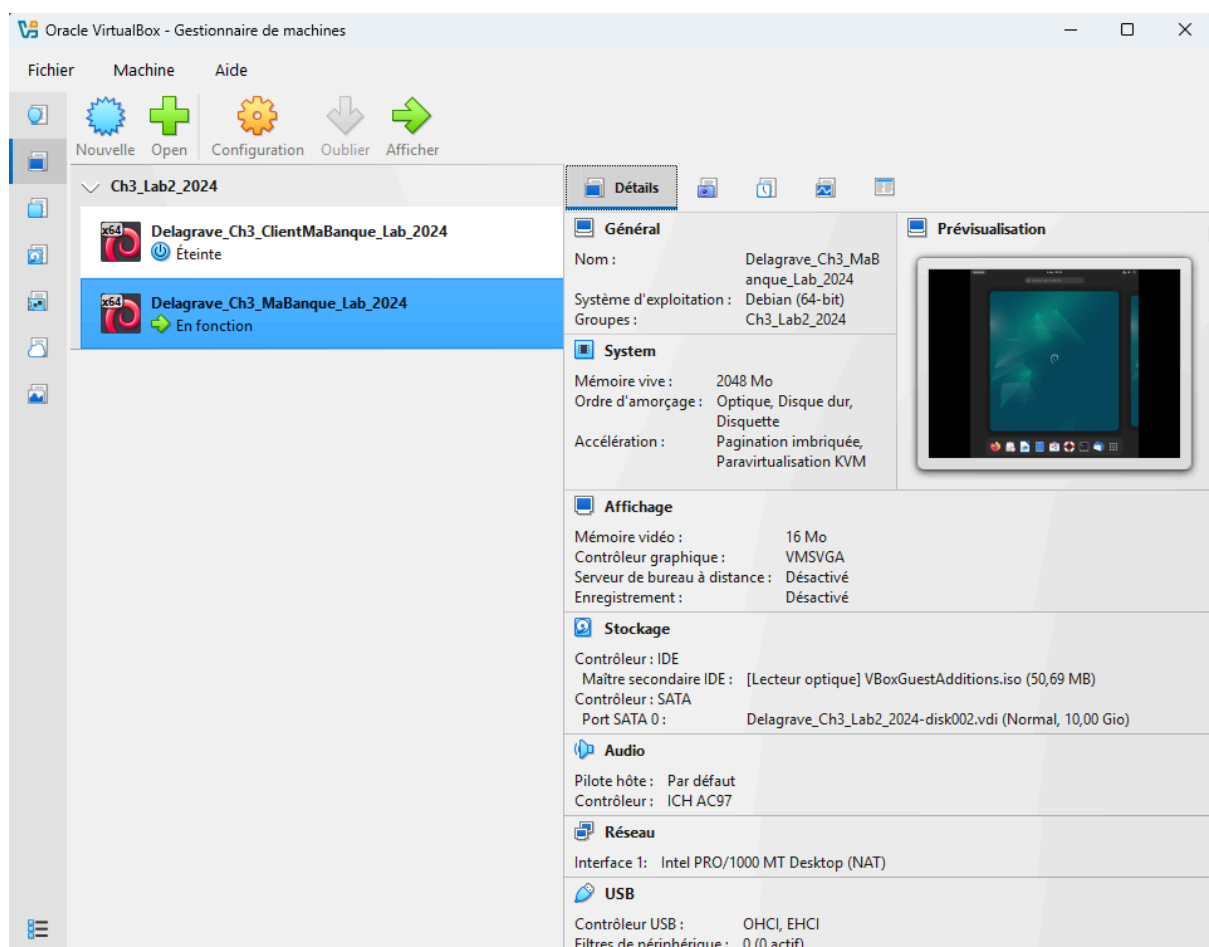
Introduction

Dans le cadre de ce travail dirigé, nous avons utilisé le logiciel VirtualBox afin de simuler un environnement de test. Ce dispositif permet de mettre en œuvre la technologie PGP et d'analyser les différentes étapes nécessaires à la sécurisation des échanges. L'objectif est d'évaluer les mécanismes permettant de renforcer la fiabilité et la conformité des moyens de preuve utilisés par une entreprise.

1. Importation des machines virtuelles

Pour exploiter les machines virtuelles, l'utilisation d'un logiciel de virtualisation est indispensable.

Dans ce contexte, VirtualBox a été choisi afin d'émuler correctement les deux environnements nécessaires aux tests.



2. Configuration des comptes de messagerie Thunderbird

Un compte de messagerie a été créé sur chaque machine virtuelle à l'aide de Thunderbird. Les adresses utilisées sont mabanque@gmail.com pour la machine bancaire et clientmabanque@gmail.com pour la machine cliente, avec les identités respectives **MaBanque** et **Client-MaBanque**.

The image shows two identical Thunderbird account configuration windows stacked vertically. Each window contains the following fields and options:

- Your full name:** A text input field containing 'Mabanque' (for the top window) or 'Client-MaBanque' (for the bottom window).
- Email address:** A text input field containing 'mabanque@gmail.com' (for the top window) or 'clientmabanque@gmail.com' (for the bottom window).
- Password:** A text input field containing 'mabanque' (for the top window) or 'clientmabanque' (for the bottom window).
- Remember password:** A checked checkbox.
- Buttons:** 'Configure manually' (blue text), 'Cancel' (grey button), and 'Continue' (blue button).

3. Vérification du chiffrement des messages

Un premier courriel a été envoyé de MaBanque vers Client-MaBanque afin de vérifier le niveau de sécurité. L'analyse du code source a montré que le contenu du message était lisible, indiquant l'absence de chiffrement.

Demande d'information compte courant

De: mabanque@gmail.com
Pour: clientmabanque@gmail.com
Date: 04 Décembre 2025 à 10:15

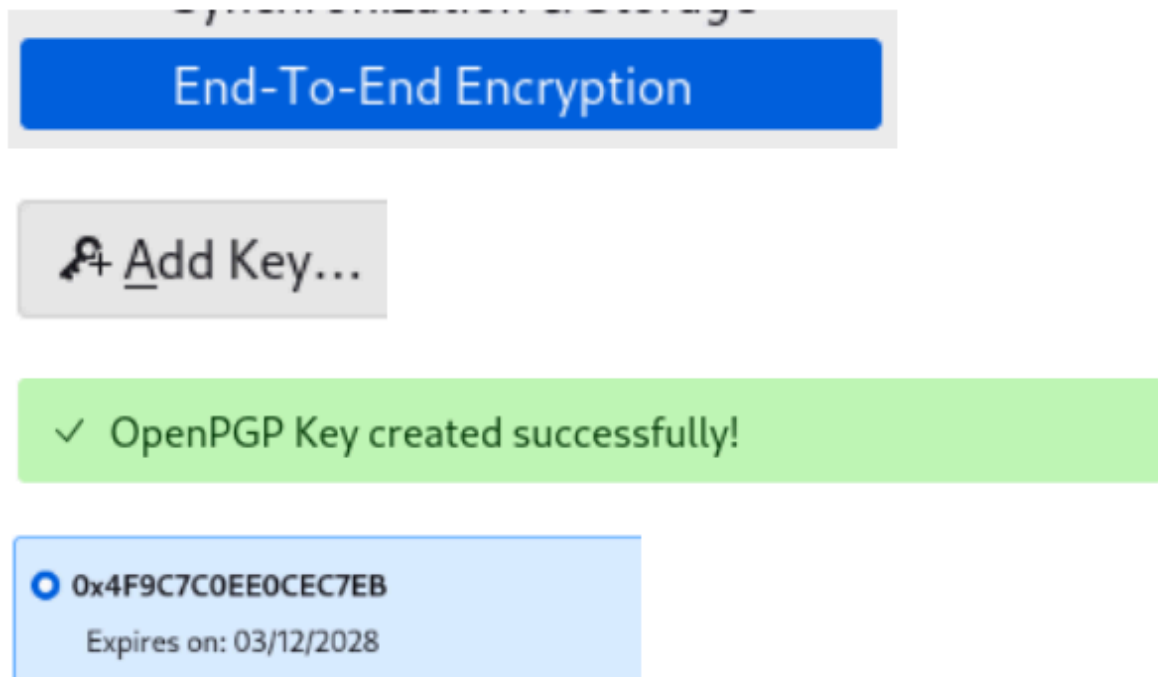
```
MIME-Version: 1.0
Date: Thu, 04 Dec 2025 10:15:00 +0100
From: mabanque@gmail.com
To: clientmabanque@gmail.com
Subject: Demande d'information compte courant
Content-Type: text/plain; charset=UTF-8

Bonjour,
Suite à votre appel, je vous confirme que les documents demandés seront envoyés par courrier postal.

Cordialement,
Votre Conseiller
```

4. Mise en place du chiffrement PGP

Le chiffrement des messages a ensuite été configuré pour les deux utilisateurs afin de sécuriser les échanges.



5. Nouvelle vérification

Après activation du chiffrement, le contenu du message devient illisible dans le code source, confirmant que la protection PGP est bien opérationnelle.



6. Signature numérique

La signature numérique garantit à la fois l'authenticité de l'expéditeur et l'intégrité du message. Elle repose sur l'utilisation d'une clé privée protégée par un mot de passe. Lors de l'envoi, l'utilisateur doit saisir ce mot de passe afin de déverrouiller la clé et permettre la signature du message

Rapport

Des tests ont été réalisés sur Thunderbird afin de vérifier l'efficacité de PGP pour sécuriser les échanges et fournir des preuves fiables. Lors d'un premier envoi sans protection, le message était totalement lisible, ce qui démontre qu'un courriel classique peut être intercepté et modifié. Lors du second test, le chiffrement PGP a été activé à l'aide d'une clé dédiée. Le contenu est alors devenu illisible et une signature numérique valide a été détectée, assurant l'authenticité et l'intégrité du message.