Fadi ALOUANI

BTS SIO 1
groupe 1
B3
20/11/25

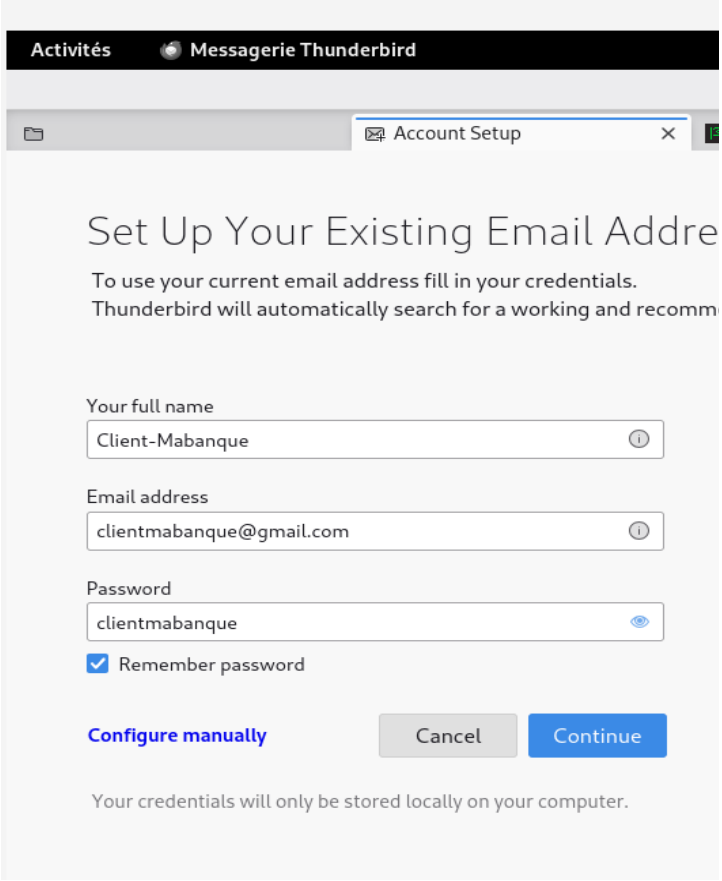
TH2 : CH3 TD2

Sommaire

Introduction

L'objectif de ce TP est de mettre en place un environnement sécurisé permettant l'échange de courriels chiffrés entre deux utilisateurs, en utilisant Thunderbird et OpenPGP.
Nous devons configurer deux machines virtuelles Debian, créer des comptes mail, échanger des clés publiques et envoyer des messages chiffrés pour démontrer l'intérêt de PGP dans les moyens de preuve électroniques.

Paramétrage des compte de messagerie client sur Thunderbird sur les deux machines.



Paramétrage du chiffrement de bout en bout des message pour les deux utilisateur

Importation des deux machines virtuelles

Les machines virtuelles “M@Banque” et “ClientM@Banque” ont été importées dans VirtualBox

Les identifiants fournis :

- Machine M@Banque
  - identifiant : mabanque
  - mot de passe : mabanque
- Machine Client
  - identifiant : clientmabanque
  - mot de passe : clientmabanque

Configuration des comptes Thunderbird
Création des adresses mail

Fadi ALOUANI

- Sur M@Banque : mabanque@gmail..com
- Sur ClientM@Banque : clientmabanque@gmail.com

Configuration dans Thunderbird

- Ajout d'un compte de messagerie
- Choix de la langue française dans les paramètres

Test d'envoi de courriel

Un premier échange de mails est effectué pour vérifier la communication entre les deux acteurs.

Résultat : les messages s'envoient correctement mais le contenu n'est pas sécurisé.

Mise en place du chiffrement OpenPGP
Génération d'une paire de clés
Dans Thunderbird :
Paramètres → Confidentialité et sécurité → OpenPGP → "Générer une nouvelle clé".

Chaque utilisateur génère :

- une clé publique
- une clé privée

Exportation et envoi de la clé publique
Chaque destinataire reçoit la clé publique de l'autre via un mail.
Représentation du menu Thunderbird (Document 3)

Importation de la clé publique du correspondant
Dans Thunderbird → Gestionnaire OpenPGP → Importer la clé reçue.

Test d'envoi de courriels chiffrés

Après importation des clés, un message est envoyé avec :
chiffrement
signature numérique

Éléments permettant de vérifier que l'envoi est sécurisé :

- Icône indiquant que le message est chiffré
- Icône indiquant que le message est signé numériquement
- Dans les en-têtes : "Message chiffré à l'aide de OpenPGP"
- Le contenu du mail n'est lisible qu'après déchiffrement par la clé privée du destinataire

Fadi ALOUANI

Pourquoi la signature numérique nécessite-t-elle une action de l'utilisateur ?

La signature numérique garantit :

- l'authenticité du message (l'expéditeur est bien celui qu'il prétend être)
- l'intégrité (le message n'a pas été modifié)
- la non-répudiation (l'expéditeur ne peut pas nier l'avoir envoyé)

Pour ces raisons, l'utilisateur doit explicitement signer le message avec sa clé privée.
Cela implique un acte volontaire, car la clé privée représente juridiquement son identité numérique.

Conclusion

intérêt de PGP dans les moyens de preuve sécurisés
L'utilisation du chiffrement PGP dans Thunderbird permet :

- de garantir la confidentialité des échanges
- de signer les messages pour prouver l'authenticité et l'origine
- de détecter toute modification du contenu (intégrité)
- d'assurer une non-répudiation, essentielle dans les échanges avec une banque ou un client

Ainsi, la mise en œuvre de PGP renforce de manière significative les moyens de preuve électroniques, tout en répondant aux exigences légales concernant la cybersécurité et la protection des données.