Rapport : Cryptographie.

# Une image contenant texte Description générée automatiquementConfiguration GPG :

# Clé GPG :

D’abord, je vérifie si j’ai déjà des clés :

gpg -K 🡪 vérifie s’il existe des clés privées

gpg -k 🡪 vérifie s’il existe des clés publiques

gpg –full-generate-key 🡪 va générer les clés.

Ensuite, différentes choses sont demandées :

Le type de clé voulu : j’ai choisi la 1 (RSA)

La taille de la clé : 4096 bits

Le temps de conservation de la clé : 0 (zéro pour dire qu’elle n’expire jamais)

Confirmation de mes choix : y

Mon nom réel : Fabrice Bodson

Mon email : [fa.bodson@student.helmo.be](mailto:fa.bodson@student.helmo.be)

Un commentaire : rien du tout

Vérification des données fournies : O(ui)

Entrée d’un mot de passe de 20 caractères qui protège la clé (créé via Dashlane).

Vérification que les clés ont bien été créées avec les commandes :

gpg -K

gpg -k

modification de la clé avec la commande :

gpg --edit-key *id\_de\_la\_clé*

gpg affiche les détails de la clé qu’on modifie.

La lettre S veut dire que je peux signer des documents. C certifie une signature de quelqu’un d’autre.

E veut dire que la clé ne sert que pour du chiffrement.

Création d’une sous-clé qui permette de signer des documents (pour ne plus utiliser la clé maitre que pour la création d’autres sous-clés).

Création au moyen de la commande :

addkey

La marche à suivre est la suivante :

Le type de clé voulu : j’ai choisi la 4 (RSA)

La taille de la clé : 4096 bits

Le temps de conservation de la clé : 0 (zéro pour dire qu’elle n’expire jamais)

Confirmation de mes choix : y

Entrée du mot de passe

Création d’un certificat de révocation :

Gpg –output *chemin* –gen-revoke *id\_de\_la\_clé\_maitre*

Je confirme que je souhaite créer un certificat de révocation : y

La raison : 1 (clé compromise)

Pas de description.

Entrée du mot de passe.

# Utilisation GPG :

Création d’un document :

Touch document.txt

Insertion d’un paragraphe :

Nano document.txt

Chiffrement du document :

gpg -c ~/document.txt

Fichier « ~/document.txt.gpg » créé.

Déchiffrement du message et insertion du résultat dans « document.txt »:

gpg -d ~/document.txt.gpg > ~/document.txt

Signature du fichier « document.txt » :

gpg --clearsign ~/document.txt

Fichier « ~/document.txt.gpg.asc » créé.