# **Installation et configuration pour SSH.**

# Présentation.

Le **SSH** (Secure SHell) est un protocole permettant la connexion sur une machine distante à travers un tunnel sécurise.  
Nous allons l'installer, puis le configurer sur un serveur pour permettre la gestion de ce serveur à distance, à travers internet par exemple.

# Fonctionnement.

Il garantit que seuls les utilisateurs autorisés peuvent se contacter et se comprendre. Il se base sur ces deux grands axes qui sont :

## Authentification

Permet de vérifier que les deux intervenants sont ceux attendus. Le serveur commence par envoyer un certificat, le client Après que les deux machines se soient identifiées mutuellement.

## Chiffrement

Après la validation de l'authentification, le serveur et le client génère une clef commune pour chiffrer les échanges, et négocie aussi un algorithme de hashage pour vérifier l'intégrité des données.

# Installation.

Sous environnement Debian 11, l’installation se fait de la façon suivante :

|  |
| --- |
| $ sudo apt install openssh-server |

On vérifie le statut de notre service avec la commande :

|  |
| --- |
| $ sudo systemctl status |

# Configuration.

Création des clés.  
Pour permettre l’authentification on va commencer par créer un groupe et un utilisateur spécifique à la manipulation des clefs.  
Creation

# Création du répertoire ou seront stockées les clefs.  
$sudo mkdir –p /etc/ssh/keys  
# Création de notre clefs privée et publique.  
$sudo ssh-keygen –t ed25519 –b 521 –f /etc/ssh/keys/server.key  
Generating public/private ed25519 key pair.

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /etc/ssh/keys/server.key

Your public key has been saved in /etc/ssh/keys/server.key.pub

The key fingerprint is:

SHA256:Tp+TBTRHlb2H9mj6ZdB+DwKZdUyG9/re3md7dLGbU0o root@linux

The key's randomart image is:

La configuration globale se fait à l’aide du fichier /etc/ssh/sshd\_config.  
Pour des raisons de sécurités on va modifier le port d’écoute par défaut et le remplacer par   
60001, et écouter sur l’adresse 192.168.1.25.