**MobaXterm et clés SSH**

Une paire de clés SSH (*Secure Shell*) permet d’établir une connexion sécurisée sur un réseau qui ne l’est pas (dont le réseau Internet).

Une paire de clé SSH est composée de deux entités …

* Une clé publique qui est à la disponibilité de tous ;
* Une clé privée qui est, quant à elle, gardée secrète.   
  Cette clé privée est utilisée pour le déchiffrement de messages chiffrés à l'aide d'une clé publique correspondante.

L'avantage d'utiliser une clé SSH lors des connexions entre hôtes distants est que seulement la clé publique nécessite d'être échangée sur le réseau où les données transitent.   
Les transmissions chiffrées avec une clé publique peuvent uniquement être décodées avec la clé privée correspondante et un mot de passe.   
Seule la clé publique est échangée sur le réseau.   
Le mot de passe correspondant à la clé secrète est quant à lui maintenu secret.

MobaXterm permet de gérer l’authentification par échange de clé SSH avec les **algorithmes …**

* **RSA** ;
* **DSA** ;
* **ECDSA** ;
* **ed25519**   
  et
* **SSH1** (RSA).

**Remarque** …  
Ce tutoriel est pour une connexion SSH pour l’utilisateur tux.

**Génération des clés**

|  |  |
| --- | --- |
| Accéder à l’utilitaire MobaXTerm  Sélectionner le menu  Tools -->  MobaKeyGen SSH (SH Key Generator)  Sélectionner le type ainsi que  la longueur des clés  Confirmer en cliquant sur Generate |  |

|  |  |
| --- | --- |
| L’utilitaire commence à générer les clés  Remarque ... Le fait de déplacer la souris sur la surface grise du générateur de clés permet de générer des données aléatoires afin de créer des clés uniques. Le fait de déplacer le pointeur de la souris permet de générer plus rapidement les clés.  La génération de la clé terminée, la clé publique est affichée dans sous la rubrique Key  Comme indiqué, cette clé devra être copiée dans le répertoire ~/.ssh/authorized\_keys  sur le serveur  Il est possible de préciser un mot de passe dans le champ Key passphrase  Ce mot de passe sera demandé lors de la connexion au serveur SSH distant Ceci permet une double authentification  (clé et mot de passe) | Une image contenant texte  Description générée automatiquement  Une image contenant texte  Description générée automatiquement |

**Sauvegarde des clés**

|  |  |
| --- | --- |
| La paire de clé étant générée, il faut la sauvegarder  On sélectionne les boutons save private key et save private key afin de sauvegarder les fichiers des clés privée et publique dans un dossier sûr de l’hôte local |  |

**Copie de la clé publique sur le serveur SSH**

|  |  |
| --- | --- |
| Pour copier la clé publique qui vient d’être générée sur le serveur SSH distant, il faut se connecter (en tant que tux) dans un premier temps se connecter à ce serveur  Accéder, avec un éditeur (vim ou nano), au fichier ~/.ssh/authorized\_keys  Remarque … Il faut créer ce fichier et ce répertoire s’ils sont absent sur le serveur distant  Copier/coller le contenu de clé SSH publique qui se trouve dans la section key Ce contenu débute par ssh-rsa, ssh-dsa,  ssh-ecdsa, …  Enregistrer le contenu du fichier authorized\_keys | Une image contenant texte  Description générée automatiquement |

**Connexion sur le serveur**

|  |  |
| --- | --- |
| À partir de maintenant,  MobaXterm va utiliser cette clé afin de se connecter sur le serveur distant |  |

.

|  |  |
| --- | --- |
| Pour copier la clé publique qui vient d’être générée sur le serveur SSH distant, il faut se connecter (en tant que tux) dans un premier temps se connecter à ce serveur  Accéder, avec un éditeur (vim ou nano), au fichier ~/.ssh/authorized\_keys  Remarque … Il faut créer ce fichier et ce répertoire s’ils sont absent sur le serveur distant  Copier/coller le contenu de clé SSH publique qui se trouve dans la section key Ce contenu débute par ssh-rsa, ssh-dsa,  ssh-ecdsa, …  Enregistrer le contenu du fichier authorized\_keys | Une image contenant texte  Description générée automatiquement |