

LES CLÉS SSH

1 - Généralités

1.1 – Les clés privées & clés publiques

Quand vous travaillez avec des clés asymétriques, par principe, vous avez deux clés (on parle de **paire** de clés) : une **clé publique**, que vous pouvez diffuser librement, voire mettre à disposition sur un serveur de clés ; et une **clé privée**, qui constitue véritablement votre « identité », et ne doit **jamais** être diffusée : elle reste simplement présente dans votre dépôt de clés personnel, ou sur votre ordinateur.

Une paire de clé permet donc de vous représenter vis-à-vis d'un système tiers, en lui fournissant à l'avance votre clé publique, pour ensuite communiquer avec lui à l'aide de votre clé privée ; puisque seules les clés d'une même paire peuvent se comprendre, le système distant est à même non seulement de vérifier que vous êtes bien celui (ou celle) que vous prétendez être, mais aussi que ce qu'il reçoit est bien ce que vous envoyez.

1.2 – SSH

OpenSSH est une version libre de la suite de protocole de SSH, des outils de connectivité de réseau sur lesquels un nombre croissant de personnes sur l'Internet viennent s'appuyer.

Beaucoup d'utilisateurs de Telnet, Rlogin, FTP, ou d'autres programmes de même acabit ne se rendent pas compte que leur données, et notamment les mots de passe, **sont transmis à travers les réseaux en clair** ce qui constitue une faille évidente dans la sécurité de leur réseau.

OpenSSH chiffre tout le trafic (mots de passe y compris), via une combinaison astucieuse de chiffrement symétrique et asymétrique. Il fournit également d'autres méthodes d'authentification alternatives au traditionnel mot de passe. Comme son nom l'indique, OpenSSH est développé dans le cadre du projet [OpenBSD](#)

SSH remplace de manière sécurisée :

- Telnet: Vous pouvez exécuter des commandes depuis un Réseau Local ou Internet via SSH

- FTP: Si vous ne souhaitez qu'ajouter ou modifier des fichiers sur un serveur, SSH est bien plus adapté que FTP

SSH permet de faire, en usage de base :

- Accès à distance sur la console en ligne commande (shell), ce qui permet, entre autres, d'effectuer la totalité des opérations courantes et/ou d'administration sur la machine distante.
- Déporter l'affichage graphique de la machine distante.
- Transferts de fichiers en ligne de commande.

SSH est installé **NATIVEMENT** sur Linux et sur Mac. Pour Windows vous devrez utiliser des logiciels tels que [Putty](#) ou [Bitvise SSH Client](#) qui possède, lui, une interface de transfert de fichier en SFTP (FTP Sécurisé)

2 – Générer ses propres clés

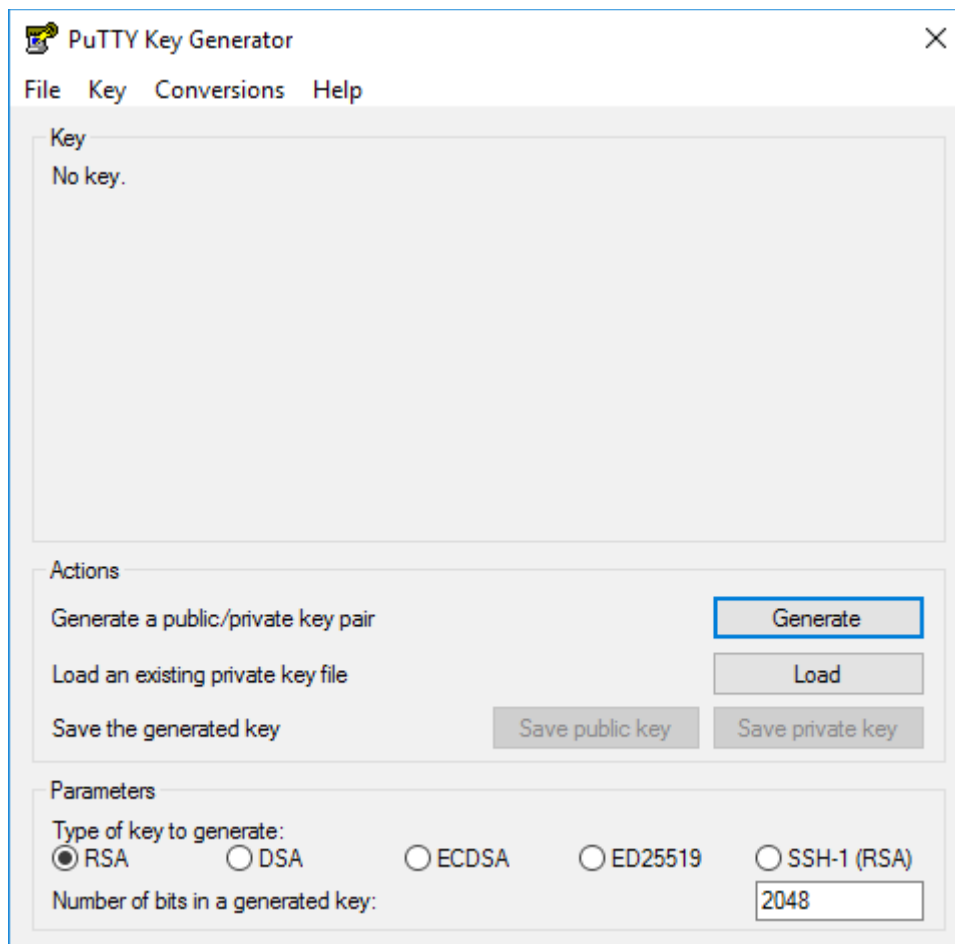
2.1 – Sous Linux

Beaucoup plus simple que sous Windows, SSH étant natif. Je vous renvoie sur le site de [Github](#) qui l'explique très bien !

2.2 – Sous Windows

SSH n'étant pas natif sous Windows, nous utiliserons un logiciel supplémentaire fourni par Putty appelé [Puttygen](#) (déjà installé si vous avez utilisé l'installateur de Putty). Il est, comme son nom l'indique, un générateur de clé [RSA](#) et [DSA](#) destiné à être utilisé par PuTTY lui-même, PSCP, et Plink, ainsi qu'avec Pageant, l'agent d'authentification de PuTTY. Il permet également de convertir une clé au format Putty.

Lorsque vous lancez PuTTYgen, vous obtenez une fenêtre où vous avez le choix entre '**Generate**' (générer une nouvelle paire de clés), ou '**Load**' pour charger une clé privée existante.



2.2.1 – Génération d’une nouvelle clé

Avant de générer une paire de clés à l'aide de PuTTYgen, vous devez choisir un type de clé. PuTTYgen reconnaît actuellement trois types de clés :

- Clés RSA à utiliser avec le protocole SSH-2.
- Clés DSA à utiliser avec le protocole SSH-2.
- Clés RSA à utiliser avec le protocole SSH-1.

La plupart du temps vous utiliserez le format RSA (SSH-2), d'ailleurs les développeurs de PuTTY conseillent **fortement** d'utiliser RSA.

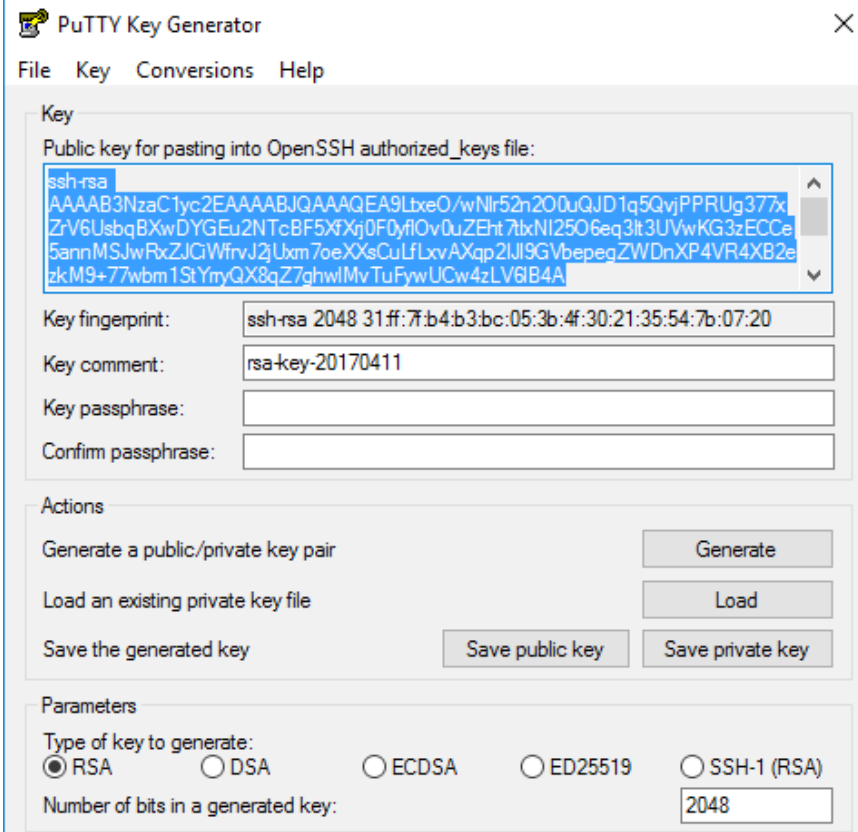
2.2.2 – Choix de la taille de la clé

Sujet qui porte à débat ... Beaucoup préconisent de ne pas hésiter à générer des clés de 4096 (plus la taille de la clé est importante, plus elle est robuste). l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) recommande elle une taille de minimum 2048 (cf recommandations [livre blanc de 2014](#))

La taille est à saisir en bas à la ligne « **Number of bits in a generated key** »

2.2.3 – Génération de la clé

Il suffit simplement de cliquer sur le bouton « **Generate** » et de bouger comme indiqué votre souris ce qui permet de générer grace à ce mouvement des bits aléatoires. N'hésitez pas à faire des ronds ou des zig-zag !!!!! Et voila, notre clé est générée !



The screenshot shows the PuTTY Key Generator application window. The 'Key' section displays a public key for pasting into an OpenSSH authorized_keys file. The key is an RSA key with a 2048-bit size. The key fingerprint is shown as 'ssh-rsa 2048 31:ff:7:b4:b3:bc:05:3b:4f:30:21:35:54:7b:07:20'. The key comment is 'rsa-key-20170411'. The key passphrase and confirm passphrase fields are empty. The 'Actions' section contains buttons for 'Generate', 'Load', 'Save public key', and 'Save private key'. The 'Parameters' section shows the 'Type of key to generate' set to 'RSA' and the 'Number of bits in a generated key' set to '2048'.

PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa  
AAAAB3NzaC1yc2EAAAABJQAAQEA9LxeO/wNlr52n200uQJD1q5QvjPPRUg377x  
ZrV6UsbqBXwDYG Eu2NTcBF5XfXj0F0yflOv0uZEht7bXNI25O6eq3lt3UVwKG3zECCe  
5annMSJwRxZJGwfrvJ2Uxm7oeXXsCuLfLxvAXqp2JI9GVbepegZWDnXP4VR4XB2e  
zkM9+77wbm1StYryQX8qZ7ghwlMvTuFywUCw4zLV6B4A
```

Key fingerprint: ssh-rsa 2048 31:ff:7:b4:b3:bc:05:3b:4f:30:21:35:54:7b:07:20

Key comment: rsa-key-20170411

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate:
☒ RSA ☐ DSA ☐ ECDSA ☐ ED25519 ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048

2.2.4 – La ligne « Key fingerprint »

C'est « l'empreinte de votre clé » générée à partir de la valeur de la clé publique, elle n'a donc pas besoin d'être sécurisée. Gardez la tout de même de côté, elle vous servira par exemple pour Github.

2.2.4 – La ligne « Key comment »

Comme son nom l'indique, elle sert de commentaire au cas où vous auriez plusieurs clés. En cas de doute laissez le commentaire par défaut.

2.2.5 – La ligne « Key passphrase »

Sans doute la ligne la plus importante. C'est un mot de passe permettant de sécuriser votre clé privée avant de l'écrire sur votre disque. Je vous conseille **FORTEMENT** de remplir ce champ au cas où vous vous fassiez voler votre clé privée, par exemple ... N'hésitez pas à utiliser un générateur de mot de passe (Google est votre ami!) et d'utiliser un mot de passe **fort**, le prénom de vos enfants ou de votre animal de compagnie est à **PROSCRIRE** .. Règle simple : choisissez des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).

(Cf [recommandations ANSSI](#))

N'oubliez pas votre passphrase, Il n'y a pas moyen de le retrouver.

2.2.6 – Sauvegarde de vos clés

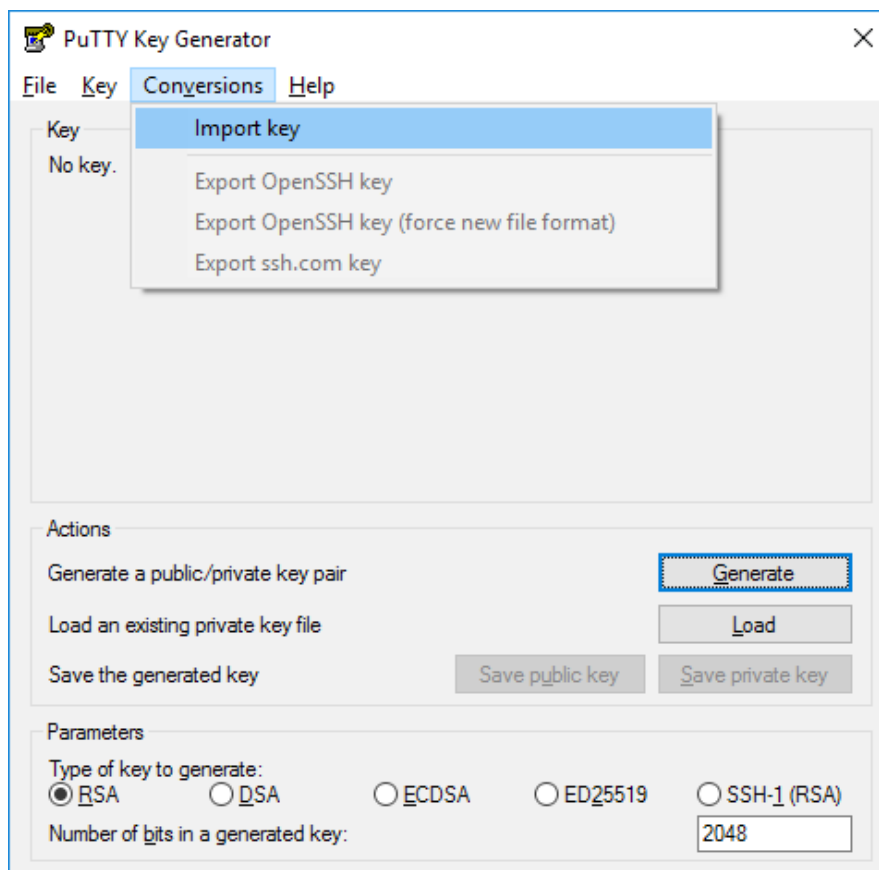
Il suffit juste de cliquer sur « Save public key » pour sauvegarder votre clé publique, et « Save private key » pour la clé privé ! Attention tout de même à l'endroit où vous les sauvegardez, le bureau de Windows est à mon avis une très mauvaise idée !

3 – Conversion d'une clé privé au format Putty

Il se peut qu'une clé privé ne soit pas au format Putty (par exemple si l'on vous fourni une clé générée sous linux). Le bon format doit posséder l'extension « .ppk » (Putty Private Key).

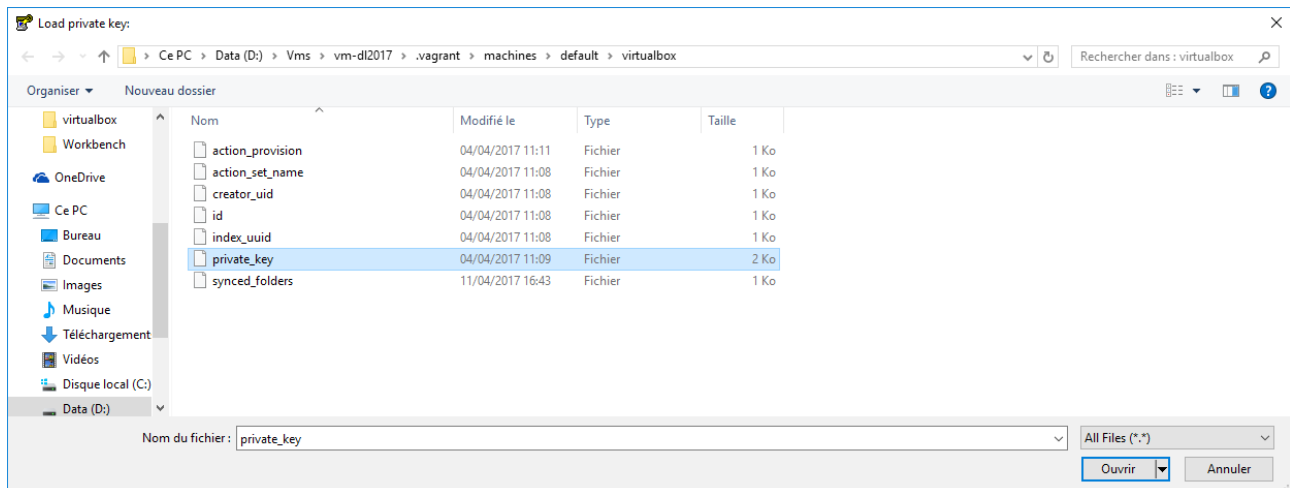
Nous allons prendre l'exemple d'une clé générée par Vagrant.

Cliquez sur « Conversions » puis « Import Key »



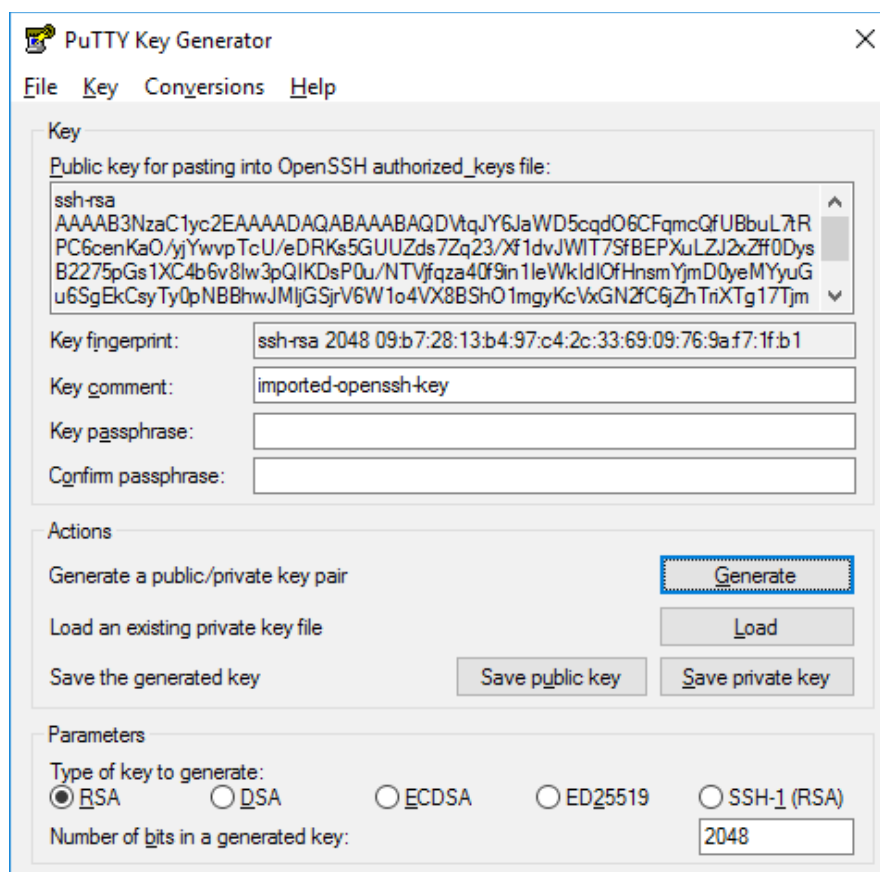
Choisissez l'emplacement du fichier « private_key », dans notre exemple

« D:\Vms\vm-dl2017\.vagrant\machines\default\virtualbox »



cliquez sur « Ouvrir » et voila, votre clé privé est importée

ATTENTION : Il se peut que un mot de passe vous soit demandé, c'est le fameux « passphrase » que nous avons vu plus haut !



Il ne vous reste plus qu'à cliquer sur « Save private Key » et le tour est joué !