

## 4. Créer votre paire de clés

Pour effectuer un envoi via SFTP, vous avez besoin d'une paire de clés SSH. Vous devez la créer vous-même.

Dans certains clients SFTP est compris un générateur de clé.

Si le client que vous avez choisi ne dispose pas d'un générateur de clé, vous devrez créer les clés via un autre générateur de clés que vous pouvez trouver facilement via une recherche sur internet. Le programme Putty Key Generator fonctionne très bien. Vous pouvez le retrouver en utilisant « puttygen » dans un moteur de recherche.

Votre clé publique doit être chargée lors de l'ouverture du canal SFTP sur le portail de la sécurité sociale.

Votre clé privée doit être chargée dans le client sftp que vous utilisez. Veuillez pour cette action consulter la documentation de votre client SFTP. Il est conseillé de protéger votre clé privée avec un mot de passe.

### **Spécifications:**

#### **Format**

Une distinction est faite entre les clés qui sont compatibles avec la version 1 de SSh et celles qui sont compatibles avec la version 2. La version 1 est considérée comme peu sûre et ne sera pas acceptée.

En plus il y a différents formats pour les clés publiques. Les plus courants sont ceux du logiciel OpenSSH et SSH. (La mise en application commerciale de SSH-protocol). Pour les clés publiques, les formats de OpenSSH et de SSH seront soutenus uniquement.

#### **L'algorithme & la longueur**

Lors de la génération des clés, vous devez faire attention au fait d'avoir choisi le type et la longueur correcte.

Il y a deux types possibles (RSA et DSA) dont seuls les RSA seront acceptés.

Comme longueur de clé, choisissez 2048 ou plus (3072, 4096). Les clés plus courtes ne seront pas acceptées.

Nous vous invitons à protéger votre clé privée par un mot de passe lorsque vous la sauvez sur votre machine.

### **Bref résumé:**

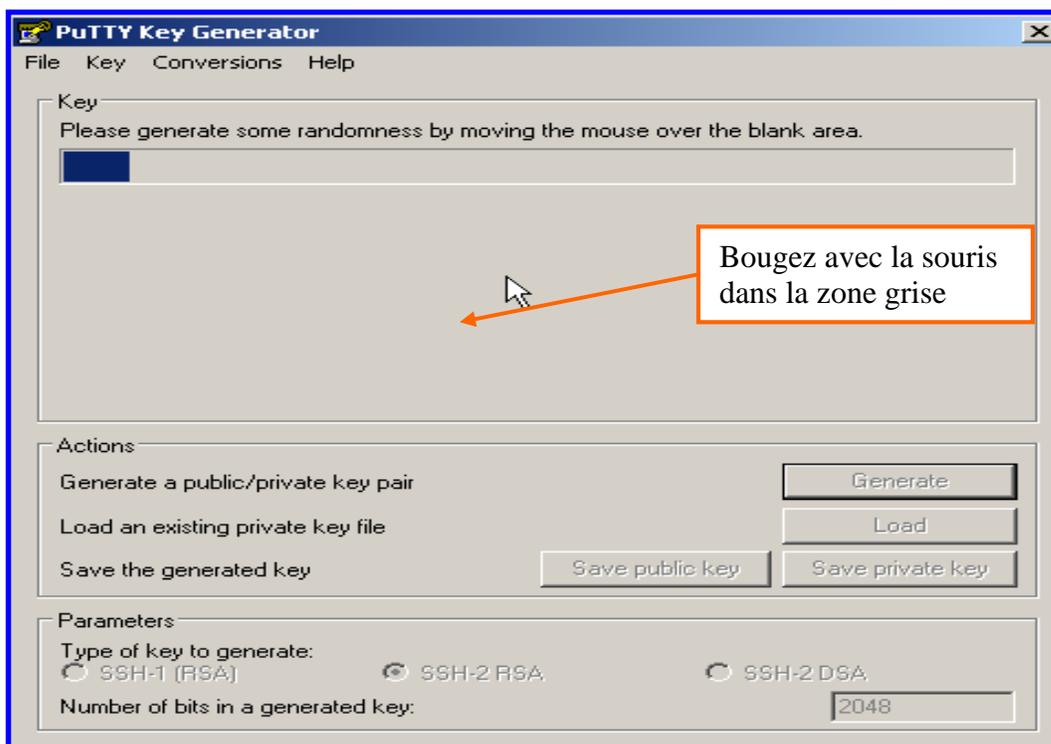
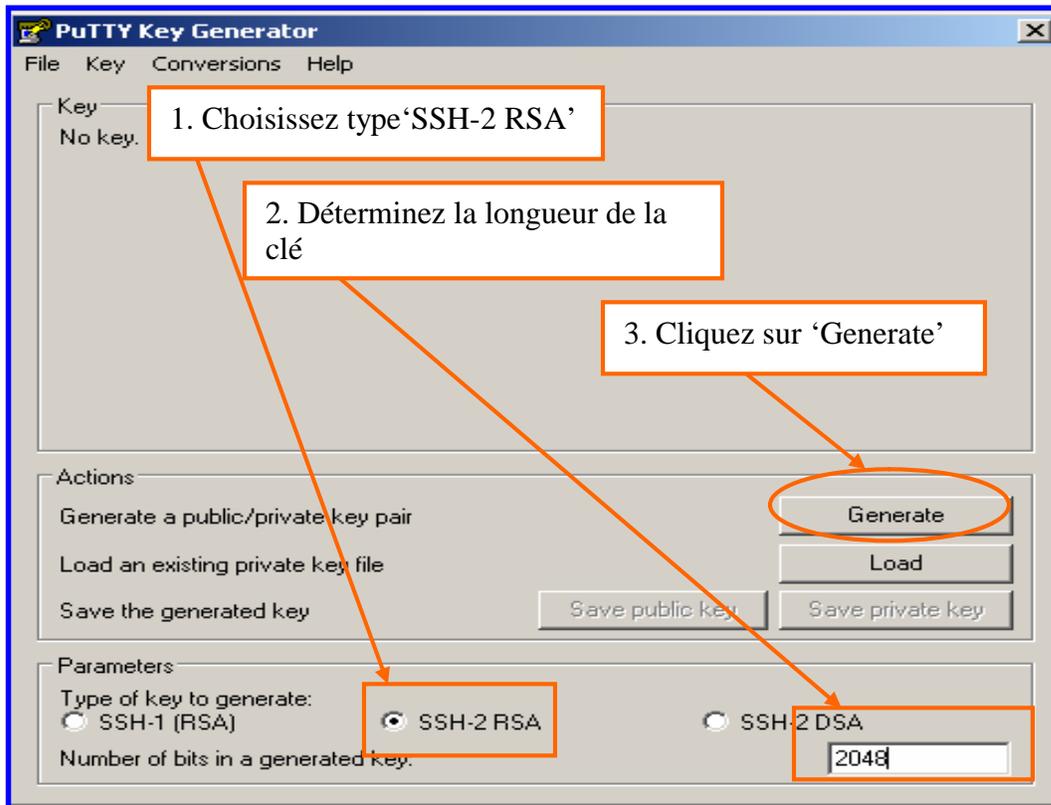
Les clés compatibles avec SSH v2

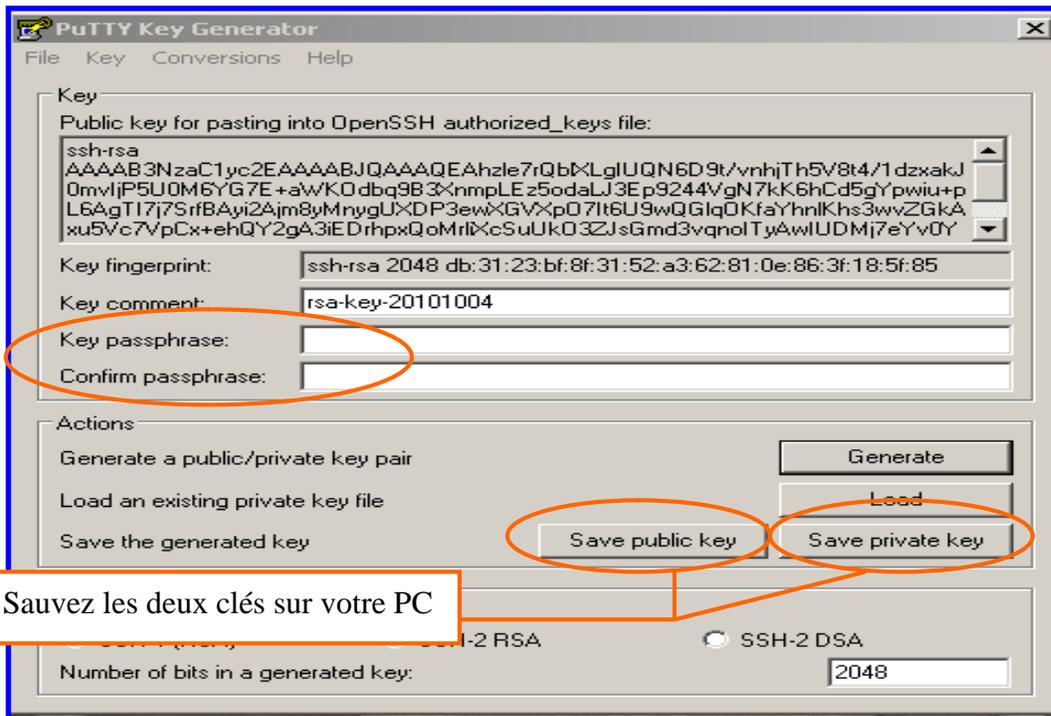
Les formats OpenSSH et SSH sont acceptés

Type de clé : SSH2-RSA

Longueur de clé : de 2048 à 4096 bits.

Exemple : création des clés avec Putty Key Generator





Il est conseillé de sauvegarder la clé privée avec un mot de passe. (Key passphrase)  
Certains SFTP-clients n'admettent toutefois pas de fonctionner avec une clé privée qui est protégée avec un mot de passe.

Si vous avez créé votre clé avec votre client SFTP, référez-vous à la documentation de celui-ci.