# Comment forcer l'activation de l'authentification RSA dans OpenSSH

Depuis OpenSSH 8.8 les version de sshd n'acceptent pas les algorithmes de clé ssh-rsa

Il est possible de réactiver l'authentification SSH (ssh-rsa) dans OpenSSH en ajoutant dans /etc/ssh/sshd_config (ou ssh_config du côté client):

```
#PubkeyAuthentication yes
PubkeyAcceptedKeyTypes=+ssh-rsa
```

Cependant, cette configuration ne permet pas d'activer l'authentification SSH (ssh-rsa) dans OpenSSH 8.8p1-1 sur Raspberry Pi 4 (5.10.74-1), même après un redémarrage du service sshd.

Pour autoriser l'utilisation d'anciennes clés RSA pour OpenSSH 8.8 et versions ultérieures, il faut ajouter les lignes suivantes au fichier sshd_config :

```
HostKeyAlgorithms=ssh-rsa,ssh-rsa-cert-v01@openssh.com
PubkeyAcceptedAlgorithms=+ssh-rsa,ssh-rsa-cert-v01@openssh.com
```

D'autres distributions (comme Arch sur Raspberry Pi) peuvent prendre en charge le protocole xmss, plus sécurisé. Clés recommandées par les dernières publications du NIST :

```
HostKeyAlgorithms=ssh-rsa,ssh-rsa-cert-v01@openssh.com,ssh-xmss-cert-
v01@openssh.com,ssh-xmss@openssh.com
KexAlgorithms=+sntrup761x25519-sha512@openssh.com
PubkeyAcceptedAlgorithms=+ssh-rsa,ssh-rsa-cert-v01@openssh.com,ssh-xmss-
cert-v01@openssh.com,ssh-xmss@openssh.com
```