# RFC 4819 : Secure Shell Public Key Subsystem

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 mars 2007

Date de publication du RFC : Mars 2007

https://www.bortzmeyer.org/4819.html

---

Le protocole SSH, jadis spécifié uniquement dans une implémentation, est désormais une norme IETF (RFC 4251[1] et RFC 4253). Cette norme permet l'ajout d'extensions, les "*subsystems*". Notre RFC ajout donc un "*subsystem*" pour la transmission de clés d'un client à un serveur.

Traditionnellement, avec un programme comme OpenSSH, le client qui voulait être authentifié via sa clé publique, copiait celle-ci sur le serveur puis l'insérait dans `/.ssh/authorized_keys`. Désormais, une fois notre RFC mis en œuvre, il pourra utiliser SSH pour le faire, simplifiant le processus et limitant les risques de fausses manœuvres.

Le client SSH pourra donc désormais ajouter des clés, les lister, les modifier, de manière standard. Notre RFC prévoit aussi les autorisations liées aux clés (comme « cette clé ne doit pas être utilisée pour faire du "*forwarding*" X11 »), autorisations qui se faisaient avec OpenSSH en ajoutant des mots-clés au début des clés.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc4251.txt`