RFC 4716 : The Secure Shell (SSH) Public Key File Format

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 décembre 2006

Date de publication du RFC : Novembre 2006

https://www.bortzmeyer.org/4716.html

Le protocole SSH, mis au point il y a de nombreuses années, est normalisé depuis quelque mois (RFC 4253 [1]) mais il manquait la spécification du format de fichier pour l'échange des clés. Chaque serveur SSH utilisait une forme différente.

Désormais, c'est fait et notre RFC spécifie donc comment représenter les clés publiques des serveurs SSH, afin de pouvoir les transmettre d'une mise en œuvre de SSH à une autre.

C'est un simple format bâti sur ASCII, pas bien méchant, mais qui n'est pas exactement le même que celui utilisé actuellement par OpenSSH et qui va donc nécessiter quelques adaptations. Mais Putty, lui, sait déjà utiliser ce format (ainsi que celui d'OpenSSH.)

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4253.txt