

RFC 7479 : Using Ed25519 in SSHFP Resource Records

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 mars 2015

Date de publication du RFC : Mars 2015

<https://www.bortzmeyer.org/7479.html>

L'algorithme de signature Ed25519 ayant été mis en œuvre dans OpenSSH, ce nouveau RFC permet d'utiliser cet algorithme dans les enregistrements DNS SSHFP (SSH "fingerprint").

Ces enregistrements SSHFP, qui permettent de trouver la clé publique d'un serveur SSH dans le DNS, sont normalisés dans le RFC 4255¹. Les valeurs possibles sont stockées dans un registre IANA <<https://www.iana.org/assignments/dns-sshfp-rr-parameters/dns-sshfp-rr-parameters.xhtml#dns-sshfp-rr-parameters-1>>. Ce registre est donc mis à jour pour inclure Ed25519 <<http://ed25519.cr.yp.to/ed25519-20110926.pdf>>, la valeur étant 4 (RSA était 1 et DSA 2).

Voici un exemple d'un tel enregistrement, pour la clé publique

```
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIGPKSUTyz1HwHRreFVvd5obVsALAgJRNarH4TRpNePnAS
```

Le condensat a été fait en SHA-256 :

```
ssh.example.com. IN SSHFP 4 2 ( a87f1b687ac0e57d2a081a2f2826723
34d90ed316d2b818ca9580ea384d924
01 )
```

(L'exemple est tiré du RFC mais celui-ci contient une légère bogue, je vous laisse la trouver.)

Question mises en œuvre, Ed25519 est dans OpenSSH depuis la version 6.5. D'autres logiciels utilisent cet algorithme, comme TeraTerm <http://sourceforge.jp/ticket/browse.php?group_id=1412&tid=33263>. Wireshark sait désormais le décoder <<https://code.wireshark.org/review/#/c/7654/>>.

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc4255.txt>