

RFC 5081 : Using OpenPGP Keys for Transport Layer Security (TLS) Authentication

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 Novembre 2007

Date de publication du RFC : Novembre 2007

<http://www.bortzmeyer.org/5081.html>

Le protocole TLS, permettant de chiffrer et d'authentifier des communications sur Internet n'a toujours utilisé qu'un seul type de certificats, ceux à la norme X.509. Désormais, on peut aussi se servir de clés PGP. (Ce RFC a depuis été mis à jour dans le RFC 6091¹.)

Pour authentifier l'autre partie, lors d'une communication TLS (utilisée par exemple avec HTTP ou bien avec SMTP), on doit signer ses messages avec sa clé privée. Le correspondant doit connaître la clé publique pour vérifier cette signature. Avec l'ancien protocole SSL et avec son successeur TLS (normalisé dans le RFC 5246), cela se faisait en présentant un certificat X.509. X.509 a plusieurs limites, notamment le fait qu'il dépende d'une autorité de certification. Tout le monde n'a pas envie de payer une telle autorité, pour un gain de sécurité contestable. Il était donc important d'avoir une alternative.

Même si celle-ci n'a pas été tout de suite standardisée par l'IETF (ce RFC n'a que le statut « expérimental », c'est son successeur, le RFC 6091 qui aura fait évoluer le statut), elle est déjà mise en œuvre dans GnuTLS (pour l'instant, le seul logiciel à le faire).

Techniquement, notre RFC dépend du mécanisme d'extension TLS spécifié dans le RFC 5246. Ces extensions permettent d'annoncer le type de certificat utilisé, et donc de choisir X.509 ou bien PGP (PGP est normalisé dans le RFC 4880). Le RFC précise que ces extensions ne doivent pas être utilisées si on ne gère que des certificats X.509, pour interopérer plus facilement avec les vieilles implémentations.

La clé PGP est envoyée encodée en binaire, ou bien peut être récupérée sur le réseau, si celui qui veut s'authentifier indique uniquement l'empreinte de la clé (de la même façon qu'un certificat X.509 peut être récupéré sur le réseau, si celui qui veut s'authentifier indique l'URL de son certificat).

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc6091.txt>