RFC 6091 : Using OpenPGP Keys for Transport Layer Security (TLS) Authentication

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 3 février 2011

Date de publication du RFC : Février 2011

https://www.bortzmeyer.org/6091.html

Le protocole TLS, permettant de chiffrer et d'authentifier des communications sur Internet n'utilisait qu'un seul type de certificats, ceux à la norme X.509 (cf. RFC 5280[1]). Désormais, on peut aussi se servir de certificats PGP. Ce RFC 6091 met à jour la première spécification de « PGP dans TLS », qui était dans le RFC 5081 et la fait passer du statut « expérimental » à « pour information ». (Depuis, le RFC 8446 a supprimé cette possibilité d'utiliser les clés PGP.)

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 connaitre 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.

Celle-ci 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 (extension `cert_type`, numéro 9 dans le registre des extensions <https://www.iana.org/assignments/tls-extensiontype-values/tls-extensionty
xhtml#tls-extensiontype-values-1>), 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. Sinon, si le client propose du PGP et que le serveur ne connait pas, ce dernier répond `unsupported_certificate`. Un

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5280.txt

registre des types de certificats possibles <https://www.iana.org/assignments/tls-extensiontype-valu
tls-extensiontype-values.xhtml#tls-extensiontype-values-2> permettra d'ajouter plus tard autre chose que X.509 ou PGP. L'algorithme de chiffrement de la session, lui, est indépendant du fait qu'on utilise X.509 ou PGP.

Notre RFC utilise le terme de **clé** pour parler des clés PGP actuelles et de **certificat** lorsque les mêmes clés sont utilisées pour l'authentification (cf. section 2). 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, cf. RFC 6066, section 5). Attention, contrairement à l'option équivalente pour X.509, la possibilité de récupérer le certificat sur le réseau ne permet pas d'indiquer le nom ou l'URL d'un serveur de certificats. Celui-ci doit être connu du serveur (qui vérifiera ensuite que les empreintes cryptographiques correspondent.)

Les changements par rapport au RFC 5081 sont résumés dans l'annexe A. Le principal, de loin, est un changement dans la sémantique du message indiquant le certificat (`Client Certificate` et `Server Certificate`) qui fait que les mises en œuvre de l'ancien RFC et celles de notre nouveau RFC 6091 ne peuvent **pas** interopérer. Comme l'ancien RFC n'avait que le statut « expérimental » et qu'il n'a jamais été largement déployé, ce n'est pas un trop gros problème en pratique.