RFC 4954 : SMTP Service Extension for Authentication

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 septembre 2007

Date de publication du RFC : Juillet 2007

https://www.bortzmeyer.org/4954.html

Le courrier électronique, tel que spécifié à l'origine, reposait entièrement sur la confiance aveugle des acteurs entre eux. N'importe quel serveur de messagerie pouvait demander n'importe quoi à n'importe quel autre et les expéditeurs de courrier pouvaient indiquer ce qu'ils voulaient dans le courrier. Aujourd'hui, les demandes de sécurité sont plus fortes, d'où ce RFC.

Il y a deux questions importantes, la **sécurité du message** (s'assurer qu'un message est authentique, quelles que soient les étapes traversées) et la **sécurité du canal** (s'assurer que le serveur à l'autre bout est le bon). Si cette dernière ne permet pas, à elle seule, d'authentifier un message (il faut pour cela utiliser des techniques comme PGP, spécifié dans le RFC 4880 [1]), elle est toutefois intéressante lorsqu'un serveur de messagerie veut n'autoriser certaines fonctions qu'à certains partenaires, dûment authentifiés.

Un exemple typique est le fait de **relayer** du courrier. On parle de « relais » lorsqu'un MTA transmet à un autre MTA un courrier dont le serveur destinataire n'est pas le destinataire final. Il devra donc relayer ce courrier. Autrefois, tous les serveurs relayaient. La montée du spam a mis fin à ces relais ouverts et, aujourd'hui, un serveur bien géré ne relaie que pour des clients autorisés et authentifiés.

Cette extension d'authentification utilise le cadre SASL, spécifié dans le RFC 4422. À l'intérieur de ce cadre sont spécifiées plusieurs méthodes d'authentification comme un mot de passe transmis en clair (RFC 4616).

Le serveur capable d'authentifier annonce cette possibilité en réponse à la requête `EHLO` :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc4880.txt`

```
% telnet mail.bortzmeyer.org smtp
...
220 mail.bortzmeyer.org ESMTP Postfix (Debian/GNU)
EHLO mail.example.org
250-mail.bortzmeyer.org
...
250-AUTH DIGEST-MD5 CRAM-MD5
```

Ici, le serveur SMTP annonce, entre autres choses, sa capacité à gérer l'authentification.

Cette extension est mise en œuvre, par exemple, dans le serveur de messagerie Postfix <https://www.bortzmeyer.org/postfix-sasl.html>.

Bien sûr, transmettre un mot de passe en clair sur Internet est le plus sûr moyen de se faire "*sniffer*". Alors, notre RFC **impose**, pour tout mécanisme d'authentification à mot de passe en clair, d'utiliser TLS, spécifié dans le RFC 3207 et également disponible dans Postfix <https://www.bortzmeyer.org/postfix-tls.html>.

Ce RFC met à jour le RFC 2554, qui avait introduit cette extension. Il n'apporte pas de changements fondamentaux. Notons par exemple l'arrivée de SASLprep (RFC 4013, pour gérer des noms d'utilisateurs en Unicode).