

RFC 4408 : Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 Mai 2006

Date de publication du RFC : Avril 2006

<http://www.bortzmeyer.org/4408.html>

On le sait, le courrier électronique, tel qu'il est spécifié dans les RFC 5321¹ et RFC 5322, ne fournit aucune authentification, même faible, de l'émetteur. Un expéditeur de courrier peut toujours prétendre être Jacques Chirac <president@elysee.fr> et il n'y a aucun moyen de l'en empêcher. SPF vise à diminuer cette facilité de frauder en permettant à un titulaire de nom de domaine de déclarer quelle(s) adresse(s) IP sont autorisées à envoyer du courrier pour ce domaine.

SPF dépend donc du DNS. Le principe de base est d'ajouter à sa zone DNS, par exemple `bortzmeyer.eu`, un enregistrement de type TXT (le SPF original) ou bien du nouveau type SPF (créé par notre RFC). Cet enregistrement déclare, dans un langage "*ad hoc*", quelle(s) adresse(s) IP peuvent envoyer du courrier pour ce domaine. Par exemple, `bortzmeyer.eu` a "`v=spf1 mx -all`", ce qui veut dire en français que seuls les MX (les serveurs qui reçoivent le courrier) de ce domaine peuvent en émettre, le reste de l'Internet (`all`) est exclu.

Pour voir ces enregistrements SPF, on peut par exemple utiliser dig :

```
% dig +short TXT freebsd.org
"v=spf1 ip4:216.136.204.119 ~all"
% dig +short TXT gentoo.org
"v=spf1 mx ptr ?all"
```

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc5321.txt>

On note que SPF, comme la plupart de ses concurrents, n'authentifie que le domaine, pas la personne émettrice (ce point, et plusieurs autres, est discuté en détail dans la section 10, « Sécurité » de notre RFC).

Authentifier le courrier électronique est plus compliqué qu'il ne semble au premier abord, en partie parce qu'il existe plusieurs **identités** possibles :

- L'expéditeur de l'enveloppe (MAIL FROM de la session SMTP),
- L'expéditeur des en-têtes, qui lui-même dépend de l'en-tête qu'on choisit (From: ? Sender: ? Une combinaison de plusieurs en-têtes comme l'algorithme PRA du RFC 4407 ?).

Les partisans de la première approche (celle de SPF) lisent le RFC 5321 et ceux de la seconde lisent plutôt le RFC 5322. Chacune a ses avantages et ses inconvénients.

La question de l'authentification du courrier électronique est très chaude. Les protocoles candidats, comme SPF, ont fait l'objet de nombreuses polémiques. C'est pourquoi l'IESG a collé un gros avertissement au début du RFC, bien que SPF soit, et de très loin, le plus testé des protocoles d'authentification (avec PGP, qui est dans une catégorie très différente).

En même temps que notre RFC a été publié le RFC 4406 sur Sender ID. SenderID, comme SPF, avait été discuté dans le défunt groupe de travail MARID de l'IETF, groupe qui avait été autoritairement dissous avant d'avoir atteint un consensus. Malgré le déploiement bien plus important de SPF, l'IESG a choisi de traiter les deux propositions de manière égale et de publier les deux RFC comme expérimentaux.