RFC 5672 : RFC 4871 DomainKeys Identified Mail (DKIM) Signatures – Update

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 août 2009

Date de publication du RFC : Août 2009

https://www.bortzmeyer.org/5672.html

Depuis sa publication, le RFC 4871 [1], qui normalise DKIM, le mécanisme d'authentification du courrier électronique, le RFC, donc, a connu un certain nombre d'implémentations et de déploiements. Ceux-ci ont mis en évidence des problèmes dans la norme. D'où ce nouveau RFC, un "*erratum*", qui corrige la norme sur quelques points. Une nouvelle version de DKIM, dans le RFC 6376, a ensuite été adoptée, rendant ce RFC 5672 inutile.

Quel était le principal problème ? Comme l'explique la section 1 de notre RFC 5672, DKIM sert à prouver une **identité**, sous la forme d'un **identificateur**, typiquement un nom de domaine. Quelle est la sémantique de cet identificateur ? C'est justement ce qui n'était pas clair dans le RFC 4871. Celui-ci spécifiait deux identités, indiquées par les marques `d=` et `i=` de la signature. Un exemple de signature est :

```
DKIM-Signature: v=1; a=rsa-sha256; s=brisbane; d=example.com;
         c=simple/simple; q=dns/txt; i=joe@football.example.com;
...
```

et on y voit deux identités légèrement différentes, `example.com` et `joe@football.example.com`. Je ne maintiens pas le suspense : la bonne, celle à indiquer l'utilisateur, est bien celle marquée par `d=`, ici `example.com`, ce qui n'était pas évident dans le RFC 4871. C'est ce nom qui devrait être affiché par le MUA comme ayant été authentifié (cf. section 15).

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc4871.txt`

Les sections suivantes du RFC mettent chacune à jour une partie du RFC 4871 original, sous la forme « texte original / nouveau texte ». Certaines sections sont entièrement nouvelles, notamment pour introduire beaucoup de nouveau vocabulaire. C'est ainsi qu'est introduit, dans la section 6, le terme de SDID ("*Signing Domain IDentifier*"), qui désigne la « vraie » identité de l'émetteur du message. Le SDID de l'exemple précédent est donc `example.com`. La section 9 de notre RFC corrige la section 3.5 du RFC original en remplaçant le vague terme « domaine » par SDID. Et la section 10 de notre RFC, pour parler du nom qui figure après la marque `i=`, emploie désormais AUID ("*Agent or User Identifier*") à la place du trop imprécis « identité ». (Le RFC 5672 précise aussi la sémantique de ce champ, insistant notamment sur le fait que sa ressemblance syntaxique avec une adresse de courrier électronique ne doit pas être prise trop au sérieux : le AUID n'est **pas** une adresse.)