RFC 6541 : DKIM Authorized Third-Party Signers

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 mars 2012

Date de publication du RFC : Février 2012

https://www.bortzmeyer.org/6541.html

Depuis la sortie de la norme DKIM d'authentification du courrier électronique (originellement RFC 4871 [1], désormais RFC 6376), il y a des incompréhensions sur ce que DKIM garantit réellement. Beaucoup d'utilisateurs croient que, lorsqu'un message prétend venir de joe@example.net et qu'il est signé par DKIM, on peut être sûr que le message vient de joe@example.net. **Rien n'est plus faux.** DKIM garantit tout autre chose. Il dit que l'identité du domaine signeur, dans le champ DKIM-Signature:, est correcte, et que ce domaine prend la responsabilité du message. Résultat, il y a un fossé entre ce qu'espère l'utilisateur et ce que DKIM livre effectivement. Ce RFC expérimental propose une solution pour combler ce fossé.

Voici une signature DKIM typique, envoyée par le service 23andme <https://www.bortzmeyer.org/23andme.html> :

```
From: 23andMe Research Team <donotreply@23andme.com>
...
DKIM-Signature: v=1; q=dns/txt; a=rsa-sha256; c=relaxed/relaxed; s=132652; d=23andme.ccsend.com;
        h=to:subject:mime-version:message-id:from:date:sender:list-unsubscribe:reply-to;
        bh=87HtUCQR/Puz+14IeKPwOPzfeG32vY3BDJBMB74Kv+w=;
        b=Omftsz+Y3ZbbSbaPWZadKuy8aP35ttpXKTTPdjY4VGttx82q5igLb2r14U3sFI7a+9OXpKODHqOC3HKz1hPQ3GW1L...
```

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

On y voit que le domaine `23andme.ccsend.com` prend la responsabilité de ce message (on peut vérifier l'authenticité de cette déclaration en vérifiant cryptographiquement la signature, qu'on a récupéré dans le DNS, pour le nom `132652._domainkey.23andme.ccsend.com`) mais que le message dit avoir été envoyé par `23andme.com`. Peut-on vérifier cette prétention ? Non, pas avec DKIM. Celui-ci ne fournit, et c'est un choix de conception délibéré, aucun mécanisme pour lier la signature à l'« identité » de l'émetteur (notez au passage que le concept d'identité d'un émetteur de courrier est déjà très flou).

Notre RFC 6541 propose un moyen de faire cette liaison : un domaine peut publier dans le DNS qu'il autorise des tiers à signer ses messages et à les garantir ainsi.

DKIM permettait déjà de déléguer la signature à des tiers (RFC 6376, sections 2.6 et 3.5) mais pas de dire « je fais entièrement confiance à tel domaine pour signer **mes** messages). C'est ce que fournit cette nouvelle norme, ATPS ("*Authorized Third-Party Signers*").

Quels sont les parties en présence (sections 2 et 3) ?

— L'émetteur du message est celui dont le domaine apparait dans le `From:` du message (RFC 5322).
— Le signeur est un tiers autorisé à signer avec DKIM. Il met son propre domaine dans le champ `d=` de la signature.
— Le vérificateur est le récepteur du message, qui voudrait bien vérifier que le message vient effectivement du domaine de l'émetteur.

Dans le monde réel, l'émetteur va par exemple être une entreprise avec une infrastructure de messagerie sommaire, ne permettant pas de signer, et le signeur ATPS va être son sous-traitant. Pour faire connaître cette relation d'affaires entre l'émetteur et son sous-traitant, ATPS permet à l'émetteur de publier dans le DNS un enregistrement TXT annonçant ce lien. Le vérificateur pourra alors récupérer cet enregistrement et se dire « le message est signé par `provider.example`, le message prétend être émis par `customer.example`, or le domaine `customer.example` contient bien un enregistrement ATPS désignant `provider.example` comme signeur autorisé »

La section 4 contient les détails techniques du protocole. D'abord, quel va être le nom de l'enregistrement TXT dans le domaine émetteur ? (Au fait, l'annexe B explique pourquoi utiliser TXT et pas un nouveau type.) Il peut être directement le nom du domaine du signeur mais aussi une version encodée de ce nom. Ensuite, que contient la signature DKIM en cas d'utilisation d'ATPS ? Deux nouveaux champs, `atps=` et `atpsh=` (désormais dans le registre IANA `<https://www.iana.org/assignments/dkim-parameters/dkim-parameters.xml#dkim-parameters-1>`) apparaissent. Si le champ `d=` contiendra, comme avant, le nom de domaine du signeur, le nouveau champ `atps=` contiendra le nom de domaine de celui pour lequel on signe, l'émetteur. Le vérificateur testera si la valeur d'`atps=` correspond à l'en-tête `From:` (ATPS est ignoré s'ils ne correspondent pas), fait une requête DNS pour le type TXT, et vérifie qu'on obtient bien une réponse positive.

Le nom de domaine interrogé pour le type TXT est, dans le cas le plus simple, le `DOMAINE-SIGNEUR._-atps.DOMAINE-ÉMETTEUR`. Si `atpsh=` contient autre chose que `none`, alors `DOMAINE-SIGNEUR` est remplacé par un condensé de son nom.

S'il y a une réponse positive, c'est-à-dire un enregistrement TXT, c'est que c'est bon (pour plus de sécurité, l'enregistrement TXT doit contenir `d=DOMAINE-SIGNEUR`). Si on récupère `NXDOMAIN` (nom non existant) ou bien `NOERROR` mais pas d'enregistrement TXT, c'est que la vérification a échoué. Le signeur n'est en fait pas autorisé à signer pour l'émetteur (section 5). Le vérificateur peut prendre une décision comme de mettre un résultat d'authentification dans les en-têtes du message (cf. section 8.2 pour la création d'un nouveau type d'authentification, `dkim-atps`, mis dans le registre IANA `<https://www.iana.org/assignments/email-auth/email-auth.xml#email-auth-methods>` nomalisé par le RFC 7001).

Et les ADSP ("*Author Domain Signing Practices*") du RFC 5617 ? Ce protocole permet à un domaine émetteur d'annoncer si ses messages sont signés ou non avec DKIM. La section 6 de notre RFC prévoit qu'ATPS doit être testé **avant** ADSP.

Ce RFC est seulement expérimental. L'idée même d'ATPS est fortement contestée (les questions de sécurité et de confiance sont toujours sensibles...) et le besoin s'est fait sentir d'un essai en vrai, pour déterminer si ATPS marche bien ou pas. ATPS est déjà mis en œuvre dans OpenDKIM `<http://www.opendkim.org/>` (il faut configurer avec les options `--enable-atps --enable-xtags`), bibliothèque utilisée notamment par sendmail. Il inclut même un outil `<http://www.opendkim.org/opendkim-atpszone.8.html>` pour générer les enregistrements TXT. Les auteurs d'ATPS ont promis de tester et de décrire dans un document ultérieur le résultat de ces tests.

Quelques points particuliers de sécurité (section 9) :

— La condensation des noms des domaines signeurs avant de faire la requête DNS ne vise pas à fournir la moindre confidentialité, mais simplement à obtenir des noms de taille fixe et connue, ce qui est plus pratique pour les requêtes DNS.
— Et, naturellement, publier un enregistrement ATPS revient à **sous-traiter** une partie de sa sécurité au signeur. Comme toute sous-traitance, il faut donc bien vérifier à qui on fait confiance.

Notez que le RFC ne fournit pas un seul exemple complet de signature avec ATPS et je n'en ai pas encore trouvé dans ma boîte aux lettres.