RFC 5617 : DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 août 2009. Dernière mise à jour le 26 novembre 2013

Date de publication du RFC : Août 2009

https://www.bortzmeyer.org/5617.html

Le protocole de signature des messages électroniques DKIM, normalisé dans le RFC 6376 [1], a un petit défaut : si un message ne porte pas de signature, comment savoir si c'est parce que le domaine émetteur ne signe pas ou bien si c'est parce qu'un attaquant a modifié le message et retiré la signature ? (À noter que la solution proposée par ce RFC a finalement été officiellement abandonnée par l'IETF en novembre 2013.)

La solution qui avait été choisie par le groupe de travail DKIM de l'IETF était, comme documenté dans ce RFC 5617, de permettre à un domaine de **publier** ses pratiques de signature. Désormais, un domaine va pouvoir annoncer dans le DNS qu'il signe tous ses messages (et donc qu'un message sans signature est suspect) ou bien qu'il ne signe pas systématiquement et qu'il faut donc être indulgent à la vérification.

Dans le futur, il est théoriquement possible que DKIM soit tellement largement déployé que cette publication soit inutile, et qu'on puisse considérer que tout message doit être signé. Mais on en est très loin (section 1 du RFC).

Le RFC 5016 avait défini le cahier des charges pour un tel mécanisme de publication des pratiques. Voici donc sa réalisation.

La section 3 du RFC définit les grandes lignes du mécanisme :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6376.txt

— Publication par l'émetteur, dans le DNS, d'un enregistrement à `_adsp._domainkey.mydomain.example`, indiquant les pratiques de signature de `mydomain.example` (mais **pas** celles des domaines fils comme `child.mydomain.example`, cf. section 3.1).
— Consultation par le destinataire de cet enregistrement, le nom de domaine utilisé étant celui qui apparait dans le champ `From:` du message (l'Auteur, en terminologie DKIM). À noter que le message peut avoir des signatures pour d'autres domaines que celui de l'Auteur, par exemple s'il a été transmis via une liste de diffusion qui signe (cf. section 3.2).
— Décision par le destinataire du sort du message, en fonction de ce qu'il a trouvé dans ADSP et de la présence ou pas d'une signature. Par exemple, si un message ne porte aucune signature mais que l'enregistrement ADSP indique que le domaine de l'auteur signe systématiquement, le message est très suspect. Par défaut, la situation actuelle est « pas de signature, pas d'enregistrement ADSP » (cf. section 3.3).

Place maintenant à la description détaillée du protocole, en section 4. Les enregistrements ADSP sont publiés sous forme d'enregistrements TXT. Les objections du RFC 5507 ne s'appliquent pas ici puisque l'enregistrement n'est pas immédiatement dans le domaine, mais dans `_adsp._domainkey.LEDOMAINE`. Dans le texte de l'enregistrement, la syntaxe habituelle de DKIM, `clé=valeur` est utilisée. Actuellement, seule la clé `dkim` est définie (section 4.2.1) et elle peut prendre les valeurs :

— `unknown` : on ne sait pas (c'est la valeur par défaut, s'il n'y a pas d'enregistrement ADSP),
— `all` : tout le courrier venant de ce domaine est signé,
— `discardable` : tout le courrier venant de ce domaine est signé et peut être jeté à la poubelle sans remords s'il ne l'est pas.

Des futures valeurs pourront apparaitre plus tard dans le registre IANA <`https://www.iana.org/assignments/adsp-parameters/adsp-parameters.xhtml`> (section 5).

On retrouve, dans le choix d'une valeur pour la clé `dkim`, un problème classique de l'authentification : que faire lorsqu'elle échoue ? Si on met `unknown`, ADSP ne sert à rien puisque le récepteur n'a aucune idée de s'il peut agir ou non. Si on met `discardable`, on fait courir un grand risque à son courrier puisque une bête erreur comme l'expédition d'un message depuis un site qui ne signe pas pourra entrainer la destruction du message. Je fais le pronostic que, par prudence, les émetteurs n'utiliseront que `unknown` ou `all` et les récepteurs ne jetteront le message que lorsqu'un `discardable` apparait. En pratique, il est donc probable qu'aucun message abusif ne sera éliminé par ADSP.

Les tests faits suite à des requêtes ADSP peuvent donc fournir des informations sur l'authenticité d'un message et ces informations peuvent être publiées dans un en-tête `Authentication-Results:` du RFC 8601. La méthode `dkim-adsp` s'ajoute donc aux méthodes d'authentification utilisables <`https://www.iana.org/assignments/email-auth/email-auth.xhtml`> (section 5.4).

La section 6, les questions de sécurité, explore les risques et les problèmes associés à ADSP. Elle note par exemple, ce qui est plutôt amusant, que puisque des MUA très courants comme Outlook n'affichent pas l'adresse de courrier de l'expéditeur, authentifier le domaine de celle-ci (tout le but de ADSP) n'apporte pas grand'chose avec ces MUA.

Comme ADSP dépend du DNS, il en partage les vulnérabilités, et l'usage de DNSSEC peut donc être nécessaire.

Voici un exemple de requête dig pour trouver l'enregistrement ADSP de `formattype.fr` :

```
% dig +short TXT _adsp._domainkey.formattype.fr
"dkim=unknown"
```

D'autres exemples, très détaillés figurent en annexe A, couvrant les différents cas.

L'annexe B est très intéressante et couvre plusieurs scénarios d'utilisation typiques, où l'usage d'ADSP n'est pas complètement évident. Le cas des listes de diffusion n'y apparait pas, alors qu'elles sont souvent un des plus gros casse-têtes avec DKIM. Si une liste de diffusion respecte le message original et ne le modifie pas, pas de problème. Elle peut laisser l'éventuelle signature DKIM originale (et, si elle le souhaite, ajouter sa propre signature, mais qui ne pourra pas utiliser ADSP puisque le domaine de l'auteur n'est pas celui de la liste). Mais si la liste modifie les messages, par exemple pour ajouter de la publicité à la fin, ou pour ajouter une étiquette dans le sujet, alors la signature DKIM originale ne correspondra plus. Le message sera alors jugé comme étant de la triche (ce qu'il est, puisque le message originel a été changé). Si le programme gestionnaire de listes supprime la signature et que le domaine de l'auteur publiait avec ADSP `dkim=discard`, ce n'est pas mieux, le message sera également considéré comme faux.

À l'heure de la publication du RFC, les mesures faites par DNSdelve <`http://www.dnsdelve.net`> montrent qu'il n'existe quasiment aucun domaine publiant de l'ADSP sous `.fr`. Si on veut tester, les domaines `catinthebox.net`, `isdg.net` ou `wildcatblog.com` publient de l'ADSP.

En novembre 2013, l'IESG a officiellement annoncé la fin d'ADSP <`http://datatracker.ietf.org/doc/status-change-adsp-rfc5617-to-historic/`> et la reclassification de ce RFC comme « intérêt historique seulement ». Il y a certes eu des mises en œuvre d'ADSP mais peu de déploiements. Et parfois, ils se sont mal passés par exemple avec des politiques trop strictes qui faisaient rejeter les messages de certains utilisateurs. Pour connaître la politique DKIM d'un domaine, il faut désormais recourir à des méthodes autres.