RFC 5451 : Message Header Field for Indicating Message Authentication Status

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 avril 2009

Date de publication du RFC : Avril 2009

https://www.bortzmeyer.org/5451.html

Il existe désormais plusieurs techniques pour authentifier les courriers électroniques. Certaines peuvent nécessiter des calculs un peu compliqués et on voudrait souvent les centraliser sur une machine de puissance raisonnable, dotée de tous les logiciels nécessaires. Dans cette hypothèse, le MUA ne recevra qu'une synthèse (« Ce message vient bien de example.com ») et pourra alors prendre une décision, basée sur cette synthèse. C'est le but du nouvel en-tête Authentication-Results: que normalisait notre RFC (depuis remplacé par le RFC 7001 [1]).

Avec des techniques d'authentification comme DKIM (RFC 6376) ou SPF (RFC 7208), les calculs à faire pour déterminer si un message est authentique peuvent être complexes (DKIM utilise la cryptographie) et nécessiter la présence de bibliothèques non-standard. Les installer et les maintenir à jour sur chaque machine, surtout en présence d'éventuelles failles de sécurité qu'il faudra boucher en urgence, peut être trop pénible pour l'administrateur système. L'idée de ce RFC est donc de séparer l'opération en deux : l'authentification est faite sur un serveur, typiquement le premier MTA du site (cf. annexe D pour une discussion de ce choix), celui-ci ajoute au message un en-tête indiquant le résultat de ladite authentification et le MUA (ou bien le MDA, voir la section 1.5.3 pour un bon rappel sur ces concepts) peut ensuite, par exemple par un langage de filtrage comme procmail ou Sieve, agir sur la base de ce résultat. Cet en-tête marche pour tous les protocoles d'authentification et surpasse donc les en-têtes spécifiques comme le Received-SPF: de SPF (section 1 du RFC et notamment section 1.4 pour le filtrage, qui n'est **pas** obligatoire).

J'ai utilisé le terme de « site » pour désigner un ensemble de machines gérées par la même organisation mais le RFC a un terme plus rigoureux, ADMD ("*ADministrative Management Domain*"). La frontière

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7001.txt

d'un ADMD est la « frontière de confiance » ("*trust boundary*"), définie en section 1.2. Un domaine administratif de gestion est un groupe de machines entre lesquelles il existe une relation de confiance, notamment du fait que, à l'intérieur de l'ADMD, l'en-tête `Authentication-Results:` ne sera pas modifié ou ajouté à tort (section 1.6 : l'en-tête n'est pas protégé, notamment il n'est pas signé). Un ADMD inclus typiquement une organisation (ou un département de celle-ci) et d'éventuels sous-traitants. Il a un nom, l'`authserv-id`, défini en section 2.2.

L'en-tête `Authentication-Results:` lui-même est formellement défini en section 2. Il appartient à la catégorie des en-têtes de « trace » (RFC 5322, section 3.6.7 et RFC 5321, section 4.4) comme `Received:` qui doivent être ajoutés en haut des en-têtes et jamais modifiés. La syntaxe de `Authentication-Result` est en section 2.2. L'en-tête est composé du `authserv-id`, le nom de l'ADMD et d'une série de doublets (méthode, résultat), chacun indiquant une méthode d'authentification et le résultat obtenu. Par exemple (tiré de l'annexe C.3), une authentification SPF réussie, au sein de l'ADMD `example.com`, donnera :

```
Authentication-Results: example.com;
          spf=pass smtp.mailfrom=example.net
Received: from dialup-1-2-3-4.example.net
              (dialup-1-2-3-4.example.net [192.0.2.200])
          by mail-router.example.com (8.11.6/8.11.6)
              with ESMTP id g1G0r1kA003489;
          Wed, Mar 14 2009 17:19:07 -0800
From: sender@example.net
Date: Wed, Mar 14 2009 16:54:30 -0800
To: receiver@example.com
```

La liste complète des méthodes figure dans un registre IANA <`https://www.iana.org/assignments/email-auth/email-auth.xhtml`> (section 6).

La section 2.3 détaille l'`authserv-id`. C'est un texte qui identifie le domaine, l'ADMD. Il doit donc être unique dans tout l'Internet. En général, c'est un nom de domaine comme `laposte.net`. (Il est possible d'être plus spécifique et d'indiquer le nom d'une machine particulière mais cette même section du RFC explique pourquoi c'est en général une mauvaise idée : comme les MUA du domaine n'agissent que sur les `Authentication-Results:` dont ils reconnaissent l'`authserv-id`, avoir un tel identificateur qui soit lié au nom d'une machine, et qui change donc trop souvent, complique l'administration système.)

La section 2.4 explique les résultats possibles pour les méthodes d'authentification (en rappelant que la liste à jour des méthodes et des résultats est dans le registre IANA <`https://www.iana.org/assignments/email-auth/email-auth.xhtml`>). Ainsi, DKIM (section 2.4.1) permet des résultats comme `pass` (authentification réussie) ou `temperror` (erreur temporaire au cours de l'authentification, par exemple liée au DNS). Des résultats similaires sont possibles pour SPF (section 2.4.3).

Notons la normalisation d'une méthode traditionnelle d'authentification faible, le test DNS du chemin « adresse IP du serveur -¿ nom » et retour. Baptisée `iprev`, cette méthode, bien que bâtie sur la pure superstition (cf. section 7.11) est utilisée couramment. Très injuste (car l'arbre des résolutions inverses du DNS, `in-addr.arpa` et `ip6.arpa`, n'est pas sous le contrôle du domaine qui envoie le courrier), cette méthode discrimine les petits FAI, ce qui est sans doute un avantage pour les gros, comme AOL qui l'utilisent. Attention aux implémenteurs : aussi bien la résolution inverse d'adresse IP en nom que la résolution droite de nom en adresse IP peuvent renvoyer plusieurs résultats et il faut donc comparer des ensembles. (Cette méthode qui, contrairement aux autres, n'avait jamais été exposée dans un RFC, est décrite en détail dans la section 3, avec ses sérieuses limites.)

Dernière méthode mentionnée, `auth` (section 2.4.5) qui repose sur l'authentification SMTP du RFC 4954. Si un MTA (ou plutôt MSA) a authentifié un utilisateur, il peut le noter ici.

Une fois le code d'authentification exécuté, où mettre le `Authentication-Results:` ? La section 4 fournit tous les détails, indiquant notamment que le MTA doit placer l'en-tête en haut du message, ce qui facilite le repérage des `Authentication-Results:` à qui on peut faire confiance (en examinant les en-têtes `Received:` ; en l'absence de signature, un `Authentication-Results:` très ancien, situé au début du trajet, donc en bas des en-têtes, ne signifie pas grand'chose). On se fie a priori aux en-têtes mis par les MTA de l'ADMD, du domaine de confiance. L'ordre est donc important. (La section 7 revient en détail sur les en-têtes `Authentication-Results:` usurpés.)

Ce n'est pas tout de mettre un `Authentication-Results:`, encore faut-il l'utiliser. La section 4.1 s'attaque à ce problème. Principe essentiel pour le MUA : ne pas agir sur la base d'un `Authentication-Results:`, même si ce n'est que pour l'afficher, sans l'avoir validé un minimum. Comme le `Authentication-Results:` n'est pas signé, n'importe qui a pu en insérer un sur le trajet. Le RFC précise donc que les MUA doivent, par défaut, ne rien faire. Et qu'ils doivent ne regarder les `Authentication-Results:` qu'après que cela aie été activé par l'administrateur de la machine, qui indiquera quel `authserv-id` est acceptable.

Naturellement, le MTA d'entrée du domaine devrait supprimer les `Authentication-Results:` portant son propre `authserv-id` qu'il trouve dans les messages entrants : ils sont forcément frauduleux (section 5). (Le RFC accepte aussi une solution plus simpliste, qui est de supprimer tous les `Authentication-Results:` des messages entrants, quel que soit leur `authserv-id`.)

Arrivé à ce stade de cet article, le lecteur doit normalement se poser bien des questions sur la valeur du `Authentication-Results:`. Quel poids lui accorder alors que n'importe quel méchant sur le trajet a pu ajouter des `Authentication-Results:` bidons ? La section 7, consacrée à l'analyse générale de la sécurité, répond à ces inquiétudes. 7.1 détaille le cas des en-têtes usurpés. Les principales lignes de défense ici sont le fait que le MUA ne doit faire confiance aux `Authentication-Results:` que s'ils portent le `authserv-id` de son ADMD **et** le fait que le MTA entrant doit filtrer les `Authentication-Results:` avec son `authserv-id`. Comme l'intérieur de l'ADMD, par définition, est sûr, cela garantit en théorie contre les `Authentication-Results:` usurpés. Le RFC liste néanmoins d'autres méthodes possibles comme le fait de ne faire confiance qu'au **premier** `Authentication-Results:` (le plus récent), si on sait que le MTA en ajoute systématiquement un (les éventuels `Authentication-Results:` usurpés apparaîtront après ; mais certains serveurs les réordonnent, cf. section 7.3).

Comme toujours en sécurité, il faut bien faire la différence entre authentification et autorisation <https://www.bortzmeyer.org/authentifier-et-autoriser.html>. Un spammeur a pu insérer un `Authentication-Results:` légitime pour **son** `authserv-id`. Même authentifié, il ne doit pas être considéré comme une autorisation (section 7.2).

Plusieurs mises en œuvre de ce système existent déjà comme dans Mdaemon, sendmail, etc. De même, Gmail met désormais systématiquement cet en-tête, par exemple :

```
Authentication-Results: mx.google.com; spf=pass \
           (google.com: domain of stephane@sources.org designates 217.70.190.232 \
               as permitted sender) smtp.mail=stephane@sources.org
```

Comme indiqué plus haut, le RFC désormais officiel pour cet en-tête est, depuis septembre 2013, le RFC 7001. Il ne contient que peu de changements.