RFC 8058 : Signaling One-Click Functionality for List Email Headers

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 31 janvier 2017

Date de publication du RFC : Janvier 2017

https://www.bortzmeyer.org/8058.html

Le RFC 2369[1] décrit des en-têtes du courrier électronique qui indiquent, entre autres, comment se désabonner d'une liste de diffusion (en-tête `List-Unsubscribe:`, qui indique des URI à activer pour se désabonner). Cela peut permettre des désabonnements sans interaction explicite avec l'utilisateur : le MUA voit cette en-tête, propose un bouton « Désabonnement » à l'utilisateur, et le MUA effectue la requête (par exemple HTTP) tout seul. L'inconvénient est que certains logiciels (par exemple des anti-spam) visitent automatiquement tous les liens hypertexte présents dans les messages, et risquent alors de désabonner l'abonné accidentellement. Pour éviter cela, la page pointée par l'URI présent dans `List-Unsubscribe:` n'est en général pas « "*one-click*" » : il faut une action explicite une fois cette page affichée. Ce nouveau RFC propose des ajouts à `List-Unsubscribe:` pour indiquer qu'un désabonnement "*one-click*" est possible.

Voici un exemple de cet en-tête traditionnel `List-Unsubscribe:` dans une liste de diffusion IETF :

```
List-Unsubscribe: <https://www.ietf.org/mailman/options/ietf>,
        <mailto:ietf-request@ietf.org?subject=unsubscribe>
```

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2369.txt`

La page indiquée dans l'URI HTTPS est une "*landing page*" : elle ne désabonne pas directement, il faut indiquer son adresse et sélectionner le bouton "*Unsubscribe*". C'est acceptable quand l'utilisateur est un humain, mais pas dans les cas où il n'y a pas d'interaction possible. Imaginons un logiciel qui traite automatiquement les messages après le départ ou le décès d'un utilisateur, et qui veut donc le désabonner proprement de toutes les listes où il était abonné avec cette adresse désormais invalide. Ce logiciel doit pouvoir fonctionner sans intervention humaine, donc sans analyser une page HTML compliquée.

À noter que l'en-tête `List-Unsubscribe:` ci-dessus, comme dans la plupart des cas, propose également un URI de plan `mailto:`, déclenchant l'envoi d'un message par courrier électronique. La plupart des services qui envoient de grosses quantités de message (les hébergeurs de listes de diffusion à grand volume) ont du mal à gérer le flot de messages de désinscription (ils sont optimisés pour envoyer beaucoup, pas pour recevoir beaucoup), et ce RFC ne prend donc en compte que les URI de plan `https:`.

La section 1 résume le cahier des charges de la solution présentée ici :

— Permettre aux émetteurs de courrier de signaler de manière standard et non-ambigüe qu'on peut se désabonner en un seul clic (« "*one-click*" »),
— Permettre aux auteurs de MUA de fournir une interface simple (par exemple un bouton « Désabonnement immédiat », lorsque le message lu est signalé comme le permettant),
— Permettre aux utilisateurs de se désabonner sans quitter leur MUA, sans avoir à basculer vers une page Web avec des instructions spécifiques (et, notre RFC oublie de le dire, page Web qui est souvent conçue pour décourager le désabonnement de la "*newsletter*" à la con).

La section 3 du RFC spécifie la solution retenue. Elle consiste dans l'ajout d'un nouvel en-tête, `List-Unsubscribe-Post:`, dont le contenu est un couple clé=valeur, `List-Unsubscribe=One-Click`. (Ce nouvel en-tête a été ajouté dans le registre IANA `<https://www.iana.org/assignments/message-headers/message-headers.xml#perm-headers>`.) Par exemple, l'en-tête montré plus haut deviendrait :

```
List-Unsubscribe: <https://www.ietf.org/mailman/options/ietf?id=66fd1aF64>,
        <mailto:ietf-request@ietf.org?subject=unsubscribe>
List-Unsubscribe-Post: List-Unsubscribe=One-Click
```

Cela indiquerait clairement que le désabonnement en un clic est possible. Le MUA, s'il désire effectuer le désabonnement, va alors faire une requête HTTPS de méthode `POST`, en mettant dans le corps de la requête le contenu de l'en-tête `List-Unsubscribe-Post:`. Le serveur HTTPS, s'il voit ce `List-Unsubscribe=One-Click` dans la requête, doit exécuter la requête sans poser de questions supplémentaires (le but étant de faire un désabonnement en un seul clic).

Notez qu'il faut indiquer quelque part l'adresse à désabonner, le serveur HTTP ne peut pas la deviner autrement. Pour rendre plus difficile la création de fausses instructions de désabonnement, cela se fait indirectement, via une donnée opaque, comprise seulement du serveur (le `id` dans l'exemple hypothétique ci-dessus).

Les données contenues dans le `List-Unsubscribe-Post:` doivent idéalement être envoyées avec le type MIME `multipart/form-data` (RFC 7578), et, sinon, en `application/x-www-form-urlencoded`, comme le ferait un navigateur Web. Bien sûr, le MUA doit avoir la permission de l'utilisateur pour effectuer ce désabonnement (on est en « un seul clic », pas en « zéro clic »).

Au fait, pourquoi la méthode `POST` ? `GET` ne peut pas modifier l'état du serveur et `PUT` ou `DELETE` sont rarement accessibles.

Le courrier électronique n'étant pas vraiment sécurisé, il y a un risque de recevoir des messages avec un `List-Unsubscribe-Post:` mensonger. C'est pourquoi le RFC demande (section 4) qu'il y ait un minimum d'authentification du message. La seule méthode d'authentification décrite est DKIM (RFC 6376), avec une étiquette `d=` identifiant le domaine. La signature DKIM doit évidemment inclure dans les en-têtes signés les `List-Unsubscribe:` et `List-Unsubscribe-Post:` dans l'étiquette DKIM `h=`.

Avec l'exemple plus haut, la requête HTTP `POST` ressemblerait à :

```
POST /mailman/options/ietf?id=66fd1aF64 HTTP/1.1
Host: www.ietf.org
Content-Type: multipart/form-data; boundary=---FormBoundaryjWmhtjORrn
Content-Length: 124

---FormBoundaryjWmhtjORrn
Content-Disposition: form-data; name="List-Unsubscribe"

One-Click
---FormBoundaryjWmhtjORrn--
```

La section 6 de notre RFC décrit les éventuels problèmes de sécurité. En gros, il en existe plusieurs, mais tous sont en fait des problèmes génériques du courrier électronique, et ne sont pas spécifiques à cette nouvelle solution. Par exemple, un spammeur pourrait envoyer plein de messages ayant l'en-tête `List-Unsubscribe-Post:`, pour faire générer plein de requêtes `POST` vers le pauvre serveur. Mais c'est déjà possible aujourd'hui en mettant des URI dans un message, avec les logiciels qui vont faire des `GET` automatiquement.

Je n'ai pas encore vu cet en-tête `List-Unsubscribe-Post:` apparaitre dans de vrais messages.

Un des auteurs du RFC a écrit un bon résumé de son utilité `<http://www.circleid.com/posts/20170126_one_click_unsubscription/>`, article qui explique bien comment fonctionne le courrier aujourd'hui.