RFC 5518 : Vouch By Reference

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 avril 2009

Date de publication du RFC : Avril 2009

https://www.bortzmeyer.org/5518.html

Le courrier électronique ne fournit pas assez de garanties pour un certain nombre d'utilisations, notamment celles exigeantes en matière de sécurité. Il y a donc beaucoup de propositions pour améliorer les choses, dont ce RFC qui propose un mécanisme par lequel un message électronique peut annoncer le nom d'un certificateur, qui se portera garant ("*to vouch for*") de son sérieux.

La section 1 résume le principe : un en-tête `VBR-Info:` est ajouté au message par l'émetteur, et le receveur qui veut vérifier le message va demander aux tiers certificateurs, listés dans cet en-tête, leur opinion. Il y a plusieurs points importants pour que cela améliore réellement la sécurité comme le fait que le receveur doit d'abord authentifier le domaine émetteur ou comme l'importance pour le receveur de ne consulter que des certificateurs qu'il connait et apprécie (autrement, l'émetteur pourrait toujours ne mettre que les noms de ses copains **à lui** dans le `VBR-Info:`, cf. section 8).

"*Vouch By Reference*" est donc une technique d'autorisation, pas d'authentification, et la différence est essentielle <https://www.bortzmeyer.org/authentifier-et-autoriser.html>.

La section 2 explique l'utilisation de l'en-tête `VBR-Info:` (ou des en-têtes ; ils peuvent être plusieurs). Il contient le nom du domaine émetteur (celui qu'il faut authentifier avant de contacter les certificateurs), le type du message (un même émetteur peut avoir des messages de types différents par exemple « publicité » et « opérationnel ») et enfin la liste des certificateurs qui peuvent se porter garant, sur le thème de « Oui, nous connaissons `example.com` et tous ses messages de type opérationnel sont utiles ». La syntaxe formelle est en section 4 et un exemple de `VBR-Info:` est :

```
VBR-Info: md=example.com; mc=operation;
          mv=certifier.example;
```

où example.com est l'émetteur du message et certifier.example le certificateur qui peut se porter garant.

Le processus exact de validation d'un message entrant fait l'objet de la section 3. En gros, le récepteur :
— Extrait le nom de domaine pertinent et l'authentifie, par exemple avec DKIM (détails en section 7 du RFC),
— Sélectionne dans la liste des certificateurs ceux auxquels il fait confiance,
— Contacte les certificateurs, via une requête DNS.

C'est la section 5 qui fournit les détails sur cette requête DNS. Elle utilisera le type d'enregistrement TXT sur le nom de domaine du certificateur, préfixé par le nom de domaine à certifier et la chaîne de caractères _vouch. Ainsi, dans l'exemple ci-dessus, la requête DNS sera pour example.com._vouch.certifier.example. S'il y a une réponse, c'est que certifier.example se porte garant et le texte de la réponse contient une liste des types garantis (par exemple « operational security » garantit les messages opérationnels et de sécurité et ne dit rien sur les message de type advertisement). Les types sont décrits plus en détail en section 6. Notez bien qu'ils sont gérés par l'émetteur et ne « prouvent » donc rien, ils ne sont là que pour la traçabilité. Il existe certains types standards comme transaction (message envoyé en réponse à une action spécifique de l'utilisateur).

Enfin, la section 7 revient en détail sur l'authentification du nom de domaine de l'émetteur. Sans précaution particulière, un VBR-Info: ne vaudrait rien puisque le méchant pourrait toujours mettre un autre domaine que le sien dans le VBR-Info:. Notre RFC recommande donc de vérifier ce nom avec DKIM (RFC 6376 [1]), présenté en section 7.1 mais il permet également d'autres techniques comme SPF (RFC 7208 et section 7.3).

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