RFC 5205 : Host Identity Protocol (HIP) Domain Name System (DNS) Extensions

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 21 avril 2008

Date de publication du RFC : Avril 2008

https://www.bortzmeyer.org/5205.html

Le protocole HIP n'avait pas encore de mécanisme pour trouver l'**identificateur** d'une machine distante. C'est désormais chose faite grâce à ce RFC qui permet de trouver l'identificateur dans le DNS (RFC qui a depuis été remplacé par le RFC 8005 [1]).

HIP fait partie de la famille des protocoles qui visent à séparer l'identificateur du localisateur <https://www.bortzmeyer.org/separation-identificateur-localisateur.html>. Les identificateurs HIP se nomment les HI ("*Host Identifier*") et, jusqu'à présent, le seul moyen de trouver l'HI d'une autre machine était d'attendre qu'elle vous contacte, ou bien de le configurer manuellement. Désormais, avec ce RFC, on peut trouver l'HI, comme une adresse IP, dans le DNS.

Notre RFC crée donc un nouveau type d'enregistrement DNS, nommé logiquement HIP, qui stocke, en échange d'un nom de domaine, le HI, son résumé cryptographique - le HIT ("*Host Identifier Tag*") - et les éventuels serveurs de rendez-vous, serveurs qui, dans le protocole HIP, servent d'intermédiaires facultatifs lorsqu'on veut contacter une machine distante (cf. RFC 5204).

Notre RFC permet de trouver l'identificateur à partir du nom mais pas le localisateur ; les serveurs de rendez-vous sont une solution possible pour cela ; une autre est d'utiliser les traditionnels enregistrements A et AAAA du DNS, le localisateur HIP étant une adresse IP.

Curieusement (pour moi), le HIT est donc stocké dans les données DNS, alors que celles-ci n'offrent aucune sécurité au point que le RFC exige en section 4.1 de recalculer le HIT qui vient d'être obtenu dans le DNS.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8005.txt

Le tout ressemble donc aux enregistrements IPSECKEY du RFC 4025, ce qui est normal, le HI étant une clé cryptographique publique.

Voici un exemple d'enregistrement HIP tel qu'il apparaitrait dans le fichier de zone de BIND. On y trouve l'algorithme cryptographique utilisé (2 = RSA), le HIT (en hexadécimal), le HI (encodé en Base64) et les éventuels serveurs de rendez-vous (ici, deux, indiqués à la fin) :

```
www.example.com.      IN  HIP ( 2 200100107B1A74DF365639CC39F1D578
                                AwEAAbdxyhNuSutc5EMzxTs9LBPCIkOFH8cIvM4p
9+LrV4e19WzK00+CI6zBCQTdtWsuxKbWIy87UOoJTwkUs7lBu+Upr1gsNrut79ryra+bSRGQ
b1slImA8YVJyuIDsj7kwzG7jnERNqnWxZ48AWkskmdHaVDP4BcelrTI3rMXdXF5D
                                rvs1.example.com.
                                rvs2.example.com. )
```

L'ensemble du RFC est assez court, ce mécanisme d'annuaire qu'est le DNS étant simple et bien connu.