RFC 8005 : Host Identity Protocol (HIP) Domain Name System (DNS) Extensions

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 novembre 2016

Date de publication du RFC : Octobre 2016

http://www.bortzmeyer.org/8005.html

Le protocole HIP n'avait pas à l'origine de mécanisme pour trouver l'**identificateur** d'une machine distante. Cela avait été fait dans le RFC 5205 [1], qui permettait de trouver l'identificateur dans le DNS. Ce nouveau RFC remplace le RFC 5205.

HIP fait partie de la famille des protocoles qui visent à séparer l'identificateur du localisateur <http://www.bortzmeyer.org/separation-identificateur-localisateur.html>. Les identificateurs HIP se nomment les HI ("*Host Identifier*") et, autrefois, le seul moyen de trouver l'HI d'une autre machine était d'attendre qu'elle vous contacte, ou bien de le configurer manuellement. 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 (numéro 55 <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-4>), qui stocke, en échange d'un nom de domaine, le HI, son condensat (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 8004).

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.

Les localisateurs peuvent changer fréquemment alors que le DNS n'est pas temps-réel et ne change pas instantanément <http://www.bortzmeyer.org/dns-propagation.html>. Si un hôte HIP

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5205.txt

veut pouvoir être contacté malgré des changements d'adresse IP rapides, il vaut peut-être mieux qu'il utilise le système de rendez-vous du RFC 8004.

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.

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 un fichier de zone (sections 5 et 6 de notre RFC). 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. )
```

Par contre, je n'ai pas réussi à trouver encore ce genre d'enregistrement dans la nature.

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

Quels sont les changements depuis le premier RFC, le RFC 5205 ? Évidement le passage sur le chemin des normes, faisant de HIP une norme complète. Mais aussi l'ajout de l'algorithme de cryptographie asymétrique ECDSA, et plusieurs clarifications du RFC original sur le format des enregistrements DNS, aussi bien leur format sur le réseau que dans le fichier de zone.