

RFC 4423 : Host Identity Protocol (HIP) Architecture

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 mai 2006. Dernière mise à jour le 21 avril 2008

Date de publication du RFC : Mai 2006

<https://www.bortzmeyer.org/4423.html>

Voici un RFC très ambitieux : il s'agit tout simplement de changer radicalement l'architecture de l'Internet en utilisant un nouveau type d'identificateur, le "*Host Identifier*" (HI) pour beaucoup d'usages qui sont actuellement ceux des adresses IP.

Une adresse IP sert actuellement à deux choses : désigner une machine (l'adresse IP sert par exemple à distinguer plusieurs connexions en cours) et indiquer comment la joindre (routabilité). Dans le premier rôle, il est souhaitable que l'adresse soit relativement permanente, y compris en cas de changement de FAI ou de mobilité (actuellement, si une machine se déplace et change d'adresse IP, les connexions TCP en cours sont cassées). Dans le second cas, on souhaite au contraire une adresse qui soit le plus "physique" possible, le plus dépendante de la topologie. Ces deux demandes sont contradictoires. (HIP est depuis normalisé dans un RFC plus récent, le RFC 9063¹.)

HIP résoud le problème en séparant les deux fonctions. Avec HIP, l'adresse IP ne serait plus qu'un identifiant "technique", ne servant qu'à joindre la machine, largement invisible à l'utilisateur et aux applications (un peu comme une adresse MAC aujourd'hui).

Pour pouvoir être vérifié, le nouvel identificateur, le HI sera une clé publique cryptographique, qui sera allouée hiérarchiquement par PKI ou de manière distribuée par tirage au sort (comme le sont les clés SSH ou PGP aujourd'hui).

Cette séparation de l'identificateur et du localisateur <<https://www.bortzmeyer.org/separation-identification.html>> est un sujet de recherche très actif actuellement et d'autres propositions que HIP existent.

Soyons patients : si la spécification du protocole est désormais publiée (notre RFC ne décrivait qu'une architecture générale, il est complété par les RFC 5201, RFC 5202, RFC 5203, RFC 5204, RFC 5205, RFC 5206 et RFC 5207, on peut consulter les projets sur la page Web du groupe de travail HIP <<http://hip.piuha.net/>>) et, si des implémentations expérimentales existent déjà et que des serveurs publics utilisent HIP, aucun déploiement significatif n'est encore en vue. (Depuis, HIP v1 a été remplacé par HIP v2, normalisé dans le RFC 7401, puis dans le RFC 9063.)

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc9063.txt>