# RFC 8004 : Host Identity Protocol (HIP) Rendezvous Extension

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 novembre 2016

Date de publication du RFC : Octobre 2016

https://www.bortzmeyer.org/8004.html

---

HIP, par défaut, nécessite que l'**initiateur** d'une association connaisse le localisateur, l'adresse IP du **répondeur**. Si celui-ci bouge souvent, et qu'il n'est donc pas pratique de mettre cette adresse dans le DNS, une solution est d'utiliser le mécanisme de **rendez-vous**, décrit par ce RFC, où l'initiateur contacte un serveur de rendez-vous qui relaie vers le répondeur.

Le schéma est clairement expliqué dans la section 3 du RFC. En fonctionnement habituel de HIP, l'initiateur trouve l'identificateur et le localisateur du répondeur (typiquement, dans le DNS, cf. RFC 8005 [1]), puis le contacte directement. Si le localisateur n'est pas connu (ce qui est fréquent si le répondeur est un engin mobile, changeant souvent d'adresse IP), l'initiateur envoie le premier paquet (**I1**) au serveur de rendez-vous, qui le relaie au répondeur. Les autres paquets (R1, I2 et R2) seront transmis directement entre les deux machines HIP. Le mécanisme est détaillé dans la section 3.3 (il faut notamment procéder avec soin à la réécriture des adresses IP, en raison entre autre du RFC 2827).

Et comment l'initiateur trouve-t-il le serveur de rendez-vous ? En général dans le DNS, via les enregistrements de type HIP. Et comment le répondeur avait-il fait connaitre au serveur de rendez-vous son adresse IP ? Via le protocole d'enregistrement du RFC 8003, comme l'explique la section 4.

Comme toute indirection, le système de rendez-vous ouvre des problèmes de sécurité amusants. Si l'initiateur connaissait déjà l'identificateur du répondeur (donc sa clé publiqué), pas de problème, le passage par le serveur de rendez-vous ne diminue pas la sécurité. Si ce n'est pas le cas, alors, il n'y a rien à faire, l'initiateur n'a aucun moyen de vérifier l'identité du répondeur (section 5 du RFC).

Aucun changement depuis la première spécification, le RFC 5204, juste l'alignement avec la nouvelle version de HIP, celle du RFC 7401, désormais norme complète (et pas juste « expérimentale »).

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