# RFC 3972 : Cryptographically Generated Addresses (CGA)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 octobre 2006

Date de publication du RFC : Mars 2005

http://www.bortzmeyer.org/3972.html

---

Ce RFC décrit un moyen d'authentifier son adresse IP en utilisant la cryptographie.

Dans le protocole IPv6, une machine sur un réseau découvre les voisins par le biais du protocole NDP. Ce protocole n'est pas sûr et rien ne garantit que le voisin qui annonce l'adresse IP du routeur du réseau local est bien le bon routeur. La norme originelle (RFC 2461 [1]) propose comme seule solution d'utiliser IPsec. Le protocole SEND, normalisé dans le RFC 3971 suggère autrement : les adresses IP sont signées par une clé cryptographique.

Notre RFC, compagnon du RFC 3971 explique comment générer des adresses IP de façon à ce que la signature puisse être vérifiée. L'adresse est simplement un résumé cryptographique calculé à partir de la clé publique et de quelques paramètres.

On notera que le problème auquel s'attaque notre RFC est presque l'opposé de celui traité par le RFC 4941, qui cherchait au contraire à empêcher de tracer un ordinateur utilisant IPv6. Les adresses CGA, définies par notre RFC, visent au contraire à permettre l'authentification.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2461.txt