RFC 6491 : RPKI Objects issued by IANA

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 février 2012

Date de publication du RFC : Février 2012

https://www.bortzmeyer.org/6491.html

La RPKI est le système de distribution de certificats et d'objets signés avec les clés de ces certificats, qui permet de poser les bases d'une sécurisation du routage <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html> dans l'Internet, en permettant aux titulaires des ressources (préfixes d'adresses IP, notamment), d'autoriser tel ou tel opérateur et uniquement ceux-ci, à utiliser ces ressources. Certains préfixes ne sont pas alloués à un utilisateur, ils dépendent directement de l'IANA et ce RFC 6491 [1] est donc consacré à lister les tâches de l'IANA pour ces préfixes. Par exemple, l'IANA devra émettre et signer un objet disant « Personne ne peut annoncer de route vers 198.51.100.0/24 (ce préfixe étant réservé, par le RFC 5737, à la documentation) ».

Rappelons que les responsabilités de l'IANA vis-à-vis de l'IETF sont fixées par le RFC 2860. Pour le cas particulier de la RPKI (RFC 6480), l'IANA va devoir verrouiller l'usage des préfixes IP qu'elle gère (section 1). Ces préfixes sont utilisées pour la documentation ou réservés pour d'autres usages. Comme personne ne doit les router, l'IANA va émettre des ROA (RFC 6482) négatifs, c'est-à-dire prouvant que ces adresses ne sont pas routables. Un routeur BGP validant (RFC 6483) va alors pouvoir les rejeter, si jamais ils apparaissent dans des annonces de routes. Ces ROA négatifs sont officiellement appelés « **AS0 ROA** », le numéro d'AS zéro étant invalide (il ne doit jamais être dans un chemin d'AS). La section 4 du RFC 6483 détaille ce concept de **désaveu de route**.

Ce désaveu s'applique aux préfixes qui sont prévus pour ne jamais apparaître dans la table de routage globale (section 5), ainsi qu'à ceux qui ne sont pas actuellement alloués et donc toujours à l'IANA (aujourd'hui, cela ne concerne plus qu'IPv6, cf. section 6). Les adresses « spéciales » (section 7, voir aussi le RFC 6890) se divisent, elles, en deux : celles prévues pour être routées globalement, pour lesquelles l'IANA ne doit rien faire, et celles non prévues pour être routées, et pour lesquelles il y aura donc un AS0 ROA.

La liste des préfixes figure en annexe A du RFC. On y trouve les suspects habituels, le préfixe 169.254.0.0/16 ou fe80::/10 des adresses locales au lien, les préfixes privés des RFC 1918 et RFC 4193, les préfixes réservés à la documentation... Tous ceux-ci ne seront jamais routés sur l'Internet.

Avant de commencer à émettre ces ROA, l'IANA devra évidemment établir une CA (section 10). Cette CA devra utiliser les extensions à X.509 du RFC 3779. Elle devra aussi publier la liste de ses objets (j'avoue n'avoir pas trouvé où c'était documenté sur le site de l'IANA...).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6491.txt