RFC 6483 : Validation of Route Origination using the Resource Certificate PKI and ROAs

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/6483.html

Ce document s'inscrit dans la longue liste des RFC sur la sécurisation du routage BGP <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>. Il décrit la **sémantique** des **ROA** ("*Route Origin Authorization*"), ces objets qui expriment l'autorisation du titulaire d'un préfixe IP à ce que ce préfixe soit annoncé initialement par un AS donné. La **syntaxe** des ROA, elle, figure dans le RFC 6482[1].

Les ROA ("*Route Origin Authorization*") sont issus de la RPKI, l'IGC du routage (RFC 6480). Ce sont des objets signés qu'un routeur BGP peut vérifier lorsqu'il reçoit une annonce. Ainsi, si un routeur BGP voit son pair lui dire « je connais un chemin vers 192.0.2.0/24 et son chemin d'AS est 64498 65551 65540 », le routeur peut vérifier que l'AS 65540 a bien été autorisé, par le titulaire du préfixe 192.0.2.0/24, à annoncer cette route (l'**origine**, le premier AS, est le plus à droite ; ce RFC ne permet de valider que l'origine, pas le chemin complet, donc on ne peut rien dire au sujet de la présence des AS 64498 et 65551). Les clés utilisées pour les signatures sont contenues dans des certificats X.509 suivant le format Internet standard (RFC 5280) avec des extensions pour stocker des informations comme les adresses IP (RFC 3779). Ces certificats permettent de vérifier que le signataire était bien titulaire de la ressource (ici, le préfixe 192.0.2.0/24). Quant au format des ROA, on l'a dit, il figure dans le RFC 6482.

Tout d'abord (section 2 du RFC), que se passe-t-il pendant la validation d'une annonce de route et quels sont les résultats possibles ? Une route est composée d'un ensemble de préfixes IP, d'un chemin d'AS et de quelques attributs. L'origine, la seule chose vérifiée par les ROA, est le premier AS du chemin (donc le plus à droite). S'il y a eu agrégation, et que le premier élément du chemin est un ensemble d'AS, l'origine est inconnue.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6482.txt

L'engin qui fait la validation (nommé RP, pour "*Relying Party*", c'est le routeur BGP, ou bien une machine spécialisée à laquelle il a sous-traité ce travail) est supposé avoir accès à tous les ROA valides (ce RFC ne décrit pas comment, a priori, ce sera le protocole standard de récupération des préfixes validés, protocole nommé **RTR**, normalisé dans le RFC 6810). Il cherche les ROA s'appliquant à l'annonce qu'il veut valider. Si un ROA correspond, l'annonce est valide. Un ROA pour un préfixe donné s'applique à tous les préfixes plus spécifiques (ceux où le masque est plus long). Ainsi, si un ROA dit « l'AS `65540` a le droit d'annoncer `192.0.2.0/24` », alors une annonce de `192.0.2.128/25` (plus spécifique) est invalide (même si l'origine est la même, cf. le tableau "*Route's validity state*"). Toutefois, l'utilisation du champ `maxLength` dans le ROA permet d'accepter des préfixes plus spécifiques (jusqu'à `maxLength`). Si une annonce ne correspond à aucun ROA, elle est dans l'état « inconnu » (également appelé « non trouvé »). Au début du déploiement, évidemment, la plupart des annonces seront dans l'état inconnu, puisque peu de ROA seront émis. Mais dès qu'un opérateur crée un ROA pour un de ses préfixes, tous les sous-préfixes non signés deviennent invalides (la RPKI suit le modèle hiérarchique des adresses IP). L'algorithme exact est décrit à la fin de la section 2. (Ceux qui ont suivi toute l'histoire de ce RFC avant sa publication noteront que l'algorithme initial était bien plus complexe.)

Maintenant, que faire de ce résultat ? La section 3 explique comment utiliser cet état (valide, invalide, inconnu) pour sélectionner une route (rappelez-vous qu'un routeur BGP typique reçoit plusieurs routes possibles pour chaque préfixe et qu'il doit choisir). En gros, le routeur doit préférer les routes valides, puis les inconnues. Mais la décision est locale : le RFC n'impose rien, notamment il ne dit pas si le routeur doit ignorer complètement les annonces invalides ou, a fortiori, les inconnues (la très grande majorité, au début du déploiement de ce système). Autre piège : la vitesse de propagation des ROA ne sera pas forcément celle des routes, et une annonce peut arriver avant le ROA correspondant.

Le problème est similaire à celui que connaissent les résolveurs DNS avec DNSSEC. Rejeter les réponses DNS non signées, aujourd'hui, reviendrait à rejeter la majorité des réponses. (Une autre expérience de DNSSEC est que les réponses invalides sont beaucoup plus souvent dues à des erreurs du gentil administrateur systèmes qu'à des attaques par les méchants.) Pour BGP, le problème est plus complexe car il est normal de recevoir plusieurs routes vers la même destination. Sans rejeter les annonces inconnues, le routeur peut donc décider de les faire passer après les valides. Et, s'il n'y a qu'une seule route pour une destination donnée, et que l'annonce est invalide, il vaut peut-être mieux l'accepter que de couper la communication avec le réseau concerné (la résilience de l'Internet le recommande).

Donc, pour résumer la section 3 : **chaque administrateur réseaux configure son routeur comme il veut, pour décider du sort des annonces inconnues, et même pour celui des annonces invalides**. Un exemple en syntaxe IOS serait :

```
route-map rpki permit 10
 match rpki invalid
 set local-preference 50

route-map rpki permit 20
 match rpki unknown
 set local-preference 100

route-map rpki permit 30
 match rpki valid
 set local-preference 200
```

Dans cet exemple, tous les états sont acceptés, mais avec des préférences différentes.

Il est également possible à un titulaire de préfixe d'interdire complètement l'utilisation de ce préfixe, en créant un ROA où le numéro d'AS est mis à zéro (section 4). L'AS 0 est réservé dans le registre IANA

<https://www.iana.org/assignments/as-numbers/as-numbers.xml> et ne doit jamais apparaître dans une annonce réelle.

Une fois une route validée, pendant combien de temps garde-t-elle son état ? Question facile à laquelle la section 5 répond : la durée de validité est celle du certificat qui a signé le ROA (rappelez-vous que les ROA indiquent l'AS d'origine, et que c'est une information relativement stable). Si on veut annuler un ROA avant, il faut révoquer le certificat qui l'a signé.

La section 6 rassemble les considérations de sécurité des ROA : d'abord, elle rappelle qu'il y a un risque réel de se tirer dans le pied. Si on publie un ROA pour un préfixe, les préfixes plus spécifiques deviennent aussitôt invalides. Si on a de ces préfixes plus spécifiques, il faut donc penser à leur créer un ROA **avant** de publier le ROA le plus général.

Voilà, si vous voulez mettre tout cela en pratique, lisez mon article sur les logiciels de la RPKI <https://www.bortzmeyer.org/rpki-tests.html>.