RFC 6916 : Algorithm Agility Procedure for RPKI

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 avril 2013

Date de publication du RFC : Avril 2013

https://www.bortzmeyer.org/6916.html

La grosse infrastructure de sécurisation du routage RPKI+ROA <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html> est en train de se mettre en place, les RFC sont sortis, mais l'IETF ne s'arrête pas là. Ce document décrit la façon de changer les algorithmes de cryptographie utilisés par la RPKI lorsque les progrès de la cryptanalyse l'exigeront.

Disons-le tout de suite, cela va être un énorme travail. La RPKI n'a pas de centre, les décisions dépendent d'un grand nombre d'acteurs non coordonnés, des AC qui émettent les certificats aux RP ("*Relying Parties*", les validateurs qui vérifient les ROA - "*Route Origin Authorizations*"). Le RFC ne sème pas d'illusion et affirme qu'un éventuel changement d'algorithmes dans la RPKI prendra plusieurs années.

Il y avait en théorie plusieurs stratégies possibles, du bas vers le haut (les acteurs situés le plus bas dans la hiérarchie migrent les premiers) ou celle finalement choisie, après de longues discussions dans le groupe de travail SIDR <http://tools.ietf.org/wg/sidr>, du haut vers le bas (les acteurs les plus haut placés commencent).

À noter qu'il s'agit bien de changer d'**algorithmes**. Remplacer les **clés** ("*key rollover*") est prévu et normal dans le fonctionnement de la RPKI (RFC 6489 [1]). Mais les algorithmes ne sont pas éternels. Ceux normalisés actuellement dans le RFC 6485 (RSA et SHA-256) ne résisteront pas toujours à la cryptanalyse et devront laisser un jour la place à d'autres (fondés sur les courbes elliptiques ?).

Comme le processus sera long, il devra commencer par une mise à jour de ce RFC 6485, documentant les nouveaux algorithmes et par la publication d'un plan de migration, avec chronologie. Puis

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6489.txt

la procédure décrite en section 4 sera appliquée, dans l'ordre chronologique : les AC commencent à émettre des certificats avec le nouvel algorithme, puis les RP (les validateurs) commencent à pouvoir vérifier le nouvel algorithme, puis les AC arrêtent d'utiliser l'ancien algorithme (période nommée "*Twilight*" dans le RFC, mais rien à voir avec Stephenie Meyer), puis on peut déclarer l'ancien algorithme mort. Le passage à chaque étape nécessite que **tous** les acteurs impliqués aient migré, ce qui explique le délai de plusieurs années envisagé (aucune procédure n'est envisagée pour le cas, catastrophique, où de brusques percées de la cryptanalyse obligeraient à un remplacement d'urgence). Le RFC est plein de phrases comme « "*If a substantial number of RPs are unable to process product sets signed with Suite B [le nouvel algorithme], the algorithm transition timeline document MUST be reissued, pushing back the date for this and later milestones [...]*" », qui donnent une idée des problèmes qui vont surgir à cause de cette règle « pas de passage sans unanimité ».

Il y aura donc une (longue) période de coexistence entre les deux algorithmes. La section 6 décrit ce que devra être le comportement des validateurs pendant cette période, notamment si les deux algorithmes donnent des résultats opposés (l'un valide et l'autre pas ; l'expérience avec des techniques cryptographiques comme DNSSEC montre que ce genre de choses arrive).

Et n'oubliez pas que ce beau plan n'a jamais été testé. Rendez-vous dans sept ou quinze ans pour le premier changement d'algorithme de la RPKI...