RFC 6725 : DNS Security (DNSSEC) DNSKEY Algorithm IANA Registry Updates

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 août 2012

Date de publication du RFC : Août 2012

https://www.bortzmeyer.org/6725.html

Lors de la conception d'un protocole cryptographique, il est essentiel de permettre l'**agilité des algorithmes**, c'est-à-dire de changer d'algorithme pour répondre aux progrès de la cryptanalyse. C'est ainsi que DNSSEC inclut dans les enregistrements DNS de clés et de signatures un numéro qui identifie l'algorithme utilisé. Les numéros possibles sont dûment notés dans un registre IANA <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml#dns-sec-alg-numbers-1> et ce nouveau RFC « nettoie » le registre, mettant à jour des entrées inutilisées.

Au passage, les érudits noteront que cette absence d'agilité cryptographique (l'algorithme n'est pas indiqué donc un seul algorithme est possible) est un des inconvénients de DNScurve <https://www.bortzmeyer.org/dnscurve.html>. Mais ne digressons pas. Quels changements a apportés notre nouveau RFC 6725[1] ? Les numéros 4, 9 et 11, correspondant à des algorithmes qui n'ont jamais été déployés sont désormais marqués comme « réservés ». C'est tout. On ne peut pas les réaffecter (au cas où il traine dans la nature des mises en œuvre expérimentales utilisant ces algorithmes).

4 était réservé pour un algorithme à courbes elliptiques (on n'a jamais su lequel), 9 et 11 n'étaient pas officiellement affectés mais l'ont apparemment été non-officiellement.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6725.txt