RFC 6014 : Cryptographic Algorithm Identifier Allocation for DNSSEC

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 novembre 2010

Date de publication du RFC : Novembre 2010

https://www.bortzmeyer.org/6014.html

L'allocation d'un nouveau numéro pour un algorithme cryptographique dans DNSSEC exigeait auparavant un RFC sur le chemin des normes. Désormais, n'importe quel RFC conviendra, ce qui est une libéralisation bienvenue.

Ces numéros sont attribués par l'IANA, stockés dans un registre public <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml> et permettent, lorsqu'on récupère un enregistrement DNSSEC, de savoir comment l'interpréter. Ainsi, le TLD .pm est signé avec l'algorithme de numéro 8, soit RSA/SHA-256 :

```
% dig +dnssec ANY pm.
...
pm.  172800 IN RRSIG SOA 8 1 172800 20100818151448 20100719141448 14659 pm. oepDlhY...
```

L'espace de nommage de ces codes ne fait qu'un seul octet, soit 256 possibilités seulement. Ce point a fait l'objet d'inquiétudes au moment de la libéralisation de l'allocation.

La norme DNSSEC, le RFC 4034[1] (section 7), reprenant des normes antérieures, impose un « "*IETF standards action*" » pour enregistrer un nouveau code, sauf pour 253 et 254, qui sont utilisables pour de expérimentations sans formalité. Une « "*IETF standards action*" », comme nous l'apprend le RFC 5226, est la publication d'un RFC situé sur le chemin des normes. C'est donc une opération plutôt lourde (mais possible : GOST a eu le numéro 12 ainsi, grâce au RFC 5933).

La section 2 du RFC explique le pourquoi de la libéralisation :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4034.txt

— Certains algorithmes méritants peuvent avoir du mal à passer sur le chemin des normes, par exemple par suite de craintes sur les brevets qui les plombent, ou simplement parce qu'il n'ont pas encore été scrutés avec suffisamment d'attention. (Voir aussi la section 5 pour une discussion sur la sécurité des algorithmes et leur normalisation.)
— Les demandes sont peu fréquentes (on n'invente pas un nouvel algorithme de cryptographie tous les jours !) et il y a donc peu de chances de voir les huits bits de l'espace occupés immédiatement.

Pour être complètement en sécurité, notre RFC demande à l'IETF de réévaluer les critères d'allocation lorsque 120 entrées du registre auront été allouées (en juillet 2010, on en a 11...). C'est pour cela que la plage 123-251 du registre est marquée comme réservée. Et les codes 253 et 254 restent disponibles pour les expérimentations.

Quelles sont les conséquences pour les mises en œuvre de DNSSEC (section 3) ? D'abord, il faut bien voir qu'un programme qui fait du DNSSEC n'a jamais été obligé d'implémenter **tous** les algorithmes du registre. Ceci ne change pas. Il y aura donc toujours des algorithmes qui ne seront pas universellement mis en œuvre. Les seuls algorithmes qui sont garantis sont ceux indiqués comme obligatoires dans le RFC 4034 (annexe A.1) ou son successeur. Actuellement, il n'y a que RSA/SHA-1.

Enfin, notons que le RFC précise que l'ordre des algorithmes dans le registre n'implique rien sur leur force cryptographique respective, ou leur sécurité...

Comme notre RFC ne fait que changer une règle d'allocation dans un registre IANA, toute sa partie normative se concentre dans la section 4, « "*IANA considerations*" ». En un mot, un RFC de n'importe quel statut suffit désormais pour demander un code dans le registre <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml>. Certains cas dans DNSSEC n'étaient pas couverts par cette libéralisation, mais c'est désormais le cas depuis le RFC 9157.