# RFC 9157 : Revised IANA Considerations for DNSSEC

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 décembre 2021

Date de publication du RFC : Novembre 2021

https://www.bortzmeyer.org/9157.html

---

Rien de très grave dans ce nouveau RFC, qui règle un problème surtout bureaucratique, le fait que les politiques d'inclusion dans les registres IANA pour certains algorithmes utilisés par DNSSEC n'étaient pas parfaitement alignées.

En effet, le RFC 6014 [1] avait modifié la politique d'enregistrement des algorithmes cryptographiques de « Action de normalisation » à la plus laxiste « RFC nécessaire » (rappelez-vous que tous les RFC ne sont pas des normes, voir le RFC 8126 qui décrit ces politiques possibles). Mais cette « libéralisation » laissait de côté certains algorithmes, ceux utilisés pour les enregistrements DS (RFC 4034), et ceux utilisés pour NSEC3 (RFC 5155), qui restaient en « Action de normalisation ». Notre nouveau RFC aligne les politiques d'enregistrement des algorithmes utilisés pour les DS et pour NSEC3 pour qu'ils soient eux aussi « RFC nécessaire ».

Il modifie également le RFC 8624 pour préciser que les algorithmes normalisés dans des RFC qui ne sont pas sur le chemin des normes sont également couverts par les règles du RFC 8624 ; en gros, ils sont facultatifs ("*MAY*" dans le langage du RFC 2119).

Les registres concernés sur celui sur NSEC3 <https://www.iana.org/assignments/dnssec-nsec3-paramete
dnssec-nsec3-parameters.xml#dnssec-nsec3-parameters-3> et celui sur DS <https://
www.iana.org/assignments/ds-rr-types/ds-rr-types.xml#ds-rr-types-1>. Ils portent désormais la mention "*RFC Required*".

Comme l'enregistrement d'algorithmes va, du fait de ce RFC, être plus léger, cela facilitera l'enregistrement de bons algorithmes, mais aussi de mauvais. Le programmeur qui met en œuvre DNSSEC, ou l'administratrice système qui le déploie, ne doit donc pas considérer que la présence dans un registre IANA vaut forcément approbation de la solidité cryptographique de l'algorithme. Il faut consulter la littérature technique avant d'utiliser ces algorithmes.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6014.txt