RFC 6944 : Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 mai 2013

Date de publication du RFC : Avril 2013

https://www.bortzmeyer.org/6944.html

Mais quel algorithme de cryptographie choisir pour mes signatures DNSSEC, se demande l'ingénieur système ? Il y a bien un registre IANA <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml#dns-sec-alg-numbers-1> des algorithmes normalisés mais c'est juste une liste non qualifiée, qui mêle des algorithmes de caractéristiques très différentes. Ce nouveau RFC vise à répondre à cette question en disant quels sont les algorithmes recommandés. (Il a depuis été remplacé par le RFC 8624 [1].)

La première liste d'algorithmes possibles avait été faite dans le RFC 4034. D'autres algorithmes avaient été ajoutés par la suite. Certains sont devenus populaires. Par exemple, RSA avec SHA-2 est utilisé pour presque tous les TLD importants et est donc difficilement contournable pour un résolveur validant. D'autres ont été peu à peu abandonnés, parfois parce que les progrès de la cryptanalyse les menaçaient trop, parfois simplement parce qu'ils n'avaient pas un bon marketing.

Aujourd'hui, le développeur qui écrit ou modifie un logiciel résolveur validant (comme Unbound ou BIND) doit donc se taper pas mal de RFC mais aussi pas mal de sagesse collective distillée dans plusieurs listes de diffusion pour se faire une bonne idée des algorithmes que son logiciel devrait gérer et de ceux qu'il peut laisser tomber sans trop gêner ses utilisateurs.

Ce RFC 6944 détermine pour chaque algorithme s'il est **indispensable** (on n'a pas le droit de faire l'impasse), **recommandé** (ce serait vraiment bien de l'avoir, sauf raison contraire impérieuse), **facultatif** (si vous n'avez rien d'autre à faire de vos soirées que de programmer) ou tout simplement **à éviter** (pour le cas de faiblesses cryptographiques graves et avérées). La liste se trouve dans la section 2.3 : RSA avec

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8624.txt

SHA-1 est le seul indispensable. RSA avec SHA-1 plus NSEC3 (voir plus loin l'explication de ce cas particulier), RSA SHA-256 ou SHA-512 (connus collectivement comme SHA-2), ECDSA avec SHA-256 ou SHA-384 sont recommandés. Tous les autres sont facultatifs (c'est par exemple le cas de GOST dans le RFC 5933) sauf RSA avec MD5 qui est à éviter (RFC 6151).

La section 2.2 justifie ces choix : RSA+SHA-1 est l'algorithme de référence, celui qui assure l'interopérabilité (tout logiciel compatible DNSSEC doit le mettre en œuvre). Normalisé pour DNSSEC avant l'apparition de NSEC3 dans le RFC 5155, il existe en deux variantes, une sans NSEC3 (celle qui est indispensable) et une avec (qui est recommandée car la plupart des TLD utilisent NSEC3). RSA+SHA-2 est recommandé car, comme indiqué plus haut, la racine <http://www.root-dnssec.org/wp-content/uploads/2010/06/icann-dps-00.txt> et la plupart des TLD l'utilisent. Un résolveur qui ne comprendrait pas ces algorithmes ne servirait pas à grand'chose.

Au contraire, ECDSA est très peu utilisé en pratique. Mais les courbes elliptiques suscitent beaucoup d'intérêt, et sont une alternative au cas où il y aurait un gros problème avec RSA. D'où le statut « Recommandé ».

Des nouveaux algorithmes vont certainement apparaître dans le registre <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml#dns-sec-alg-numbers-1> (cf. RFC 6014). Ils seront automatiquement considérés comme facultatifs, jusqu'à la sortie d'un nouveau RFC (qui a été le RFC 8624, qui privilégie désormais les algorithmes utilisant les courbes elliptiques).

Et si vous parlez plutôt la langue de Manuel Puig, ce RFC est également commenté en espagnol <http://hugo.salga.do/post/54044111061/rfc6944-applicability-statement-dns-security-dr