# Signature DNSSEC de la racine du DNS en 2010

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 octobre 2009. Dernière mise à jour le 16 décembre 2009

https://www.bortzmeyer.org/signature-racine.html

---

À la réunion RIPE du 6 octobre, l'ICANN et Verisign ont conjointement annoncé la signature DNSSEC de la racine du DNS pour le 1er juillet 2010. (Le processus pratique a commencé en janvier 2010 <https://www.bortzmeyer.org/la-racine-commence-signature.html>.)

Cette annonce spectaculaire, quoique attendue, comportait notamment un calendrier pour la signature :

- signature (non publiée) le 1er décembre 2009,
- publication des signatures (mais pas de la clé) : de janvier-juin 2010, et de manière différenciée selon les serveurs racine,
- publication officielle de la clé (et donc vrai lancement, puisque cela permettra aux résolveurs de valider) : 1er juillet 2010,
- ajout des délégations vers les TLD (enregistrements DS) : non spécifié et c'est là le point le plus noir. Comme (malgré ce qu'écrivent les journalistes au sujet d'une soi-disant indépendance que l'ICANN aurait récemment gagné) **tout** changement dans la racine du DNS, même purement technique, doit être approuvé par écrit et à l'avance par le gouvernement états-unien, ce point va sérieusement handicaper le déploiement de DNSSEC. Les TLD déjà signés comme `.se` ou `.org` ne sont donc pas près de pouvoir être validés.

L'annonce a été faite à deux voix (Joe Abley pour l'ICANN et Matt Larson pour Verisign) car, si la grande majorité des acteurs de l'Internet voulaient confier la responsabilité de la signature à l'ICANN, Washington a finalement préféré renouveler sa confiance à une société privée à but lucratif, Verisign. L'ICANN gérera donc la clé de signature de clé (KSK pour "*Key Signing Key*") et Verisign la clé de signature de zone (ZSK pour "*Zone Signing Key*").

Le délai entre la signature et la publication officielle de la clé, via un canal sécurisé à déterminer, s'explique par le fait que, tant qu'on ne publie pas la clé officiellement (on peut toujours la prendre dans le DNS avec `dig DNSKEY .`), les gens sérieux ne valident pas les signatures et, donc, rien ne peut aller vraiment mal. Quand on publie la clé, les gens s'en servent et, là, ça peut portentiellemnt aller mal. Il est donc prudent de prévoir une marge. Avant que la clé soit publiée officiellement, on peux toujours arrêter de signer (`.gov` l'avait fait pendant leurs essais). Après, ce n'est plus possible, les résolveurs validateurs casseraient.

Quelques décisions techniques ont également été annoncées hier :

— KSK RSA de 2048 bits,
— changée tous les 2-5 ans (avec cérémonie solenelle de génération de la nouvelle clé),
— condensats de la famille SHA2 (SHA-256).

Les transparents de l'annonce sont en ligne <http://www.ripe.net/ripe/meetings/ripe-59/presentations/uploads/presentations/Tuesday/Plenary%2014:00/Abley-DNSSEC_for_the_Root_Zone.mId7.pdf>. Un site officiel d'informations sur le processus a été créé en <http://www.root-dnssec.org/>.

La signature de la racine soulève quelques problèmes techniques spécifiques liés à l'augmentation de taille des réponses <https://www.bortzmeyer.org/dns-size.html>, problèmes discutés en "*Preparing K-root for a Signed Root Zone*" <http://labs.ripe.net/content/preparing-k-root-signed-roo