

# Valider la racine du DNS

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 Juillet 2010

<http://www.bortzmeyer.org/valider-racine.html>

---

Comme tout le monde le sait, la racine du DNS a été complètement signée (c'est-à-dire avec publication de la clé) le 15 juillet dernier. Comment valider des noms de domaine avec DNSSEC désormais ?

D'abord, un pré-requis : la racine étant signée en utilisant l'algorithme SHA-256 (comme le sera `.fr` le 14 septembre prochain), il faudra des logiciels assez récents. Le RFC 5702<sup>1</sup> qui normalisait l'usage de SHA-256 ne date que d'octobre 2009. Pour BIND, il faut une version  $\geq 9.6.2$  pour valider la racine. Pour Unbound <<http://www.bortzmeyer.org/unbound.html>>, une version  $\geq 1.4$  (publiée le 26 novembre 2009). Avant cela, Unbound 1.3 pouvait utiliser SHA-256 mais, c'était une option de compilation `--enable` (qui n'était pas activée par défaut).

Ensuite, il faut mettre la clé publique de la racine comme clé de confiance ("*trust anchor*") dans la configuration du résolveur validant. On pourrait la récupérer dans le DNS lui-même (`dig DNSKEY .`) mais ce serait stupide, puisque non sécurisé. DNSSEC ne résoudra aucun problème de sécurité si on gère les clés aussi imprudemment. Il faut donc un canal sécurisé et authentifié pour amorcer la validation DNSSEC. La clé de la racine est distribuée officiellement par l'IANA en <<https://data.iana.org/root-anchors/root-anchors.xml>>. On peut authentifier avec uniquement X.509 puisque c'est du HTTPS. Mais le fichier est aussi signé avec PGP et on peut donc le valider ainsi. Il est signé avec la clé 0x0F6C91D2, qui est elle-même signée par plusieurs personnes connues avec lesquelles vous aurez peut-être un chemin de confiance. La clé 0x0F6C91D2 se trouve sur les serveurs de clé et aussi en <<https://data.iana.org/root-anchors/icann.pgp>>. Un exemple de validation est :

```
wget -nc -O root-anchors.xml https://data.iana.org/root-anchors/root-anchors.xml
wget -nc -O root-anchors.asc https://data.iana.org/root-anchors/root-anchors.asc
gpg --verify root-anchors.asc root-anchors.xml
```

Le fichier de la clé de confiance est au format XML et contient un enregistrement DS. Pour le convertir au format qu'attendent nos résolveurs, il y a plusieurs solutions. Pour Unbound, qui accepte les enregistrements DS comme clés de confiance, j'ai fait un petit script (en ligne sur <http://www.bortzmeyer.org/files/anchors2ds.xsl>) en XSLT qui fait cette conversion. Par exemple :

---

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc5702.txt>

```
% xsltproc anchors2ds.xml root-anchors.xml
. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
```

Le processus peut s'automatiser à l'aide de mon Makefile (en ligne sur <http://www.bortzmeyer.org/files/anchors2ds.make>).

Pour BIND, qui n'accepte pas les enregistrements DS mais seulement les DNSKEY, c'est un peu plus compliqué. La solution que j'utilise est à base de cut, de sed et de awk et n'est peut-être pas très robuste mais elle marche. Le principe est de récupérer la clé dans le DNS, de manière non sécurisée, puis de fabriquer le DS avec l'outil BIND `dnssec-dsfromkey`, puis de comparer avec la DS obtenue de l'IANA. C'est également automatisé dans le Makefile (en ligne sur <http://www.bortzmeyer.org/files/anchors2ds.make>).

Donc, pour Unbound, il faut taper `make root-anchors.txt` puis mettre le contenu de `root-anchors.txt` dans `unbound.conf` par exemple :

```
trust-anchor: ". IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5"
```

Pour BIND, on tape `make root-anchors.dnskey` puis on met le contenu de ce fichier dans `named.conf`. Doit-on le mettre dans `trusted-keys` (clés statiques) ou bien dans `managed-keys` (clés mises à jour automatiquement suivant le RFC 5011)? À l'heure actuelle, il ne semble pas que les gestionnaires de la racine aient formellement annoncé qu'ils utiliseraient le RFC 5011 donc je préfère le `trusted-keys` :

```
trusted-keys {
. 257 3 8 "
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW008gcCjF FVQUTf6v58fLjwBd0YI0Ezr
AcQqBGCzh/RStIo08g0NfnfL2MTJRkxoX bfDaUeVPQuYEhg37NzWAJQ9VnmMVDxP/VHL496M/QZxkjf5
/Efucp2gaD X6RS6CXpoY68LsvPVjr0ZSwzzlapAzvN9dlzEheX7ICJBBtuA6G3LQpz W5hOA2hzCTMj
JPJ8LbqF6dsV6DoBQZgul0sGIcGOYl7OyQdXfZ57re1S Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmR
LKBP1dfwhYB4N7knNnulq QxA+Uk1ihz0= ";
```

Il existe d'autres solutions pour BIND : le script `ta-tool` <<http://www.kirei.se/xfiles/dnssec/ta-tool.pl>>, le script `rootanchorkeys` <<http://www.mork.no/~bjorn/rootanchor2keys.pl>>, on peut aussi par exemple utiliser les scripts <<https://itar.iana.org/instructions/>> qui avaient été conçus pour ITAR <<http://www.bortzmeyer.org/itar-dnssec.html>>. Le format des fichiers XML n'est pas le même donc ces scripts ne fonctionnent pas directement avec `root-anchors.xml`, il faut les convertir, à la main, ou bien via un script que vous allez devoir écrire. Une autre solution est de tout faire manuellement comme indiqué en « *Using the root DNSSEC key in BIND 9 resolvers* » <<http://www.isc.org/community/blog/201007/using-root-dnssec-key-bind-9-resolvers>> » ou dans « *How to set up DNSSEC validation with BIND-9.7* » <<http://fanf.livejournal.com/107310.html>> ».

Sauf si vous faites confiance au RFC 5011, pensez surtout à recommencer les étapes ci-dessus lors de la sortie de la prochaine clé de la racine, dans quelques années. Cette sortie sera sans doute annoncée très largement.

Merci à Alain Thivillon pour son aide.