RFC 4034 : Resource Records for the DNS Security Extensions

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 avril 2008

Date de publication du RFC : Mars 2005

https://www.bortzmeyer.org/4034.html

Complétant la série des RFC sur DNSSEC, ce RFC 4034[1] décrit les types d'enregistrements utilisés par ce protocole, DNSKEY, RRSIG, DS et NSEC.

DNSSEC, décrit dans les RFC 4033 et RFC 4035, permet de **signer** cryptographiquement les **enregistrements** DNS de façon à garantir leur authenticité. Pour cela, DNSSEC ne modifie pas le format des paquets DNS, mais il ajoute plusieurs types d'enregistrement nouveaux. Notre RFC fait partie de la série de RFC qui décrit DNSSEC-bis (la première version de DNSSEC, assez différente, n'ayant eu aucun succès) et il succède au RFC 2535.

La plupart des exemples ci-dessous ont été obtenus pour la zone sources.org qui est désormais signée. Vous pouvez interroger en DNSSEC ses serveurs de noms (dig NS sources.org. vous en donnera la liste).

Chacun des nouveaux types d'enregistrement va faire l'objet d'une section. La section 2 est consacrée à DNSKEY, les clés publiques des zones. Un de ces enregistrements stocke notamment l'algorithme de chiffrement utilisé et la clé. La représentation texte officielle (chaque type d'enregistrement DNS a une représentation binaire, utilisée sur le câble, et une représentation texte, utilisée par exemple dans les fichiers de zone de BIND), décrite en section 2.2, affiche la clé encodée en Base64 :

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

```
sources.org.                        86400   DNSKEY  256 3 3 (
   CL9vwM+5gCMZdycMOYJQ7lSspHDTsaZmZkDR
   l+KNx/VytmbPSfcdYmhJJHyTdGpzqXmm6qEd
   4Kpyqbd59RXv9JCVVM3MntiX/hruxbB3WsV0
   hlVej1IuWFDncJFLWhaD9UjgGm+UoqlQJGVJ
   rGZf7KvwL4iKZhr1fiDEJFD7e9cxU8dojhHp
   mmAOZLjEYKytDMB0rj8/Mnm5cVVu29UFS+0y
   jvkdbQD0EJ9FwF/8MwG4DHj6ZtFwxeNp2NCD
   6oj0kxDi5ktY0rQtSv506aAMmGBqS6tNno+g
   9KgCLZ5jk5e8fpl9Rlmd2SlVMAyf8E3C9joB
   ZqCqYX+VcooSrcvgn/4m6CTDPxK+DuE+KW5/
   NiE062MKdID7xAxiCj14Suj9K9TKL60buuFa
   gJ3qTjhS5C62uPk8U9+zHpQ0qjcb0gv3/M+l
   RcXi46g0OF17cTLy83lgU6s2ApMmaboeUbm2
   3lfCEl8B6R2BhE98mfoDNg+Xlj63X8w93LCo
   XP/c1SZivNolol/Ky6apULe3euFuwdOFfYCR
   ) ; key id = 55957
```

Ici, la clé 55957 utilise DSA/SHA-1 (valeur 3). Ces clés peuvent être générées, par exemple, par le programme `dnssec-keygen`, qui fait partie de BIND. Bien lire la liste des algorithmes utilisables pour une zone dans l'annexe A.1 sinon, on aura un message du genre "*a key with algorithm 'HMAC-SHA256' cannot be a zone key*".

Les enregistrements `RRSIG` sont le cœur de DNSSEC, puisqu'ils stockent les signatures des autres enregistrements. Ce sont les `RRSIG` que vérifie un validateur DNSSEC. Un enregistrement `RRSIG` contient notamment :

— le type de l'enregistrement couvert par la signature,
— l'algorithme de chiffrement utilisé (la liste des algoritmes possibles à l'origine figure dans l'annexe A.1 et la liste actuelle `<https://www.iana.org/assignments/dns-sec-alg-numbers>` est maintenue par l'IANA),
— les dates de signature et d'expiration,
— la signature elle-même.

Sous la forme texte décrite en section 3.2, voici un tel enregistrement :

```
laperouse.sources.org.  86400   IN MX   10 aetius.bortzmeyer.org.
                        86400   RRSIG   MX 3 3 86400 20080522104407 (
                                        20080422104407 55957 sources.org.
                                        CIxBOzsaxBexcAQQE1ukqNfBz5yDnPBVhgxr
                                        MNR7FrfM2iH/AOWoO/8= )
```

Ici, ce `RRSIG` signe un `MX`.

La section 4 est consacrée à `NSEC`, un type d'enregistrement qui va résoudre un problème délicat, la « preuve de non-existence ». En effet, DNSSEC fonctionne en joignant une signature aux enregistrements existants, ce qui permet de prouver leur existance. Mais si un nom n'existe pas et que le serveur veut renvoyer `NXDOMAIN` ("*No Such Domain*")? On ne peut pas signer un enregistrement qui n'existe pas. La solution DNSSEC est de créer des enregistrements `NSEC` qui sont signés et qui indiquent l'enregistrement **suivant** (l'ordre est défini dans la section 6, c'est simplement l'ordre des codes ASCII). Ainsi, si je demande `nexistepas.example.org` et que je récupère :

```
lulu.sources.org.    43200   IN      NSEC    patou.sources.org. AAAA RRSIG NSEC
```

je sais que nexistepas.sources.org n'existe pas, puique le NSEC ci-dessus me garantit qu'il n'y a rien entre lulu et patou.

Un autre type d'enregistrement permettant la « preuve de non-existence », le NSEC3, est décrit dans le RFC 5155. En effet, le NSEC a un gros inconvénient, il permet l'**énumération** complète de la zone, en suivant simplement les NSEC. Cette faiblesse des NSEC est une des raisons pour lesquelles DNSSEC n'a pas été d'avantage déployé.

C'est très bien de signer sa zone mais ensuite, comment les résolveurs partout dans le monde vont-ils connaitre sa clé ? Ils ont pu l'obtenir par un autre moyen et la mettre dans leur configuration (ce qu'on nomme une "*trust anchor*"). Mais un tel mécanisme ne se généralise évidemment pas à tout l'Internet. Il faut donc un seul "*trust anchor*", la clé de la racine, et un système de délégations. Ces délégations sont mises en œuvre par les enregistrements DS, décrits en section 5. Ces enregistrements contiennent un condensat cryptographique de la clé :

```
sources.org.            IN DS 55957 3 1 A12F149F84B34E09501C32CC9F984FB9E1ED196A
```

Ici, 55957 est l'identité de la clé, 3 l'algorithme de la clé et 1 celle du condensat (SHA-1, la liste complète <https://www.iana.org/assignments/ds-rr-types> est maintenue par l'IANA).