RFC 3757 : Domain Name System KEY (DNSKEY) Resource Record (RR) Secure Entry Point (SEP) Flag

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 janvier 2009

Date de publication du RFC : Avril 2004

https://www.bortzmeyer.org/3757.html

Le protocole DNSSEC de signature des enregistrements DNS par des signatures cryptographiques repose sur des clés dont la partie publique est distribuée dans le DNS lui-même. La partie privée sert à signer les enregistrements ou d'autres clés. Certaines de ces clés ne servent qu'à signer des clés, afin d'être moins exposées que les autres. Pour permettre de distinguer ces clés, un bit spécial est réservé par ce RFC.

DNSSEC est normalisé dans les RFC 4033 [1] et suivants. Ces documents ont intégré une distinction, qui n'existait pas dans le protocole originel, et qui a été introduite par notre RFC 3757, entre les clés servant à signer les enregistrements, les **ZSK** ("*Zone Signing Key*") et les clés servant à signer d'autres clés, les **KSK** ("*Key Signing Key*"). Depuis la publication du RFC 4034, notre RFC 3757 est donc dépassé mais il garde son intérêt historique.

Faire cette distinction entre ZSK et KSK n'est pas obligatoire. On peut parfaitement faire du DNSSEC avec une seule clé, à la fois ZSK (servant à signer la zone) et KSK (mise dans les résolveurs validateurs, ou bien envoyée au registre de la zone parente pour qu'il la publie sous forme d'enregistrement DS). Pour le protocole de validation des enregistrements (RFC 4035), ZSK et KSK sont identiques (voir section 3).

Mais cette simplification présente un inconvénient : comme la clé va servir à signer des enregistrements, qui peuvent être très nombreux, et que les signatures sont renouvelées souvent (par défaut, un mois, avec BIND), et que les données DNS sont publiques, on va fournir à un cryptanalyste beaucoup de matériel. Et, en cryptographie, plus on a de matériel signé à analyser, plus on a de chances.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4033.txt

Il est donc recommandé de changer de clé souvent. Mais, si cette clé a été publiée, que ce soit via une page Web (comme le fait IIS <https://www.iis.se/docs/ksk.txt>, le registre de .se) ou bien via une zone parente, changer cette clé est pénible et le risque que certains continuent à utiliser l'ancienne clé est non négligeable.

D'où l'idée, qui est au cœur de notre RFC, d'avoir deux genres de clé. Comme le note la section 1, en pastichant La ferme des animaux, « toutes les clés sont égales mais certaines sont plus égales que d'autres ».

Il y a donc désormais deux sortes de clé, différenciées par un bit dans le champ "*Flags*" de l'enregistrement DNSKEY (RFC 4034, section 2.1) :

— Les ZSK ("*Zone Signing Key*"), où ce bit vaut zéro, et qui servent à signer les enregistrements. Elles ne sont pas publiées « officiellement » et ne doivent donc jamais se retrouver dans un fichier de configuration. Pour les raisons expliquées plus haut, elles doivent être changées relativement souvent (par exemple tous les six mois).
— Les KSK ("*Key Signing Key*"), où ce bit vaut un, et qui servent uniquement à signer les ZSK. Utilisées pour un plus petit nombre d'enregistrements, elles peuvent être de longueur plus grande, et sont changées moins souvent (par exemple tous les deux ans). Elles sont typiquement publiées par la zone parente, ou bien sur une page Web sécurisée (comme au RIPE-NCC <https://www.ripe.net/projects/disi//keys/index.html>). (Comme le rappelle la section 5, l'existence du bit SEP ne suffit pas en elle-même, car un attaquant a pu le définir. Il faut donc récupérer la KSK par un canal sûr.) Les KSK peuvent alors être mises dans la configuration d'un résolveur validateur, d'où le nom de SEP ("*Secure Entry Point*") que leur donne ce RFC.

(La section 1 du RFC détaille tous ces points.)

La section 2 normalise le format du bit SEP. C'est le quinzième du champ "*Flags*" de l'enregistrement DNSKEY donc celui du plus faible poids (il est enregistré dans le registre IANA <https://www.iana.org/assignments/dnskey-flags/dnskey-flags.xhtml>). Si la valeur du champ "*Flags*" est paire, c'est une ZSK, si elle est impaire, c'est une KSK. Si je demande les DNSKEY du domaine generic-nic.net, j'obtiens :

```
% dig DNSKEY generic-nic.net.
...
generic-nic.net.        64800   IN      DNSKEY  256 3 5 AwEAAbLKp5/pZ+5E8nZgxRiUzr1hxV8Y64/63JUqttROZKqkvnAs
generic-nic.net.        64800   IN      DNSKEY  256 3 5 AwEAAfNNMrML2opUMF4ImMpy8fr90YCb/czyb3ASxMys1FlbbQRS
generic-nic.net.        64800   IN      DNSKEY  257 3 5 AwEAAd+KNrUQaor2JiLB/oodx9HrUjiGBjn5WpsZHiu2a7oTQYTi
```

Le champ "*Flags*" est le premier après le type DNSKEY. Les deux premières clés sont des ZSK (bit de plus faible poids à zéro), la troisième une KSK (notez aussi sa longueur plus importante, elle fait 4096 bits, contre 1024 pour les ZSK, c'est l'option -b du dnssec-keygen de BIND). (Il y a deux ZSK car l'une est la future clé de signature, publiée en avance, RFC 6781, section 4.1.1.1.) -f KSK

La section 4 rappelle un mode d'emploi des différentes clés, mais le RFC 6781, plus récent, est une meilleure source.

Avec les outils de gestion de clés de BIND, la génération d'une KSK se fait simplement en ajoutant l'option -f KSK.