# Combiner DNSSEC avec les mises à jour dynamiques

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 novembre 2009

https://www.bortzmeyer.org/dnssec-dynupdate.html

---

Un certain nombre de zones DNS sont mises à jour par le protocole "*Dynamic Update*" du RFC 2136[1]. Peut-on encore signer les données ainsi avitaillées, pour DNSSEC ? Même avec NSEC3 ? Même avec l'"*opt-out*" ? La réponse est oui.

Le fonctionnement le plus courant de DNSSEC est de signer la zone d'un coup, avec un outil comme `dnssec-signzone` de BIND ou comme `ldns-signzone` de ldns <http://www.nlnetlabs.nl/projects/ldns/>. Mais un tel mode n'est pas compatible avec les mises à jour dynamiques ("*dynamic updates*") du RFC 2136).

Une solution est mise en œuvre par BIND, sous le nom de "*online key*" (cf. RFC 3007). Si le serveur a accès à la clé privée, il peut signer les nouveaux enregistrements qui arrivent. Les exemples suivants ont été testés avec la version beta de BIND 9.7. Ils marcheraient sans doute avec des versions antérieures mais la 9.7 apporte suffisamment de choses du point de vue de DNSSEC pour que cela vaille la peine.

Voici la configuration de BIND :

```
zone "example" {
        type master;
        allow-update {
              localhost; // Cette ACL est définie par défaut dans BIND
        };
        file "example.db.signed";
};
```

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2136.txt`

On est parti d'une zone ordinaire, qu'on a signé avec une clé de type NSEC3RSASHA1 (NSEC3 est normalisé dans le RFC 5155 et rend le recalcul des signatures plus délicat). La suite de l'évolution de la zone se fera uniquement par mise à jour dynamique.

Un exemple de script de mise à jour est :

```
#!/bin/sh

NUM=$(date +%s)
PID=$$

nsupdate -d <<EOF
  server ::1 8053
  zone example
  update add created-dyn-$NUM-$PID.example 3600 NS ns1.nic.example
  send
EOF
```

Il contacte le serveur local (adresse `::1`), sur le port 8053 et lui demande d'ajouter un enregistrement pour le nom `created-dyn-$NUM-$PID.example` (qui n'existait pas avant). Ce genre d'ajout est typique de l'activité d'un TLD (une zone DNS ordinaire utiliserait plutôt des enregistrements de type A ou AAAA).

La mise à jour se passe bien :

```
% ./dynupdate
Sending update to ::1#8053
...
;; UPDATE SECTION:
created-dyn-1258541343-2833.example.    3600    IN      NS      ns1.nic.example.
...
Reply from update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:   1926
;; flags: qr ; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
```

Et le serveur de noms note :

```
18-Nov-2009 11:27:47.327 client ::1#46234: updating zone 'fr/IN': adding an RR at 'created-dyn-1258541343-28
18-Nov-2009 11:27:47.708 zone fr/IN: sending notifies (serial 2222229958)
```

Et on peut vérifier que le serveur connait bien le nouvel enregistrement :

```
% dig +dnssec -p 8053 @::1 ANY  created-dyn-1258541343-2833.example.
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1019
...
;; AUTHORITY SECTION:
created-dyn-1258541343-2833.example.    3600    IN      NS      ns1.nic.example.
DE3SCFLTLOBRFQAAO85TGISFO23QDLO5.example. 5400 IN NSEC3 1 1 10 F00DCAFE FU8ND8DK3QVMR9JNDR9LIM31K0RPAS43 NS
...
```

Comme les enregistrements de délégation, les NS, ne font pas autorité, la réponse ne figure pas dans la section Réponse mais dans la section Autorité. Les enregistrements NSEC3 sont inclus dans la réponse mais ils ne sont pas modifiés par les ajouts dynamiques puisqu'on est en "*opt-out*", on ne modifie pas les chaînes NSEC3 pour des enregistrements ne faisant pas autorité. (BIND découvre tout seul que la zone avait été signée avec "*opt-out*", en regardant le champ "*Flags*" de l'enregistrement NSEC3 précédent, cf. section 3.1.2 du RFC 5155. L'enregistrement NSEC3PARAM ne peut pas être utilisé, car son champ "*opt-out*" est toujours à zéro, cf. section 4.1.2 du RFC 5155, cet enregistrement ne servant qu'à informer les serveurs secondaires.)

Passons maintenant à l'enregistrement d'un domaine signé, ayant un enregistrement DS, qui fera donc autorité. On modifie le script :

```
#!/bin/sh

NUM=$(date +%s)
PID=$$

nsupdate -d <<EOF
  server ::1 8053
  zone fr
  update add created-dyn-$NUM-$PID.example 3600 NS ns1.nic.example
  update add created-dyn-$NUM-$PID.example 3600 DS 24045 7 1 c5746...
  send
EOF
```

Et, cette fois, le nombre d'enregistrements NSEC3 dans la zone change, BIND en a ajouté automatiquement un.

Toutes ces signatures nécessitent évidemment que BIND aie accès à la clé **privée** (c'est-à-dire le fichier `Kexample.+007+39888.private` où 39888 est l'identicateur de la clé). BIND la cherche dans le répertoire indiqué par l'option `directory`. (BIND peut aussi utiliser PKCS #11 pour parler à un équipement qui garde la clé.)

Si jamais on a « retiré le tapis » de sous les pieds du serveur de noms, par exemple en déplaçant les clés (les fichiers `Kexample...`), logiquement, BIND n'arrive plus à signer :

```
18-Nov-2009 11:05:03.162 client ::1#32072: updating zone 'example/IN': found no private keys, unable to generate
18-Nov-2009 11:05:03.162 client ::1#32072: updating zone 'example/IN': RRSIG/NSEC/NSEC3 update failed: not found
```

et il renvoie donc SERVFAIL au client.

Enfin, on peut noter que, bien que le RFC 3007 le permettre, il n'est pas actuellement possible de calculer la signature dans le client avant de l'envoyer au serveur :

```
18-Nov-2009 12:29:36.777 client ::1#36479: updating zone 'example/IN': update failed: \
    explicit RRSIG updates are currently not supported in secure zones \
    except at the apex (REFUSED)
```

Un bon article sur le même sujet, allant jusqu'à la création d'un service de DNS dynamique, est « "*How-To : Create your own 'DynDNS' Service*" <https://www.chrisk.de/posts/2011/02/how-to-create-your-> ».

---