RFC 3007 : Secure Domain Name System (DNS) Dynamic Update

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 mai 2010

Date de publication du RFC : Novembre 2000

https://www.bortzmeyer.org/3007.html

Comment combiner le mécanisme de signature DNSSEC (normalisé à l'époque dans le RFC 2535 [1], aujourd'hui dans le RFC 4033) avec les mises à jour dynamiques du DNS par le protocole du RFC 2136 ? Ce RFC détaille les questions que cette combinaison pose et apporte des réponses.

La méthode la plus classique pour signer une zone DNS avec DNSSEC est de le faire sur une zone complète (typiquement un fichier de zone au format décrit par la section 5 du RFC 1035) avec un outil comme `dnssec-signzone` (dans BIND) ou bien OpenDNSSEC. Mais parfois, la zone est avitaillée (contenu créé, modifié et détruit) par les "*dynamic updates*" du RFC 2136. Peut-on encore la signer dans ce cas ? Oui. Ce RFC, successeur du RFC 2137 explique comment (ce RFC a lui-même été légèrement mis à jour par les RFC ultérieurs comme le RFC 4035). Le principe est simple : le client doit s'authentifier, par exemple avec TSIG (RFC 2845) et le serveur doit signer lui-même les données mises à jour (ce qui implique qu'il connaisse la clé secrète DNSSEC, ou bien qu'il aie accès à un dispositif de signature comme un HSM, cf. section 4.3). Un logiciel comme BIND sait aujourd'hui faire cela <https://www.bortzmeyer.org/dnssec-dynupdate.html>. L'articulation entre l'authentification de la mise à jour dynamique et celle, ultérieure, faite avec DNSSEC, est expliquée en sections 1.3 et 1.4.

Petit rappel en section 1.1 la mise à jour dynamique se fait en indiquant l'opération d'avitaillement souhaitée (ajout ou suppression, la modification se faisant en combinant les deux, section 2.5 du RFC 2136) et ses valeurs. Avec `nsupdate`, voici un exemple :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2535.txt`

```
# Génération de la clé
dnssec-keygen -a HMAC-SHA256 -b 256 -n HOST dynamic.test-update

# Configuration de BIND
key "dynamic.test-update." {
        algorithm hmac-sha256;
        secret "TRESSECRET=";
};
zone "dynamic.test" {
       type master;
       file "dynamic.test";
        allow-update {
                key "dynamic.test-update.";
        };
};

# Commande de mise à jour
nsupdate -kKdynamic.test-update.+163+49211 -d <<EOF
server localhost
zone dynamic.test
update add toto$$.dynamic.test 600 A 192.0.2.1
send
EOF

# Le journal de BIND
May 20 08:28:19 golgoth named[836]: client ::1#65379: signer "dynamic.test-update" approved
May 20 08:28:19 golgoth named[836]: client ::1#65379: updating zone 'dynamic.test/IN': adding an RR at 'toto
```

L'authentification de la requête (ici, avec la clé contenue dans les fichiers `Kdynamic.test-update.+163+49211` est évidemment impérative. La signature avec DNSSEC ne servirait à rien, si n'importe qui pouvait modifier la zone ! La section 2 détaille cette authentification et explique que, même si les enregistrements DNS transmis sont déjà signés, cela ne **doit pas** être utilisé pour authentifier la requête de mise à jour, qui doit se faire avec TSIG (comme dans mes exemples) ou SIG(0) (RFC 2931, qui n'est jamais utilisé en pratique).

À noter que la même section (et aussi la 4.1) précise qu'on peut quand même envoyer des enregistrements déjà signés (à condition que la requête soit authentifiée autrement) mais BIND, dans sa version 9.7, ne les accepte pas.

La section 3 rappelle que l'acceptation ou pas d'une mise à jour d'une zone signée dépend de la politique locale. Avec un BIND, voici un exemple :

```
# Configuration de BIND
options {
        ...
        key-directory "/etc/namedb/keys"; // Les fichiers K* sont mis
// dans ce répertoire
...
// Pas d'autre changement pour BIND, qui détecte tout seul que la zone
// est signée et qu'il est responsable de la signature de nouveaux
// enregistrements.

# Commande de mise à jour identique : le client n'a rien à faire

# Journal de BIND
May 20 08:43:53 golgoth named[1188]: client ::1#65345: signer "dynamic.test-update" approved
May 20 08:43:53 golgoth named[1188]: client ::1#65345: updating zone 'dynamic.test/IN': adding an RR at 'tot

# Et le nouvel enregistrement a été signé :
% dig +dnssec @localhost A toto668.dynamic.test
...
;; ANSWER SECTION:
toto668.dynamic.test.   600     IN      A       192.0.2.1
toto668.dynamic.test.   600     IN      RRSIG   A 5 3 600 20100619064353 20100520054353 39751 dynamic.test.
```

Notons que BIND ne met pas en œuvre toutes les recommandations de cette section. Par exemple la 3.1 suggère fortement que la politique de modification puisse dépendre du type (`A`, `AAAA`, `MX`, etc) mais cela n'est pas possible avec BIND.

La mise à jour dynamique nécessite des règles spécifiques pour certains types d'enregistrements. On a vu que l'envoi de `RRSIG` (les signatures, appelées `SIG` à l'époque de notre RFC 3007) était permis par le protocole (mais pas par BIND). En revanche, la mise à jour des enregistrements de non-existence (les `NXT` à l'époque, devenus depuis les `NSEC` et `NSEC3`) est explicitement interdite (section 3.1.1) car ils doivent être correctement chaînés et seul le serveur connait toute la zone. BIND crée donc tout seul les `NSEC` et `NSEC3` lors de l'ajout ou de la suppression d'un nom.

Enfin, les risques de sécurité entraînés par cette technique (puisque le serveur de noms doit connaître la clé privée, et qu'elle doit donc être « en ligne », d'accès plus facile pour un éventuel attaquant) sont détaillés en section 5.

Pour les détails pratiques de mise en œuvre, voir mon article « Combiner DNSSEC avec les mises à jour dynamiques <https://www.bortzmeyer.org/dnssec-dynupdate.html> ».