Un exemple de remplacement de clé DNSSEC, avec OpenDNSSEC

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 octobre 2012

http://www.bortzmeyer.org/key-rollover.html

Si vous avez déjà un peu regardé DNSSEC, vous avez dû noter qu'on vous suggère fortement de remplacer ("*to roll over*") les clés cryptographiques de temps en temps. La nécessité de ces remplacements ne fait pas l'unanimité, notamment en raison de sa complexité. Toutefois, avec les outils modernes, le problème est nettement simplifié. Voici l'exemple pas-à-pas du récent remplacement de la KSK ("*Key Signing Key*") du domaine bortzmeyer.fr.

Le domaine est hébergé chez moi, le serveur maître est un nsd <http://www.bortzmeyer.org/nsd.html> et les clés sont gérées par OpenDNSSEC <http://www.bortzmeyer.org/opendnssec-debut.html>, ce qui simplifie beaucoup les choses. Le principe d'OpenDNSSEC est qu'on exprime la **politique** (taille des clés, remplacement, durée de vie) dans le fichier de configuration et OpenDNSSEC s'occupe de tout. Le fichier de configuration est bien documenté <https://wiki.opendnssec.org/display/DOCS/kasp.xml>. Voici la configuration de la KSK ("*Key Signing Key*") de mes zones :

```
<KSK>
   <Algorithm length="2048">8</Algorithm> <!-- 8 = RSA/SHA-256 -->
   <Lifetime>P2Y</Lifetime> <!-- P2Y = two years . Probably useless
   if we have ManualRollover set -->
   <Repository>SoftHSM</Repository>
   <ManualRollover/>
</KSK>
```

Il existe évidemment des tas d'autres politiques possibles, configurables dans kasp.xml, par exemple en utilisant des "*Standby Keys*" (<Standby>1</Standby>), où la clé est générée mais pas publiée dans le DNS.

À noter que l'utilisation de nsd nécessite un petit bricolage d'intégration avec OpenDNSSEC <http://www.bortzmeyer.org/opendnssec-nsd.html>.

Voyons maintenant l'opération. La KSK avait le "*keytag*" 44461. DNSviz <http://dnsviz.net/> affiche l'ancienne configuration :

Le 5 octobre vers 1000 UTC, je lance le processus :

```
# ods-ksmutil key rollover --zone bortzmeyer.fr --keytype KSK
```

La nouvelle clé, la 3445 est créé et aussitôt publiée dans le DNS. (J'ai un moniteur de mes zones qui surveille les clés et leurs remplacements, le code est sur Github <https://github.com/bortzmeyer/key-checker>, il m'a servi pour un article à la conférence SATIN <http://www.bortzmeyer.org/satin.html> et m'a prévenu tout de suite de l'arrivée de la nouvelle clé.)

Mais la nouvelle clé n'est pas utilisable tout de suite : il faut attendre la réjuvénation <http://www.bortzmeyer.org/dns-propagation.html> complète dans le DNS, des caches ont encore le vieil ensemble DNSKEY. C'est pour cela qu'OpenDNS affiche pour cette clé 3445 un état "*publish*" et pas encore "*active*" :

```
# ods-ksmutil key list --zone bortzmeyer.fr  --verbose
bortzmeyer.fr                   KSK           active    2012-10-05 12:14:02 ... 44461
bortzmeyer.fr                   KSK           publish   2012-10-06 00:14:03 ... 3445
```

(Les états d'OpenDNSSEC ont fait l'objet d'un autre article <http://www.bortzmeyer.org/opendnssec-states.html>.) Les durées (par exemple le TTL) sont configurées également dans kasp.xml, éléments <TTL>, <*Safety>, etc.

Pas besoin de surveiller en permanence, OpenDNSSEC se charge de vérifier qu'il n'y aura pas d'erreur de "*timing*" (cf. RFC 7583 [1]). C'est donc seulement trois jours après que j'ai repris le dossier. 3445, toujours publiée, a changé d'état :

```
bortzmeyer.fr                   KSK           ready     waiting for ds-seen ... 3445
```

Le remplacement d'une KSK nécessite une interaction avec le parent. OpenDNSSEC n'a pas à l'heure actuelle de code pour vérifier que l'interaction a été faite (on peut utiliser pour cela le script de Mathieu Arnold <https://gist.github.com/3945132>) et l'enregistrement DS publié. Il faut donc lui indiquer, une fois la manipulation faite. Les bureaux d'enregistrement le font souvent par EPP (RFC 5910, et cela peut s'automatiser, voir par exemple un script de Mathieu Arnold <https://gist.github.com/3143290>). Les autres passent en général par un formulaire Web. (Une solution utilisant le DNS a depuis été normalisée dans le RFC 7344 mais n'est pas très répandue encore.) Dans mon cas, la zone parente était .fr donc l'AFNIC, et le bureau d'enregistrement était Gandi. Je demande à OpenDNSSEC le DS :

```
# ods-ksmutil key export --ds
SQLite database set to: /var/lib/opendnssec/db/kasp.db
;active KSK DS record (SHA1):
bortzmeyer.fr.  3600    IN      DS      3445 8 1 53ad69094ea377347c5538f076d889af5a4f6243
;active KSK DS record (SHA256):
bortzmeyer.fr.  3600    IN      DS      3445 8 2 7cc6f2980fd42b5fbf587cad5b00712bfe568343691135434b719c2bebc
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7583.txt

Et je soumets la clé à l'AFNIC, via Gandi (je l'ai fait à la main mais, là encore, Mathieu Arnold a un script pour automatiser cela <https://gist.github.com/3135484>, via l'API de Gandi)

Le second DS a été publié quelque temps après (une vérification technique est systématiquement faite avec Zonecheck <http://www.bortzmeyer.org/zonecheck-3-0.html>, ce qui est particulièrement important pour DNSSEC, plus sensible aux erreurs de configuration). dig montrant que le second DS est bien là (rappelez-vous bien de **tester** à chaque fois avant de passer à l'étape suivante), je le dis à OpenDNSSEC :

```
# ods-ksmutil key ds-seen --zone bortzmeyer.fr --keytag 3445
SQLite database set to: /var/lib/opendnssec/db/kasp.db
Found key with CKA_ID 02656a5fe158c6e25f7c965eb9a1ca3d
Key 02656a5fe158c6e25f7c965eb9a1ca3d made active
Old key retired
```

Ainsi prévenu, OpenDNSSEC change l'état de la clé :

```
# ods-ksmutil key list --zone bortzmeyer.fr  --verbose
SQLite database set to: /var/lib/opendnssec/db/kasp.db
Keys:
Zone:                           Keytype:      State:    Date of next transition: ...      Keytag:
bortzmeyer.fr                   KSK           retire    2012-10-09 17:52:03      ...      44461
bortzmeyer.fr                   KSK           active    2013-10-09 13:05:24      ...      3445
```

L'ancienne clé, la 44461 est toujours publiée dans le DNS à ce stade. Dès que les caches auront tous le nouveau DS, elle sera abandonnée. En effet, le lendemain, elle a disparu :

```
# ods-ksmutil key list --zone bortzmeyer.fr  --verbose
SQLite database set to: /var/lib/opendnssec/db/kasp.db
Keys:
Zone:                           Keytype:      State:    Date of next transition:  ...      Keytag:
bortzmeyer.fr                   KSK           active    2013-10-09 13:05:24       ...      3445
```

Tout est donc terminé. Il n'a fallu que trois étapes explicites de ma part :

— Lancer le processus de remplacement avec `ods-ksmutil key rollover`,
— Transmettre le DS au registre, via le BE,
— Prévenir OpenDNSSEC que cette étape a été terminée, avec `ods-ksmutil key ds-seen`.

Tout le reste est automatique. OpenDNSSEC s'occupe de tout et surveille le "*timing*" (ainsi, `ods-ksmutil key export` n'acceptera pas d'exporter la clé si elle n'a pas été créée depuis assez longtemps).