RFC 8078 : Managing DS records from the Parent via CDS/CDNSKEY

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 mars 2017

Date de publication du RFC : Mars 2017

https://www.bortzmeyer.org/8078.html

Un problème fréquent avec DNSSEC est de transmettre à sa zone parente les clés publiques de signature de sa zone, pour que le parent puisse signer un lien qui va vers ces clés (l'enregistrement de type DS). Le RFC 7344 [1] apportait une solution partielle, avec ses enregistrements CDS et CDNSKEY. Il y manquait deux choses : la création du premier DS (activation initiale de DNSSEC), et le retrait de tout les DS (on arrête de faire du DNSSEC). Ce nouveau RFC 8078 comble ces deux manques (et, au passage, change l'état du RFC 7344, qui passe sur le Chemin des Normes).

Avant le RFC 7344, tout changement des clés KSK ("*Key Signing Key*") d'une zone nécessitait une interaction avec la zone parente, par le biais d'un mécanisme non-DNS (« "*out-of-band*" », par exemple un formulaire Web). La solution du RFC 7344, elle, n'utilise que le DNS (« "*in-band*" »). Ce nouveau RFC complète le RFC 7344 pour les configurations initiales et finales. (Le problème est complexe car il peut y avoir beaucoup d'acteurs en jeu. Par exemple, le BE n'est pas forcément l'hébergeur DNS. Ces difficultés ont certainement nui au déploiement de DNSSEC.)

Lorsqu'on change d'hébergeur DNS, la solution la plus propre est de faire un remplacement des clés, depuis celle de l'ancien hébergeur jusqu'à celle du nouveau. Cette solution préserve en permanence la sécurité qu'offre DNSSEC. Mais une des procédures mentionnées par notre RFC passe au contraire par un état non sécurisé, où la zone n'est pas signée. C'est dommage mais cela est parfois nécessaire si :

— Les logiciels utilisés ne permettent pas de faire mieux, ou l'un des deux hébergeurs ne veut pas suivre la procédure « propre »,
— Ou bien le nouvel hébergeur ne gère pas DNSSEC du tout, ou encore le titulaire de la zone ne veut plus de DNSSEC.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7344.txt

Une zone non signée vaut certainement mieux qu'une signature invalide. Mais le RFC oublie de dire que cela va casser certaines applications de sécurité qui exigent DNSSEC comme DANE (RFC 6698) ou SSHFP (RFC 4255).

Avant de lire la suite de ce RFC, deux conseils :
— Lisez bien le RFC 7344. Vraiment.
— Rappelez-vous qu'il y a des tas d'acteurs possibles dans le DNS. Le modèle RRR (Titulaire-BE-Registre, "*Registrant-Registrar-Registry*") n'est **pas** le seul. Et il n'y a pas que les TLD qui délèguent des zones ! Le RFC parle donc uniquement de « parent » (responsable parental ?) pour désigner l'entité à laquelle on s'adresse pour obtenir des changements dans la zone parente.

Les enregistrements CDS ("*Client-side Delegation Signer*") servent à trois choses (section 2 du RFC) :
— Installer le DS ("*Delegation Signer*") initial dans la zone parente,
— Remplacer ("*rollover*") la clé publique de signature des clés (KSK, "*Key-Signing Key*") dans la zone parente,
— Supprimer le DS de la zone parente, débrayant ainsi la validation DNSSEC de la zone fille chez les résolveurs.

Avec le RFC 7344, seule la deuxième était possible (c'est la moins dangereuse, qui ne nécessite aucun changement dans les relations de confiance,notamment entre parente et fille). Notre RFC 8078 permet désormais les deux autres, plus délicates, car posant davantage de problèmes de sécurité.

La sémantique des enregistrements CDS (ou CDNSKEY) est donc désormais « la publication d'un ou plusieurs CDS indique un souhait de synchronisation avec la zone parente ; celle-ci est supposée avoir une politique en place pour accepter/refuser/vérifier ce ou ces CDS, pour chacune des trois utilisations notées ci-dessus ». Quand des CDS différents des DS existants apparaissent dans la zone fille, le responsable parental doit agir.

D'abord, l'installation initiale d'un DS alors qu'il n'y en avait pas avant (section 3 du RFC). La seule apparition du CDS ou du CDNSKEY ne peut pas suffire car comment le vérifier, n'ayant pas encore de chaîne DNSSEC complète ? Le responsable parental peut utiliser les techniques suivantes :
— Utiliser un autre canal, extérieur au DNS, par exemple l'API du responsable parental,
— Utiliser des tests de vraisemblance, du genre un message de confirmation envoyé au contact technique du domaine, ou bien regarder si la configuration du domaine est stable,
— Attendre un certain temps, de préférence vérifier depuis plusieurs endroits dans le réseau (pour éviter les empoisonnements locaux), puis considérer le CDS comme valable s'il est resté pendant ce temps (l'idée est qu'un piratage aurait été détecté, pendant ce délai),
— Envoyer un défi au titulaire de la zone fille, par exemple génerer une valeur aléatoire et lui demander de l'insérer sous forme d'un enregistrement TXT dans la zone (bien des applications qui veulent vérifier le responsable d'un domaine font cela, par exemple Keybase <`https://keybase.io/`> ou bien Google webmasters),
— Accepter immédiatement s'il s'agit d'une nouvelle délégation. Ainsi, le domaine sera signé et validable dès le début.

La deuxième utilisation des CDS, remplacer une clé est, on l'a vu, déjà couverte par le RFC 7344.

Et pour la troisième utilisation, la suppression de tous les DS chez le parent ? Elle fait l'objet de la section 4 du RFC. Pour demander cette suppression, on publie un CDS (ou un CDNSKEY) avec un champ « algorithme » à zéro. Cette valeur n'est pas affectée à un vrai algorithme dans le registre officiel <`https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml#dns-sec-alg-numbers-1`>, elle est réservée (cf. section 6 du RFC) pour dire « efface ». (Le RFC 4398 utilisait déjà le même truc.)

Pour éviter tout accident, le RFC est plus exigeant que cela et exige cette valeur spécifique pour ces enregistrements :

```
DOMAINNAME IN CDS 0 0 0 0
```

ou bien :

```
DOMAINNNAME IN    CDNSKEY 0 3 0 0
```

(Le 3 étant l'actuel numéro de version de DNSSEC, voir le RFC 4034, section 2.1.2.)

Une fois le CDS (ou CDNSKEY) « zéro » détecté, et validé par DNSSEC, le parent retire le DS. Une fois le TTL passé, le fils peut « dé-signer » la zone.

À noter que ce RFC a été retardé par la question du déplacement du RFC 7344, de son état « pour information », au Chemin des Normes. La demande était discrète, et avait été raté par certains relecteurs, qui ont protesté ensuite contre ce « cavalier ». L'« élévation » du RFC 7344 est désormais explicite.

Cette possibilité est opérationnelle en .ch ou .cz. Jan-Piet Mens a fait un excellent article sur son utilisation dans .ch <https://jpmens.net/2021/10/05/dnssec-cds-cdnskey-in-the-real-world/>.