RFC 7344 : Automating DNSSEC Delegation Trust Maintenance

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 septembre 2014. Dernière mise à jour le 12 septembre 2014

Date de publication du RFC : Septembre 2014

https://www.bortzmeyer.org/7344.html

Un des obstacles à un plus large déploiement de DNSSEC est la nécessité de faire mettre, par le gestionnaire de la zone parente, un enregistrement faisant le lien avec la clé de signature de la zone fille. Cet enregistrement, nommé DS (pour "*Delegation Signer*") est indispensable pour établir la chaîne de confiance qui va de la racine du DNS à la zone qu'on veut sécuriser. Mais, autant signer sa zone ne nécessite que des actions locales, qu'on peut faire tout seul, mettre cet enregistrement DS dans la zone parente nécessite une interaction avec une autre organisation et d'autres personnes, ce qui est souvent compliqué et réalisé d'une manière non standardisée. Ce nouveau RFC propose une méthode complètement automatique, où la zone fille publie les enregistrements de clé localement, et où la zone parente va les chercher (via le DNS) et les recopier.

Faire passer de l'information de la zone fille à la zone parente se fait actuellement avec des mécanismes ad hoc, par exemple via un formulaire Web ou une API chez le BE (cf. section 2.2 du RFC). Un exemple de l'opération est décrit dans mon article sur le remplacement d'une clé <https://www.bortzmeyer.org/key-rollover.html>. Il faut transmettre les clés (ou leur condensat, le futur enregistrement DS, cf. RFC 4034 [1]) à la zone parente pour que la zone soit vérifiable avec DNSSEC. Et il faut le refaire lorsqu'on change la clé. Comme pour tout processus qui franchit les frontières entre deux organisations humaines, bien des choses peuvent aller de travers, surtout lorsqu'il est partiellement effectué manuellement. Et l'absence de techniques normalisées rend difficile le changement de prestataire.

Notre nouveau RFC propose donc une autre méthode : le gestionnaire de la zone signée publie ses clés uniquement dans **sa** zone, et la zone parente l'interroge à la recherche de nouvelles clés à publier. La sécurité du processus est assurée par les signatures DNSSEC. Ce mécanisme ne marche donc que

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4034.txt

pour les mises à jour, pas pour la configuration initiale (puisque celle-ci ne peut pas être vérifiée par DNSSEC). Depuis, le RFC 8078 a présenté un moyen de faire la configuration initiale.

En attendant le déploiement du RFC 8078, ce mécanisme supprimera néanmoins une opération pénible et qui est apparemment mal maitrisée par bien des gérants de zones DNS. Naturellement, les anciennes solutions resteront disponibles pour ceux qui préfèrent, et pour le premier envoi des clés, lorsque la zone devient signée. À noter que cette solution est spécifique aux informations DNSSEC (clés de signature). Il y a d'autres informations qu'on pourrait vouloir transmettre automatiquement au parent (serveurs de noms, colle) mais cela dépendra d'autres RFC.

Un petit mot de terminologie : il existe plusieurs mécanismes de gestion (au sens organisationnel) de la relation entre une zone DNS parente et une zone fille. Cette relation peut être directe (par exemple, dans une université, entre l'administrateur de la zone du département de mathématiques et l'administrateur de la zone de l'université), indirecte (passage par un intermédiaire, le BE, imposé, celui-ci communiquant ensuite avec le registre, souvent via EPP) ou complexe (gestion de la racine où le gérant d'un TLD passe par l'ICANN pour un changement qui est fait par le NTIA et Verisign). Pour traiter tous ces cas, le RFC utilise le terme d'« agent du parent » ("*parental agent*") pour désigner l'entité avec lequel le gestionnaire de la zone fille communique, que cette entité soit le gestionnaire de la zone parente ou pas. L'agent du parent est donc l'administrateur de la zone de l'université dans le premier cas, le BE dans le second et l'ICANN dans le troisième. L'annexe A de notre RFC revient en détail sur ces différents modèles et leurs conséquences.

À noter d'ailleurs une complication supplémentaire : le titulaire de la zone fille ne gère pas forcément ses serveurs DNS lui-même (section 2.2.1 du RFC). Il a pu les déléguer à un tiers, l'hébergeur DNS, ou à son agent du parent (il est fréquent que les gens qui louent un nom de domaine à un BE lui confient également l'hébergement DNS). Dans ce dernier cas, tout est simple, l'utilisateur active la signature DNSSEC (ça peut même être fait par défaut, pour épargner ce choix technique à l'utilisateur) et l'hébergeur DNS s'occupe de tout.

Autre point à garder en tête : on peut transmettre à la zone parente un enregistrement DS (le condensat d'une clé) ou bien DNSKEY. Certains gérants de zones demandent un DS, d'autres un DNSKEY, d'autres acceptent les deux. La solution technique de ce RFC marche dans tous les cas.

Voyons maintenant la solution technique choisie. Elle est décrite en section 3. Deux nouveaux enregistrements DNS sont créés, CDS et CDNSKEY, correspondant respectivement aux DS et DNSKEY. Ils sont publiés dans la zone fille (le C initial veut dire "*Child*") et indiquent à la zone parente les informations que la zone fille veut lui transmettre. Le CDS, type 59, a le même format que le DS (RFC 4034, section 5) et le CDNSKEY, type 60, le même format que le DNSKEY (RFC 4034, section 2). Comme on l'a vu plus haut, certains parents demandent un DS, d'autre un DNSKEY. La fille peut publier juste le CDS ou juste le CDNSKEY, selon la parente, ou bien les deux.

L'utilisation de CDS et de CDNSKEY (section 4) est facultative. S'ils sont absents, tout continue comme aujourd'hui. S'ils sont présents, la zone parente qui les détecte peut les publier sous forme d'enregistrement DS (en copiant le CDS ou bien en calculant un DS à partir du CDNSKEY). CDS et CDNSKEY doivent évidemment être signés avec DNSSEC (autrement, on pourrait empoisonner la zone parente) et doivent correspondre à ce qui est réellement dans la zone fille (par exemple, le CDS doit correspondre à une DNSKEY réellement existante). Le mécanisme marche aussi pour les suppressions, la zone parente pouvant retirer les DS qui n'ont plus de CDS mais avec des précautions (section 4.1) : pas question de « dé-sécuriser » la zone en retirant tous les DS valides, par exemple (la possibilité de retrait de DS de la zone parente est, à mon avis, pas très clairement expliquée dans le RFC, mais le RFC 8078 a présenté une solution). La parente peut ensuite prévenir la fille que les nouveaux DS ont été pris en compte et les anciens retirés (par exemple par courrier). Une fois que c'est fait, la zone fille peut

supprimer CDS et CDNSKEY. (Attention à bien les supprimer tous : si on en supprime certains, la zone parente va retirer les DS correspondants. Aucun CDS/CDNSKEY ne veut pas dire « supprimer tous les DS » mais « ne faire aucun changement .)

(Au passage, pourquoi avoir un CDNSKEY, pourquoi la zone parente ne regarde pas directement le DNSKEY ? Il y a deux raisons : la première est qu'en général, on ne veut pas publier le DS tout de suite, on souhaite d'abord tester la configuration DNSSEC pendant plus ou moins longtemps. La zone va donc rester signée mais pas rattachée de manière sécurisée à sa parente. Ce rattachement doit être volontaire et explicite car, à partir du moment où il est fait, les erreurs DNSSEC ne pardonnent plus. La deuxième raison est qu'il peut y avoir plusieurs clés dans la zone fille, dont certaines sont, par exemple, en cours de retrait et ne doivent pas être utilisées pour faire un DS.)

Comment l'agent du parent sait-il qu'une zone fille a publié de nouveaux CDS ou CDNSKEY ? Une possibilité est l'interrogation régulière des zones. C'est simple à faire et automatique pour le gérant de la zone fille mais cela peut poser des problèmes de performance pour, par exemple, un gros BE qui gérerait des centaines de milliers de zones (section 6.1). Une autre est de fournir aux clients un bouton à pousser sur un formulaire Web quelconque, indiquant qu'il y a du nouveau dans la zone. Cette deuxième possibilité peut aussi permettre, si le formulaire Web est authentifié et qu'on présente à l'utilisateur le DS pour vérification, de faire l'ajout initial du DS (cela suppose que l'utilisateur fasse une vérification sérieuse…voir à ce sujet le RFC 8078). On peut aussi envisager une API simple pour cela, mais rien n'est encore normalisé. (C'était l'une des plus grosses controverses lors du développement de ce RFC : la méthode décrite ici doit-elle être **la** méthode officielle ou bien juste une méthode parmi d'autres ? Pour l'instant, c'est la seule normalisée mais elle n'est nullement obligatoire.)

La section 9 du RFC est l'analyse de sécurité de ce système. En automatisant le plus possible la transmission des clés de la fille à la parente, on espère augmenter la sécurité, en diminuant les risques d'erreurs humaines (copier/coller maladroit d'une DS dans un formulaire Web, par exemple). Cette décroissance des incidents aiderait au déploiement de DNSSEC. Mais il n'y a pas de miracle : le gérant de la zone fille pourra toujours faire des bêtises comme de supprimer de sa zone toutes les DNSKEY correspondant aux DS dans la zone parente.

Si le système d'avitaillement de la zone fille est piraté, le pirate pourra évidemment créer des CDS et CDNSKEY signés. Bien sûr, aujourd'hui, il peut déjà créer des enregistrements mais, dans ce cas, cela permettra peut-être d'étendre la durée de l'attaque (il faudra republier les bons CDS/CDNSKEY et attendre la mise à jour de la parente).

Dans le cas où la la gestion de la zone fille est sous-traitée à un hébergeur DNS, cette nouvelle technique a l'avantage que l'hébergeur DNS peut publier les CDS/CDNSKEY lui-même et donc mettre à jour la zone parente sans qu'on ait besoin de lui confier le mot de passe du compte chez le BE.

On peut mettre facilement des CDS et des CDNSKEY dans BIND depuis la version 9.10.1. Sinon, quels « agents de parent » mettent en œuvre ce RFC ? Pour l'instant, le serveur FRED <https://fred.nic.cz/>, et ça marche dans .cz. Et, sinon, il existe un logiciel public qui fait ce travail de récupération et validation des CDS et CDNSKEY, cds-monitor <https://github.com/fcelda/cds-monitor>. Jan-Piet Mens a fait un récit de son utilisation avec PowerDNS et BIND <http://jpmens.net/2017/09/21/parents-children-cds-cdnskey-records-and-dnssec-cds/> et l'outil dnssec-cds.