RFC 9975 : Clarifications on CDS/CDNSKEY and CSYNC Consistency

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 mai 2026

Date de publication du RFC : Mai 2026

https://www.bortzmeyer.org/9975.html

Pour compléter un processus de sécurisation des noms de domaine avec DNSSEC, il faut transmettre au domaine parent votre clé publique. Le faire manuellement via l'interface Web du BE n'est pas pratique donc il existe un moyen d'automatiser cela, les CDS/CDNSKEY, moyen décrit dans le RFC 7344 [1]. Mais attention à la sécurité ! Ce moyen n'est sûr que si on suite quelques précautions, décrites dans ce nouveau RFC.

Bon, je sais, j'ai simplifié, on ne transmet pas forcément au domaine parent sa clé publique mais parfois un condensat de celle-ci. (Le domaine parent publiera ensuite un enregistrement DS, contenant un condensat que vous aurez donné ou bien qu'il aura calculé à partir de la clé.) Ça ne change pas grand'chose en pratique. Le RFC 7344 décrit comment automatiser le changement de clé en publiant dans **son** domaine des enregistrements CDS et/ou CDNSKEY, qui informent le parent. (Et le RFC 9615 permet de le faire pour la configuration initiale, pas juste pour un changement.) Avec une technique proche, les enregistrements CSYNC du RFC 7477, on peut aussi automatiser le changement des serveurs de noms faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>.

À partir de là, le gestionnaire du domaine parent (typiquement un registre de noms de domaine) va récupérer ces enregistrements et agir (modifier les enregistrements DS et NS dans son domaine). La façon la plus simple de récupérer les CDS, CDNSKEY et CSYNC est de faire une bête requête DNS classique, donc via son résolveur <https://www.bortzmeyer.org/resolveur-dns.html> par défaut :

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

```
% dig turris.cz CDS
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16850
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
turris.cz.  5 IN CDS 53148 13 2 9A0E997A2992D4089CE39C1976DC65C00C9D20A6C36187F897E71D6E 23368E6E

;; Query time: 24 msec
;; SERVER: 192.168.2.254#53(192.168.2.254) (UDP)
;; WHEN: Fri Jan 09 11:15:20 CET 2026
;; MSG SIZE  rcvd: 86

% dig alatienne.fr CDNSKEY
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53877
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
alatienne.fr.  3600 IN CDNSKEY 257 3 13 (
    mdsswUyr3DPW132mOi8V9xESWE8jTo0dxCjjnopKl+Gq
    JxpVXckHAeF+KkxLbxILfDLUT0rAK9iUzy1L53eKGQ==
    ) ; KSK; alg = ECDSAP256SHA256 ; key id = 2371

;; Query time: 52 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu Feb 05 16:35:32 CET 2026
;; MSG SIZE  rcvd: 229
```

Mais cette méthode n'est pas très sûre et nous allons voir pourquoi, et comment arranger les choses.

Ici, la réponse CDS était signée par DNSSEC (le "*flag*" `ad`, pour "*Authentic Data*"). Mais ce n'est pas toujours le cas (avec les CSYNC, ou tout simplement lors de la configuration initiale de DNSSEC, cf. RFC 8078). Le fond du problème est que les serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> pour le domaine qui publie CDS, CDNSKEY ou CSYNC peuvent être en désaccord. (Ou bien, mais le RFC ne semble pas le mentionner, il y a eu empoisonnement de la mémoire du résolveur.) Ce désaccord peut être dû à un piratage d'un des serveurs (ou à une malveillance de ses opérateurs) mais il peut être aussi le résultat d'un cafouillage technique <https://www.bortzmeyer.org/dns-afrinic-stale.html> (un serveur ne se synchronisant plus) ou organisationnel, les serveurs n'étant pas forcément gérés par la même entité. Sans compter le risque d'une délégation boiteuse ("*lame delegation*") où un des serveurs listés dans l'ensemble NS n'est pas censé être serveur pour ce domaine. D'ailleurs, même DNSSEC ne protège pas dans tous les cas, s'il y a plusieurs signeurs (RFC 8901), ils peuvent aussi déconner séparement. Avec le comportement par défaut du résolveur typique (accepter la réponse du premier serveur faisant autorité qui répond), un seul des serveurs faisant autorité peut déclencher un changement de configuration dans le domaine parent. Le cœur de notre nouveau RFC est de dire que le logiciel qui récupère CDS/CDNSKEY/CSYNC doit s'assurer que les serveurs faisant autorité sont **cohérents**, qu'ils renvoient tous la même réponse.

Cela ne peut pas se faire via un résolveur typique, je n'en connais pas qu'on puisse configurer pour faire cela, il faut donc interroger directement les serveurs faisant autorité. Par exemple, pour la requête dig ci-dessus, un moyen de le faire serait, par exemple en shell :

```
% for ns in $(dig +short turris.cz NS); do
  dig @$ns +short turris.cz CDS
done
53148 13 2 9A0E997A2992D4089CE39C1976DC65C00C9D20A6C36187F897E71D6E 23368E6E
53148 13 2 9A0E997A2992D4089CE39C1976DC65C00C9D20A6C36187F897E71D6E 23368E6E
53148 13 2 9A0E997A2992D4089CE39C1976DC65C00C9D20A6C36187F897E71D6E 23368E6E
```

Et il faudrait ensuite s'assurer que toutes les réponses sont identiques. Sinon, le domaine parent s'abstient d'agir. (Comme les lecteurs et lectrices de ce blog sont très fort·es en réseau, ielles ont certainement remarqué que j'avais simplifié : comme un serveur peut avoir plusieurs adresses IP, il faudrait les tester toutes. Des exemples de programmes plus perfectionnés figurent par la suite.)

Ces nouvelles règles amènent à mettre à jour quelques RFC, qui ne les spécifiaient pas : les RFC 7344 et la section 3.1 du RFC 7477, qui conseillait de ne demander qu'à un seul serveur faisant autorité (ce que fait le résolveur typique mais qui n'est pas assez sûr).

La section 3 du RFC liste plus formellement les nouvelles exigences :

— Tester la présence et le contenu des CDS/CDNSKEY/CSYNC via **toutes** les adresses IP des serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>.
— Toutes les réponses **doivent** être identiques.
— On peut arrêter le test dès qu'au moins une des réponses correspond au DS/NS existant. Cela veut dire qu'au moins un des serveurs faisant autorité ne veut pas qu'on change.

Si et seulement si toutes les réponses sont identiques, et différentes de la situation actuelle, le gestionnaire du domaine parent peut envisager de modifier NS et DS.

Notez que, si les serveurs faisant autorité utilisent l'"*anycast*", le test ne sera pas complet, le vérificateur de cohérence ne testera qu'une seule instance d'un nuage "*anycast*". Dans ce cas, il peut être intéressant de tester la cohérence depuis plusieurs points de mesure, pour avoir des chances de contacter plusieurs instances "*anycast*".

La même règle s'applique aux enregistrements CSYNC du RFC 7477. La section 3.2 de notre RFC détaille comment traiter ces enregistrements, qui permettent notamment de synchroniser les enregistrements NS du domaine parent (et la colle <https://www.afnic.fr/observatoire-ressources/papier-expert/le-dns-ca-colle-ou-ca-ne-colle-pas/>) avec ceux du domaine fils. Il y a une petite nuance pour le numéro de série de la zone que contient l'enregistrement CSYNC (il doit être identique à celui du SOA du même serveur, pas forcément à ceux des CSYNC des autres serveurs faisant autorité).

La section 5 de notre RFC discute les conséquences pour la sécurité. Si on ne fait pas les vérifications décrites ici, il y a un risque de copier dans la zone parente des données incorrectes, voire créées par un attaquant, par exemple parce qu'il a réussi à pirater un des serveurs faisant autorité ou bien parce qu'il gérait un de ces serveurs mais agissant sans autorisation du gérant de la zone (cas courant si on sous-traite certains de ses serveurs secondaires). Ce RFC privilégie donc l'intégrité des données, au risque, on peut le remarquer, qu'un changement souhaité prenne davantage de temps, si un des serveurs faisant autorité a des problèmes. Que faire si un de ces serveurs ne veut vraiment pas jouer le jeu et, par exemple, ne se synchronise plus et ne publie pas le nouveau CDS/CDNSKEY/CSYNC ? La section 5 dit qu'il faut donc maintenir un canal traditionnel (via le BE, par exemple <https://www.afnic.fr/observatoire-ressources/papier-expert/que-se-passe-t-il-quand-on-enregistre-un-nom-de-dom>), pour pouvoir changer quand même les données publiées par la zone parente. C'est par exemple le rôle d'EPP (RFC 5730).

Cette vérification de la cohérence a déjà été mise en œuvre dans les logiciels de TANGO <https://www.knipp.de/it-es/tango> et CORE <https://corenic.org/>, ainsi que déployée par le registre suisse. Zonemaster <https://zonemaster.fr/> fait ce test <https://doc.zonemaster.net/latest/specifications/tests/DNSSEC-TP/dnssec15.html>.

Enfin, l'annexe A du RFC décrit plus en détail des scénarios où l'incohérence entre les serveurs faisant autorité pour un domaine a eu des conséquences fâcheuses. Par exemple, si un domaine a une délégation

boiteuse, vers un serveur qui n'existe pas, un malveillant peut créer le serveur en question, mettre un CSYNC en indiquant uniquement des serveurs qu'il contrôle et transformer une simple délégation boiteuse en un détournement complet du nom. Si le serveur non-existant était dans un nom de domaine non enregistré, l'attaquant n'a qu'à enregistrer ce nom (attaque flamant). Si le serveur non-existant était sur une adresse IP libre chez un hébergeur public, l'attaquant n'a qu'à créer des machines chez cet hébergeur jusqu'à tomber sur l'adresse en question (une variante de l'attaque des sous-domaines). Ce genre d'attaques est décrit dans des articles comme « "*Unresolved Issues : Prevalence, Persistence, and Perils of Lame Delegations*" <https://dl.acm.org/doi/10.1145/3419394.3423623> » ou « "*Risky BIZness : risks derived from registrar name management*" <https://dl.acm.org/doi/10.1145/3487552.3487816> ». Bon, si le domaine est signé avec DNSSEC, il est protégé, non ? Oui, sauf si l'attaquant peut changer la clé avec un CDS. . .D'où l'importance de la vérification de cohérence de ce RFC.

Autre exemple d'accident possible (et qui n'est pas dû à une attaque délibérée), dans le cas où un domaine a plusieurs signeurs DNSSEC (RFC 8901), si un des serveurs faisant autorité ne publie que ses propres clés dans un CDS. Sans vérification de cohérence, au lieu d'avoir plusieurs DS comme prévu, on n'en aura qu'une partie.

Et si vous cherchez un programme simple qui fait à peu près ce que demande le RFC, vous avez :

```
% ./cds-consistency.py knot-resolver.cz
knot-resolver.cz is consistent, data is "None"

% ./cds-consistency.py àlacon.fr
àlacon.fr is consistent, data is "7177 13 2 fa99827c7aca1681b8905285e7fa33ec5adccb430393b4fa1e9f9aa3d926370
```