RFC 4431 : The DNSSEC Lookaside Validation (DLV) DNS Resource Record

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 3 novembre 2006. Dernière mise à jour le 14 novembre 2007

Date de publication du RFC : Février 2006

https://www.bortzmeyer.org/4431.html

L'une des faiblesses les plus souvent citées du DNS est son manque de sécurité. Pour authentifier les données servies, le protocole DNSSEC a été développé, dans les RFC 4033 [1] et suivants. Notre RFC vient d'ajouter un nouveau type de données, pour indiquer une racine de signature différente de la "vraie" racine. (Notez que ce RFC a ensuite été ramené à la catégorie « Intérêt historique seulement », en novembre 2019, et que DLV est donc abandonné depuis, voir le RFC 8749.)

DNSSEC calque sa structure sur celle du DNS : hiérarchique, avec une racine, gérée par le gouvernement des États-Unis, via l'IANA. Normalement, la racine est signée par l'IANA, qui signe les délégations des TLD qui à leur tour signent les délégations des titulaires de noms de domaine. (Ces délégations apparaissent dans les enregistrements de type DS - "*Delegation Signer*".)

Mais cette hiérarchie pose des problèmes : que faire si l'IANA, par exemple parce que l'ICANN est bloquée par des problèmes politiciens, ne veut ou ne peut pas signer la racine ? (Aujourd'hui, la seule racine du DNS signée l'est en PGP et par Verisign, l'opérateur à qui le gouvernement états-unien a délégué la gestion technique de la racine. Elle est accessible en <ftp://rs.internic.net/domain/root.zone.gz>, la signature étant dans le même répertoire.)

D'ou l'idée de base de DLV ("*DNSSEC Lookaside Validation*") : dissocier la racine du DNS et la racine de signature DNSSEC. Avec DLV, on peut créer une racine de signature en, par exemple, `dlv.isc.org` et la peupler d'enregistrements DLV. Si les résolveurs DNS sont configurés pour les chercher là, DNSSEC marchera bien et on aura contourné le problème policitien.

Les enregistrements DS sont donc remplacés par des DLV, spécifiés dans notre RFC, et qui ont exactement le même format. BIND les met en œuvre depuis la version 9.3.2 et 9.4.0. Voici un exemple de récupération de DLV avec dig :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc4033.txt`

```
% dig DLV sources.org.dlv.isc.org.

; <<>> DiG 9.5.0-P2 <<>> DLV sources.org.dlv.isc.org.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30687
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;sources.org.dlv.isc.org.       IN      DLV

;; ANSWER SECTION:
sources.org.dlv.isc.org. 3600   IN      DLV     22107 5 2 AF12A23DFBCDB5609DCEC2C2FBD3CD65AEEFE49CBE0751C650
sources.org.dlv.isc.org. 3600   IN      DLV     14347 3 2 0D5D5B209264BBA5EDAEC9B95843901073BF27F01702B144FE
...
```

À noter que notre RFC normalise un format de données, pas la façon de l'utiliser. C'est l'objet du RFC 5074 qui, entre autres, décrit ce qui se passe si deux racines DLV coexistent, peut-être pour des parties différentes du DNS.