RFC 6605 : Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 avril 2012

Date de publication du RFC : Avril 2012

http://www.bortzmeyer.org/6605.html

Le mécanisme de sécurité DNSSEC permet évidemment de choisir entre plusieurs algorithmes de signature cryptographique, à la fois pour pouvoir faire face aux progrès de la cryptanalyse et pour pouvoir choisir en fonction de critères particuliers (taille des clés, temps de signature et de vérification, etc). La palette de choix s'agrandit avec ce RFC qui normalise l'usage d'ECDSA, un algorithme à courbes elliptiques (le deuxième dans DNSSEC après le RFC 5933 [1]).

DNSSEC est normalisé dans le RFC 4033 et les suivants. Il permet d'authentifier les enregistrements DNS par une signature cryptographique et l'algorithme de loin le plus fréquent aujourd'hui est RSA, avec des clés de 1024 ou 2048 bits. Beaucoup de gens préfèrent les courbes elliptiques, décrites dans l'excellent RFC 6090. Notre RFC étend donc la liste des algorithmes disponibles à :

— ECDSA avec la courbe P-256 et l'algorithme de condensation SHA-256. On considère généralement que cette courbe a à peu près la résistance de RSA avec des clés de 3072 bits.
— ECDSA avec la courbe P-384 et l'algorithme de condensation SHA-384.

ECDSA est normalisé dans FIPS 186-3 <http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf>. Les paramètres des courbes sont pris dans le RFC 5114.

Les clés ECDSA et les signatures étant bien plus petites que celles de RSA, on peut espérer des économies sur la capacité réseau. Signer est également bien plus rapide avec ECDSA (20 fois plus dans certains tests). Par contre, vérifier les signatures est plus long (5 fois plus dans certains tests) et le processeur des résolveurs DNS validants va donc souffrir.

Au passage, notre RFC normalise aussi (section 2) l'utilisation de SHA-384 dans DNSSEC, ce qui n'avait pas été fait précédemment (mais n'a aucun rapport avec les courbes elliptiques). SHA-384 était

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5933.txt

déjà décrit dans le RFC 6234 et DNSSEC a juste eu à lui ajouter un numéro de code <https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xml>, 4. (La première personne qui voit un DS de numéro 4 dans la nature est priée de me le signaler, pour ma collection.)

La section 4 décrit les formats utilisés pour DNSSEC. Une clé publique ECDSA est juste une valeur, notée Q, qu'on met telle quelle dans l'enregistrement DNSKEY. La signature, elle, est faite de deux valeurs, r et s. On les concatène simplement avant de les mettre dans le RRSIG. Les codes enregistrés <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml#dns-sec-alg-numbers-1> pour les deux nouveaux algorithmes sont 13 pour "*ECDSA Curve P-256 with SHA-256*" et 14 pour "*ECDSA Curve P-384 with SHA-384*". (Là encore, si quelqu'un en trouve dans la nature, je suis preneur...)

La section 6 fournit des exemples. Voici une clé et le DS correspondant, avec le premier algorithme (notez la petite taille par rapport aux DNSKEY RSA) :

```
example.net. 3600 IN DNSKEY 257 3 13 (
           GojIhhXUN/u4v54ZQqGSnyhWJwaubCvTmeexv7bR6edb
           krSqQpF64cYbcB7wNcP+e+MAnLr+Wi9xMWyQLc8NAA== )

example.net. 3600 IN DS 55648 13 2 (
           b4c8c1fe2e7477127b27115656ad6256f424625bf5c1
           e2770ce6d6e37df61d17 )
```

Et les signatures qui l'utilisent (également toutes petites) :

```
www.example.net. 3600 IN A 192.0.2.1
www.example.net. 3600 IN RRSIG A 13 3 3600 (
           20100909100439 20100812100439 55648 example.net.
           qx6wLYqmh+l9oCKTN6qIc+bw6ya+KJ8oMz0YP107epXA
           yGmt+3SNruPFKG7tZoLBLlUzGGus7ZwmwWep666VCw== )
```

Question mises en œuvre, on notera qu'OpenSSL, bibliothèque utilisée par de nombreux programmes DNS, a ECDSA, avec nos deux courbes (au moins depuis la version 1.0.1, celle que j'ai testée). C'est apparemment activé par défaut (il faut faire un `./config no-ecdsa` pour ne **pas** l'avoir). Voir le source dans `crypto/ecdsa`. Mais le code a été retiré de certains systèmes (comme Fedora) en raison des brevets, une infection fréquente pour les courbes elliptiques.

Dans les serveurs de noms, le seul à gérer déjà ECDSA semble être PowerDNS <http://doc.powerdns.com/dnssec-supported.html>. BIND ne semble pas avoir encore ECDSA (version 9.9, la dernière officiellement publiée). Même chose pour Unbound dans sa version 1.4.16, la dernière. nsd comprend ECDSA depuis la version 3.2.11, publiée en juillet 2012. Enfin, pour Go-DNS <http://miek.nl/projects/godns/>, c'est en cours de développement. Enfin, pour la bibliothèque ldns <http://nlnetlabs.nl/projects/ldns>, ECDSA a été ajouté dans la version 1.6.13, sortie en mai 2012. Pour les autres, il va donc falloir patienter un peu. Notez que certains des registres de noms de domaine ont une liste limitative des algorithmes acceptés et que cette liste ne comprend pas forcément déjà ECDSA.

Si vous voulez regarder une zone signée avec ECDSA (c'est très rare), il y a `ecdsa.isc.org`.