

RFC 5933 : Use of GOST signature algorithms in DNSKEY and RRSIG Resource Records for DNSSEC

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 Juillet 2010

Date de publication du RFC : Juillet 2010

<http://www.bortzmeyer.org/5933.html>

L'algorithme de signature russe GOST R 34.10-2001 ayant été spécifié en anglais dans le RFC 5832¹, plus rien ne s'opposait à son utilisation dans DNSSEC. Ce RFC marque donc l'arrivée d'un nouvel algorithme dans les enregistrements DNSSEC, algorithme portant le numéro 12.

La liste originelle des algorithmes DNSSEC figurait dans le RFC 4034, annexe A.1. La liste actuelle est un registre à l'IANA, <<http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml#dns-sec-alg-numbers-1>>. Elle comprend désormais GOST. Notez que GOST désigne en fait une organisation de normalisation, le terme correcte serait plutôt « GOST R 34.10-2001 » pour l'algorithme de signature et « GOST R 34.11-94 » pour celui de hachage, décrit dans le RFC 5831 (voir la section 1 de notre RFC 5933).

La section 2 décrit le format des enregistrements DNSKEY avec GOST, dans lequel on publie les clés GOST R 34.10-2001. Le champ Algorithme vaut 12, le format de la clé sur le réseau suit le RFC 4491. GOST est un algorithme à courbes elliptiques, courbes décrites par $Q = (x,y)$. Les 32 premiers octets de la clé sont x et les 32 suivants y (en petit-boutien, attention, contrairement à la majorité des protocoles Internet). Les autres paramètres de la clé figurent dans le RFC 4357.

Les bibliothèques cryptographiques existantes sont parfois capables de lire des clés GOST (section 2.1). Pour OpenSSL, il existe une distribution de GOST <http://www.cryptocom.ru/OpenSource/OpenSSL_eng.html> (par la même entreprise où travaille l'auteur des RFC GOST).

La section 2.2 donne un exemple de clé GOST publiée dans le DNS mais autant utiliser ici un exemple réel :

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc5832.txt>

```
% dig DNSKEY m-system.net

; <<>> DiG 9.6-ESV-R1 <<>> DNSKEY m-system.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43317
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;m-system.net. IN DNSKEY

;; ANSWER SECTION:
m-system.net. 86400 IN DNSKEY 257 3 12 BDtDa2UxLe7cdDs9bX/X1Y/UXuhJnDrGDRuVQW0BBo8QF1Pr959WBI5Q y1NxyKp9Rm4y
m-system.net. 86400 IN DNSKEY 256 3 12 vvJWsxH3J5IZ6YEcG1C+MaYGX/YwzIeFoIXgUOuGHx/fvet0SJefkPE0 i140Sm4T4y5

;; Query time: 159 msec
;; SERVER: ::1#53(::1)
;; WHEN: Mon Jun 28 08:59:27 2010
;; MSG SIZE rcvd: 201
```

La section 3 décrit le format des enregistrements RRSIG, les signatures. On suit les RFC 4490 et RFC 4357. Voici un exemple actuellement présent dans le DNS :

```
% dig +dnssec MX m-system.net

; <<>> DiG 9.6-ESV-R1 <<>> +dnssec MX m-system.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56828
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;m-system.net. IN MX

;; ANSWER SECTION:
m-system.net. 86400 IN MX 10 mail.m-system.net.
m-system.net. 86400 IN RRSIG MX 12 2 86400 20100723062450 20100623062450 64666 m-system.net. kfb73QrBWmzQb8p

;; AUTHORITY SECTION:
m-system.net. 86400 IN NS ns.cplire.ru.
m-system.net. 86400 IN NS step.reedcat.net.
m-system.net. 86400 IN RRSIG NS 12 2 86400 20100723062450 20100623062450 64666 m-system.net. YQ+taRLlgemXVk

;; Query time: 219 msec
;; SERVER: ::1#53(::1)
;; WHEN: Mon Jun 28 08:58:57 2010
;; MSG SIZE rcvd: 331
```

Attention, une particularité de GOST fait que deux signatures des mêmes données peuvent donner des résultats différents, car un élément aléatoire est présent dans la signature.

La section 4 décrit le format des enregistrements DS pour GOST. La clé publique de la zone fille est condensée par GOST R 34.11.94, algorithme de numéro <http://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml> 3. Je n'ai pas trouvé de DS GOST dans la nature mais voici l'exemple du RFC, pour la clé 6204 :

<http://www.bortzmeyer.org/5933.html>

```
example.net. 3600 IN DS 6204 12 3 (
    0E6D6CB303F89DBC614DA6E21984F7A62D08BDD0A05B3A22CC63D1B
    553BC61E )
```

Les sections 5 et 6 couvrent des questions pratiques liées au développement et au déploiement de systèmes GOST, par exemple un rappel sur la taille de la clé (512 bits) et sur celle du condensat cryptographique (256 bits).

GOST peut se valider avec Unbound (au moins depuis la version 1.4.4, voir l'option de compilation `--enable-gost`) et avec BIND (depuis la version 9.8, si elle est compilée avec un OpenSSL qui a GOST). On peut trouver des conseils pratiques pour l'utilisation de GOST en anglais à <http://www.cryptocom.ru/dns/dnssec-cryptocom-en.html>.