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. Dernière mise à jour le 30 août 2019

Date de publication du RFC : Juillet 2010

https://www.bortzmeyer.org/5933.html

L'algorithme de signature russe GOST R 34.10-2001 ayant été spécifié en anglais dans le RFC 5832 [1], 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. (Depuis, le GOST R 34.10-2012 a été publié, mais pas normalisé pour DNSSEC.)

La liste originelle des algorithmes DNSSEC figurait dans le RFC 4034, annexe A.1. La liste actuelle est un registre à l'IANA, <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml#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 condensation, 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/openssl100.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 (ce domaine a des clés GOST **et** aussi des clés RSA de type 5) :

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

```
% dig +multi DNSKEY caint.su

; <<>> DiG 9.9.2 <<>> +multi DNSKEY caint.su
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61873
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;caint.su.              IN DNSKEY

;; ANSWER SECTION:
caint.su.              3600 IN DNSKEY 256 3 12 (
                               HQUwRfZDsGuso1XEVztO9nIt7S6MrC/XNYQ9Agup8oW0
                               FCfy0T52buB3czWe9YHa0kLgrcFP1pHpu19jdmO70A==
                               ) ; ZSK; alg = ECCGOST; key id = 35724
caint.su.              3600 IN DNSKEY 257 3 5 (
                               AwEAAdfmAyxcSu09Ik449sIGygbD78jxCKaBek3fhC1a
                               hO7363pdMGlXf8ZEzv7Kl+9yOokmMoTI0peVUqF57it3
                               hmqcIJQ+OsrKdsF1XBwa8VULaLh+TNb67dkdbj6iZ6Gd
                               WxkD6i2vbjvmVHtoQyKswgeR7lUn42XMRYRbYiIrI5r8
                               zT/xllwtCCxaC68V6azpk//7GrYpnwS9NGzr2cBignwj
                               Jj6VeAGfrBe5AM0XNplaFLf7NNU34qqGBKpYbogdAYzM
                               Il02dhPvruzDcadbm2a53OI2/fqchjOgZ8wSTfekuJQb
                               ReYWsNUasgqxjydMU5vweSiogGqkrUEzqn5PD/0=
                               ) ; KSK; alg = RSASHA1; key id = 697
caint.su.              3600 IN DNSKEY 257 3 12 (
                               qMxkfdx4fNxdLDU3z5KGAxrEiL1fm+dxw03js+ACY996
                               wc1wYiVbmqA1QVUmLg5bO3/IawdItM3jQcigFEi/3A==
                               ) ; KSK; alg = ECCGOST; key id = 33831
caint.su.              3600 IN DNSKEY 256 3 5 (
                               AwEAAawWrWjeYqJ+07pakuybnkLQz3xbe1rnG2g7ihfO
                               NpSLNYrNOyhcCTRbt3cgJLWR29Qh6uko9Zcd9uylHlY1
                               ru1HpBQxpzKffwUUki2e7SiTiGrj/DvJz9UH52VZyxi5
                               qf9neYBz0sxvlrLWC5JMqqGIBRUMx/clPjab72BV7exR
                               ) ; ZSK; alg = RSASHA1; key id = 15876

;; Query time: 326 msec
;; SERVER: 192.168.2.254#53(192.168.2.254)
;; WHEN: Tue Oct 23 15:59:57 2012
;; MSG SIZE  rcvd: 621
```

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 (notez qu'il y a double signature, avec RSA et GOST, la clé GOST étant la 35724) :

```
dig +dnssec MX caint.su

; <<>> DiG 9.9.2 <<>> +dnssec MX caint.su
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61031
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;caint.su.                      IN      MX
```

```
;; ANSWER SECTION:
caint.su.               3600    IN      MX      10 mail.caint.su.
caint.su.               3600    IN      RRSIG   MX 5 2 3600 20121027063752 20120927063752 15876 caint.su. E5d1eZ
caint.su.               3600    IN      RRSIG   MX 12 2 3600 20121027063752 20120927063752 35724 caint.su. 52NgP

...
```

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 <`https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml`> 3. Voici un exemple dans la nature :

```
% dig DS caint.su
...
caint.su.               345330  IN      DS      33831 12 3 267B93EB54BF7707BF5500900722F3B0FBFCA04FF4F1BF22735F9
```

Notez que ce domaine a d'autres clés et aussi la même clé condensée par les algorithmes de la famille SHA, soit six DS en tout. Ou un autre exemple dans `.fr` ?

```
absolight.fr. 172724 IN DS 12545 8 3 (
DDA74E5E94CEA6057072B073F60A5DD37D16DC8E896A
EC57B055888DB84B4210 )
```

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). nsd a GOST depuis la version 3.2.11, pubiée en juillet 2012. Pour les programmeurs Java, DNSjava a GOST depuis la version 2.1.7. Pour le statut (recommandé ou non) de l'algorithme GOST pour DNSSEC, voir le RFC 8624. On peut trouver des conseils pratiques pour l'utilisation de GOST en anglais à <`http://www.cryptocom.ru/dns/dnssec-cryptocom-en.html`>.