# RFC 9558 : Use of GOST 2012 Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 21 octobre 2024

Date de publication du RFC : Avril 2024

https://www.bortzmeyer.org/9558.html

---

Ce RFC marque l'arrivée d'un nouvel algorithme de signature dans les enregistrements DNSSEC, algorithme portant le numéro 23. Bienvenue au GOST R 34.10-2012 (alias ECC-GOST12), algorithme russe, spécifié en anglais dans le RFC 7091 [1], une légère mise à jour de GOST R 34.10-2001.

La liste des algorithmes DNSSEC 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 R 34.10-2012 (qui succède au R 34.10-2001 du RFC 5933). Notez que GOST désigne en fait une organisation de normalisation, le terme correct serait donc de ne jamais dire « GOST » tout court, mais plutôt « GOST R 34.10-2012 » pour l'algorithme de signature et « GOST R 34.11-2012 » pour celui de condensation, décrit dans le RFC 6986 (voir la section 1 de notre RFC 9558).

La section 2 décrit le format des enregistrements DNSKEY avec GOST, dans lequel on publie les clés GOST R 34.10-2012. Le champ Algorithme vaut 23, le format de la clé sur le réseau suit le RFC 7091. 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).

Parmi les bibliothèques cryptographiques existantes, au moins OpenSSL met en œuvre GOST R 34.10-2012 (testé avec la version 3.3.2). Voir RFC 9215 pour de l'aide à ce sujet. Sinon, on trouve parfois seulement l'ancienne version dans certains logiciels et certaines bibliothèques.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7091.txt

La section 2.2 donne un exemple de clé GOST publiée dans le DNS, je n'ai pas trouvé d'exemple réel dans la nature, même en `.ru`.

La section 3 décrit le format des enregistrements `RRSIG`, les signatures (avec un exemple). On suit les RFC 5958 et RFC 7091. 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 34.11-2012, algorithme de numéro <`https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xml`> 5.

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 si la bibliothèque de cryptographie utilisée gère GOST. Et, comme indiqué plus haut, ce ne sera sans doute que l'ancienne version, celle du RFC 5933. Pour les programmeurs Java, DNSjava a le dernier GOST depuis la version 3.6.2. Pour le statut (recommandé ou non) de l'algorithme GOST pour DNSSEC, voir le RFC 8624. En Python, dnspython <`https://www.dnspython.org/`> en version 2.7.0 n'a que l'ancien algorithme.