RFC 7091 : GOST R 34.10-2012: Digital Signature Algorithm

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 décembre 2013

Date de publication du RFC : Décembre 2013

https://www.bortzmeyer.org/7091.html

L'algorithme de signature GOST est une norme russe de cryptographie. Son utilisation est obligatoire en Russie pour les services publics. L'ancienne version de cet algorithme de signature, GOST R 34.10-2001, était dans le RFC 5832 [1], que ce nouveau RFC met à jour.

Le caractère très étatique de GOST est rappelé dès la section 1.1 du RFC qui note que l'algorithme a été développé par la FAGCI (ou FAPSI), la NSA russe. Il remplace l'ancien GOST R 34.10-2001 (mais ce RFC ne contient malheureusement pas de description des changements entre les deux versions). GOST est obligatoire en Russie pour les services nationaux (section 2 du RFC).

GOST R 34.10-2012, décrit dans ce RFC, est donc un algorithme de pure signature, ne pouvant pas servir au chiffrement. Reposant sur la cryptographie asymétrique, il est donc sur le même créneau que DSA. Mais, contrairement à lui, il repose sur les courbes elliptiques.

Je vous laisse découvrir ledit algorithme dans le RFC, personnellement, mes compétences en cryptographie sont bien trop faibles pour y comprendre quelque chose. Et le code source ? Il ne semble pas être dans OpenSSL qui a apparemment toujours (version 1.0.1e) l'ancienne version de GOST R 34.10. Pour DNSSEC, le numéro d'algorithme <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml#dns-sec-alg-numbers-1> 12 est explicitement marqué pour l'ancienne version donc il faudra sans doute un nouveau RFC, succédant au RFC 5933, pour passer à GOST R 34.10-2012.

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