RFC 5832 : GOST R 34.10-2001 digital signature algorithm

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 mars 2010

Date de publication du RFC : Mars 2010

https://www.bortzmeyer.org/5832.html

L'algorithme de signature GOST est une norme russe de cryptographie. Son utilisation est obligatoire en Russie pour les services publics. GOST est un algorithme purement local, qui n'avait été décrit qu'en russe et qui n'avait donc jamais suscité d'intérêt à l'étranger (ni, probablement, beaucoup d'essais de cryptanalyse). Ce RFC 5832 [1] (et son compagnon, le RFC 5830, sur l'algorithme de chiffrement) semblent être les premières descriptions de GOST en anglais (il a depuis été remplacé par le RFC 7091). Les RFC précédents comme le RFC 4490 ou le RFC 4491 ne portaient que sur l'usage de GOST.

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 « sous la direction du Président de la Fédération ». GOST étant obligatoire en Russie pour les services nationaux (section 2 du RFC) , les responsables du TLD `.ru` ont donc annoncé qu'ils ne pourraient pas déployer DNSSEC si celui-ci ne fournit pas un moyen d'utiliser GOST (en plus de DSA et RSA). Une des étapes nécessaires à l'utilisation de GOST dans DNSSEC était la disponibilité d'un texte stable décrivant GOST, ce qui est désormais le cas. (Et du RFC 5933 qui spécifie son intégration dans DNSSSEC.)

GOST R 34.10-2001, 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 ? Pour OpenSSL, il existe une distribution de GOST <http://www.cryptocom.ru/opensource/openssl100.html>.

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