RFC 6986 : GOST R 34.11-2012: Hash Function

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 septembre 2013

Date de publication du RFC : Août 2013

https://www.bortzmeyer.org/6986.html

Ce RFC documente en anglais une norme russe de l'organisme GOST. GOST R 34.11-2012 est une fonction de condensation cryptographique. Elle pourra notamment être utilisée pour DNSSEC.

Les algorithmes GOST (un abus de langage puisque GOST est normalement le nom de l'organisme de normalisation) sont une alternative russe aux algorithmes de cryptographie d'origine états-unienne comme RSA ou ECDSA (qui peuvent être remplacés par GOST R 34.10-2001) ou comme SHA-2 (qui peut être remplacé par GOST R 34.11-2012, qui fait l'objet de ce RFC). Pour être utilisés dans les protocoles IETF, il leut fallait une documentation en anglais. GOST R 34.10-2001 avait été documenté dans le RFC 5832 [1]. Notre RFC 6986 documente le petit dernier membre de la famille (son prédécesseur pour la condensation, GOST R 34.11-94, était dans le RFC 5831). Notez que les algorithmes GOST sont normalisés pour un usage dans le cadre de DNSSEC (RFC 9558).

Comme les autres algorithmes GOST, notre R 34.11-2012 est donc un algorithme officiel en Russie. Il a été approuvé par le décret n° 216 de l'agence fédérale chargée de la régulation technique, en août 2012. À terme, il vise à remplacer l'ancien R 34.11-94. C'est un algorithme de condensation cryptographique, qui peut produire des condensats de 256 ou 512 bits.

Je ne vais pas essayer de vous expliquer son principe de fonctionnement (sections 4 à 10), car c'est trop loin de mon domaine de compétence. Si vous êtes plus courageux que moi, notez qu'il y a beaucoup de maths et que, dans le formatage texte brut des RFC, ce n'est pas forcément idéal.

Questions mises en œuvre, notez qu'OpenSSL 1.0.1c n'a apparemment pas d'algorithmes de condensation GOST par défaut. `openssl dgst -h` pour voir la liste. Il faut apparemment éditer le openssl.cnf <http://stackoverflow.com/questions/10959771/openssl-and-gost-engine-issue-statically-lin pour y avoir accès.

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