RFC 8891 : GOST R 34.12-2015: Block Cipher "Magma"

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 septembre 2020

Date de publication du RFC : Septembre 2020

https://www.bortzmeyer.org/8891.html

Ce RFC décrit un algorithme russe de chiffrement symétrique, « GOST R 34.12-2015 », surnommé Magma. N'attendez pas de ma part des conseils sur l'utilisation ou non de cet algorithme, je résume juste le RFC.

GOST est le nom des normes de l'organisme de normalisation officiel en Russie (et, par abus de langage, leurs algorithmes sont souvent cités sous le nom de « GOST » tout court). Cet organisme a normalisé plusieurs algorithmes de chiffrement symétrique dont Kuznyechik (décrit dans le RFC 7801 [1]) et l'ancien « GOST 28147-89 » (RFC 5830). Ce dernier est remplacé par « GOST R 34.12-2015 », qui fait l'objet de ce RFC. (La norme russe officielle est disponible en ligne <http://tc26.ru/standard/gost/GOST_R_3412-2015.pdf> mais, de toute façon, le russe plus la cryptographie, ce serait trop pour moi). Comme d'autres algorithmes de cryptographie normalisés par GOST, Magma a été développé en partie par le secteur public (Service des communications spéciales et d'information du Service fédéral de protection de la Fédération de Russie) et par le secteur privé (InfoTeCS <http://www.infotecs.ru/>). Le décret n° 749 du 19 juin 2015, pris par l'Agence fédérale pour la régulation technique et la métrologie en a fait un algorithme russe officiel.

Du fait de ce caractère officiel, si vous vendez des produits ou des prestations de sécurité en Russie, vous serez probablement obligés d'inclure les algorithmes GOST.

Je vous laisse lire le RFC pour la description de l'algorithme (ou l'original russe <http://tc26.ru/standard/gost/GOST_R_3412-2015.pdf>, si vous lisez le russe). Notez que, contrairement à son prédécesseur (cf. RFC 5830, sections 5 à 7), il ne décrit pas les modes utilisables, chacun choisit celui qui lui semble adapté.

Question mises en œuvre, il y en a une compatible <http://gostcrypto.com/index.html> avec WebCrypto, ou bien une <https://github.com/gost-engine/engine> pour OpenSSL.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7801.txt