RFC 8998 : ShangMi (SM) Cipher Suites for TLS 1.3

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 mars 2021

Date de publication du RFC : Mars 2021

https://www.bortzmeyer.org/8998.html

La cryptographie est un outil essentiel pour la sécurité sur les réseaux numériques. N'avoir comme algorithmes de cryptographie que des algorithmes développés à l'étranger peut être jugé dangereux pour la sécurité nationale. Des pays comme la Russie et, bien sûr, les États-Unis, recommandent ou imposent des algorithmes « nationaux ». La Chine s'y met, avec les algorithmes de chiffrement ShangMi (« SM »), dont ce RFC décrit l'utilisation dans TLS.

Comme ces algorithmes sont obligatoires en Chine pour certaines applications (comme c'est le cas de l'algorithme russe Magma décrit dans le RFC 8891 [1]), il était nécessaire que TLS (RFC 8446) puisse les utiliser, indépendamment de l'opinion des cryptographes « occidentaux » à leur sujet. Ce RFC traite de deux algorithmes de chiffrement symétrique (« SM4 ») avec chiffrement intègre, une courbe elliptique (« curveSM2 »), un algorithme de condensation (« SM3 »), un algorithme de signature (« SM2 ») utilisant curveSM2 et SM3, et un d'échange de clés fondé sur ECDHE sur SM2. (Au passage, saviez-vous qu'il existe une courbe elliptique française officielle <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000024668816> ?)

On notera que les Chinois n'ont pas poussé leurs algorithmes qu'à l'IETF, certains sont aussi normalisés à l'ISO (ISO/IEC 14888-3 :2018 <https://www.iso.org/standard/76382.html>, ISO/IEC 10118-3 :2018 <https://www.iso.org/standard/67116.html> et ISO/IEC 18033-3 :2010 <https://www.iso.org/standard/54531.html>).

Le RFC ne décrit pas les algorithmes eux-mêmes, uniquement comment les utiliser dans le contexte de TLS 1.3 (RFC 8446). Si vous êtes curieux, les normes chinoises sont :

— Pour l'algorithme de condensation SM3 : Norme GBT.32905-2016 <http://www.gmbz.org.cn/upload/2018-07-24/1532401392982079739.pdf>.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8891.txt

— Pour l'algorithme de chiffrement symétrique SM4 : Norme GBT.32907-2016 <http://www.gmbz.org.cn/upload/2018-04-04/1522788048733065051.pdf>.
— Pour l'algorithme de signature SM2 : normes GBT.32918.2-2016 <http://www.gmbz.org.cn/upload/2018-07-24/1532401673138056311.pdf> et GBT.32918.5-2016 <http://www.gmbz.org.cn/upload/2018-07-24/1532401863206085511.pdf>.

Les deux algorithmes de chiffrement symétrique sont désormais dans le registre IANA <https://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-4> sous les noms de TLS_SM4_GCM_SM3 et TLS_SM4_CCM_SM3. L'algorithme de signature, sm2sig_sm3 est dans le registre approprié <https://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-signaturescheme>. La courbe elliptique curveSM2 a été ajoutée à un autre registre <https://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-8>.

Je ne connais pas de mise en œuvre de ces algorithmes dans les bibliothèques TLS habituelles. Si vous avez des informations…Mais Wireshark va bientôt savoir les afficher <https://gitlab.com/wireshark/wireshark/-/merge_requests/2434>.

Ah, et si vous vous intéressez à l'Internet en Chine, je vous recommande le livre de Simone Pieranni, Red Mirror <https://www.bortzmeyer.org/red-mirror.html>.