RFC 9151 : Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 avril 2022

Date de publication du RFC : Avril 2022

https://www.bortzmeyer.org/9151.html

Le choix est vaste parmi les algorithmes de cryptographie. Des protocoles comme TLS offrent de l'agilité cryptographique, c'est-à-dire la possibilité d'avoir différents algorithmes pour un même protocole. Pour l'administrateur système qui n'est pas un ou une expert en cryptographie, lesquels choisir ? Pour l'aider, les agences de sécurité nationales font souvent des documents synthétisant leur analyse des bons algorithmes du moment. C'est le cas du RGS en France, par exemple. Ce RFC définit le profil TLS de CNSA ("*Commercial National Security Algorithm*"), les bons algorithmes recommandés par la NSA.

C'est d'ailleurs le deuxième RFC écrit par un employé de cette agence étatsunienne, après le RFC 5903 [1] mais il est évidemment possible que certains auteurs aient été discrets sur leur affiliation.

Ce profil CNSA ("*Commercial National Security Algorithm*") est destiné à être utilisé dans le cadre de TLS, plus exactement ses versions 1.2 (RFC 5246) et 1.3 (RFC 8446). Le cadre réglementaire étatsunien est SP 80059 <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf>. Un rappel : il s'agit d'un profil, une restriction des algorithmes possibles, il ne définit pas de nouvel algorithme, il liste juste ceux à utiliser, par exemple ceux des RFC 5288 et RFC 5289. C'est en effet une de missions de la NSA que de conseiller l'État et les entreprises en matière de cryptographie. (La NSA a également une mission offensive, qui va en sens inverse, les encourageant par exemple à garder secrètes des vulnérabilités, pour qu'elle puisse les exploiter.) Cette suite CNSA n'a rien de très novateur, elle est dans la continuation des précédentes, le prochain grand changement, estime la NSA, sera le passage aux algorithmes post-quantiques. (Notez que l'analyse de la NSA sur les mesures à prendre en attendant les calculateurs quantiques est très discutée <https://eprint.iacr.org/2015/1018.pdf>.)

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5903.txt

Après ces préliminaires, la suite CNSA elle-même (section 4). Elle inclut les grands classiques, Diffie-Hellman avec les corps finis, les courbes elliptiques du NIST et encore RSA, les signatures avec les courbes elliptiques (ECDSA seulement) et RSA, et l'algorithme de chiffrement symétrique AES en intègre avec GCM (ChaCha - RFC 8439, sans doute pas assez officiel, n'est pas cité). CNSA impose des tailles minimales de clés, par exemple 3 072 bits pour une signature avec RSA. Pour la condensation, c'est SHA-384 seulement (j'ignore pourquoi SHA-256 et les autres ne sont pas cités).

Pour la version de TLS, la section 5 de notre RFC impose au minimum 1.2 (c'est un des points où le blog que vous êtes en train de lire n'est pas conforme aux recommandations de la NSA…). Si on utilise une courbe elliptique (cf. RFC 8422), cela doit être la P-384 du NIST. (Saviez-vous d'ailleurs qu'il existe une courbe elliptique française, « FRP256 », publiée `<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000024668816>` au Journal officiel ?) Et au passage, les certificats doivent suivre le profil du RFC 8603.

Pour TLS 1.3 (RFC 8446), CNSA impose de tirer profit de certaines nouveautés de cette version, comme l'extension `signature_algorithms`. Par contre, il faut refuser `early_data` (les raisons sont dans la section 2.3 du RFC 8446).