RFC 5581: The Camellia Cipher in OpenPGP

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 juin 2009

Date de publication du RFC : Juin 2009

https://www.bortzmeyer.org/5581.html

La cryptographie évoluant sans cesse, il est nécessaire, pour tous les protocoles Internet qui en dépendent, de prévoir la possibilité d'utiliser plusieurs algorithmes de cryptrographie, au fur et à mesure que les anciens craquent sous les coups de la cryptanalyse. Le format PGP, normalisé dans le RFC 4880 ¹ peut ainsi désormais utiliser l'algorithme de chiffrement symétrique Camellia. (Depuis, notre RFC 5581 a été intégré dans la norme OpenPGP, qui est désormais le RFC 9580.)

Le RFC est très court car il n'y a pas grand'chose à dire. Camellia, un algorithme symétrique à blocs, d'origine japonaise, est décrit dans le RFC 3713. Notre RFC 5581 se contente de l'ajouter à la liste officielle des algorithmes PGP https://www.iana.org/assignments/pgp-parameters/pgp-parameters-13, aux côtés de protocoles comme AES et Twofish.

^{1.} Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4880.txt