RFC 9155 : Deprecating MD5 and SHA-1 signature hashes in (D)TLS 1.2

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 décembre 2021

Date de publication du RFC : Décembre 2021

https://www.bortzmeyer.org/9155.html

Vous le savez certainement déjà, car toutes les lectrices et tous les lecteurs de ce blog sont très attentif·ves et informé·es, mais les algorithmes de condensation MD5 et SHA-1 ont des failles connues et ne doivent pas être utilisés dans le cadre de signatures. Vous le savez, mais tout le monde ne le sait pas, ou bien certain·es ont besoin d'un document « officiel » pour agir donc, le voici : notre RFC dit qu'on ne doit plus utiliser MD5 et SHA-1 dans TLS.

Si vous voulez savoir **pourquoi** ces algorithmes sont mauvais, le RFC 6151 [1] vous renseignera (et la section 1 de notre RFC 9155 vous donnera une bibliographie récente).

La section 2 à 5 sont le cœur du RFC et elle est sont très simples : pas de MD5, ni de SHA-1 pour les signatures. Dans le registre IANA <https://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-signaturescheme>, ces algorithmes sont désormais marqués comme déconseillés.

Les fanas de cryptographie noteront qu'on peut toujours utiliser SHA-1 pour HMAC (où ses faiblesses connues n'ont pas de conséquences).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6151.txt